Universidad Cenfotec

Maestría en Ciberseguridad

Documento Final de Proyecto de Investigación Aplicada 2

Reconocimiento de sitios web sospechosos por medio de una aplicación móvil de escaneo

Rodríguez Valverde Douglas

Mayo, 2019

Declaratoria de derechos de autor

Agradecimientos

A Dios, que me brinda la motivación, salud, sabiduría y perseverancia para poder trabajar y cumplir las metas que me propongo. Y esa ha sido la constante a lo largo de toda la maestría.

A mis padres, que han sido un pilar fundamental con su apoyo. Siempre han estado ahí cuando los necesito y de manera desinteresada me han ayudado. Como así también mis familiares (abuela, tíos, tías, hermanos) que con palabras de apoyo o simples gestos han contribuido en este caminar.

Profesores de maestría, que con su esfuerzo logran compartir conocimiento para la correcta formación académica, y muchas veces dando de más. Sin duda que es digno de señalar. También agradecer a todos los miembros administrativos de la Universidad Cenfotec, que son los que hacen posible que las cosas marchen, aportando su grano de arena para ofrecer una educación decente y de calidad.

Por último, agradezco a mis amigos y amigas, que con sus palabras, consejos y muestras de afecto han servido de aliciente para la lucha de este sueño.

Dedicatoria

La dedicatoria del presente proyecto va dirigida a mi familia: mi padre Edwin, mi madre Carmen, mis hermanas; Ana Lucía, María Eugenia y mi hermano Edwin.

Tabla de Contenido

Índice de imágenes y tablas

Resumen Ejecutivo

El proyecto en curso y toda su investigación van dirigidos a todos aquellos usuarios que de una u otra forma tienen poca experiencia en el uso de Internet y todo el entorno que éste conlleva.

En el día a día, cada vez son más los servicios y facilidades que se migran al ciberespacio, siendo Internet el medio preferido por las personas para realizar negocios, compras y un sinfín de actividades que nos pueden hacer la vida un poco más fácil. Sin embargo, al igual que el mundo físico nos expone a peligros o riesgos tales como robo, estafas y extorsiones, en el mundo digital existen los mismos peligros, pero en otras versiones. Dado esto y el creciente aumento en sitios web maliciosos que sirven como la antesala a posibles fraudes o infección de nuestros equipos por malware, es que se planea diseñar una aplicación móvil que le permita a cualquier tipo de usuario –pero en especial a aquellos con menos pericia- a escanear los sitios URL por medio del teléfono celular y de esta forma poder alertar de posibles riesgos si se ingresa a dicho sitio.

Palabras Clave: investigación, Internet, peligros, riesgos, URL, aplicación móvil, escanear

Capítulo 1. Introducción

1.1 Generalidades

Son muchos los casos de fraude electrónico, casos de phishing, suplantación de identidad, que en la gran mayoría trae consigo un sitio web falso o de dudosa fuente. Es por esto que sugerir la revisión y análisis de los URL, viene a aminorar o convertir en conato ciertas acciones contra usuarios despistados o desinformados. La creación de la aplicación móvil de escaneo de URLs por parte del autor de este proyecto en conjunto con la empresa Zimplifica S.A, trae beneficios como; crear conciencia en los usuarios a no confiar en todos los sitios URL, tener un punto de respaldo para evitar ser presa de una estafa, dar seguridad a los usuarios que sus equipos no están siendo infectados con códigos maliciosos.

1.2 Antecedentes del Problema

Ante la duda e incertidumbre que está presente en la navegación web, de si el sitio es potencialmente peligroso o no, no existe una aplicación móvil a la fecha (tercer cuatrimestre del año 2018 a primer cuatrimestre del año 2019) que pueda escanear las direcciones URL de las páginas web y pueda emitir un aviso al usuario si se encuentra ante un sitio peligroso o no.

1.3 Definición y Descripción del Problema

El problema se centra en los riesgos que están presentes en algunos sitios web, que roban información a usuarios, otros, infectan los equipos por medio de descarga sin consentimiento de software malicioso, o en algunos casos, la ejecución de minado de criptomonedas, donde se saca provecho de los recursos de las

máquinas de los usuarios. La mayor parte de los usuarios no técnicos no se dan cuenta de que todas estas cosas suceden en segundo plano, y es éste el problema principal que se desea aminorar.

1.4 Justificación

En Internet existen diferentes sitios que ayudan a realizar la tarea de análisis y revisión de sitios web potencialmente peligrosos, al indicar así que los mismos poseen inyección de código, descarga de archivos sin consentimiento, entre otros.

El valor agregado en este proyecto está en conjugar los servicios que brindan esos sitios en una aplicación móvil accesible a cualquier usuario, pudiendo así ejecutar el análisis desde su teléfono celular. Con esto se llega a solventar un problema, el cual es engaño o descuido de usuarios ante una posible amenaza web. Además, se crea conciencia en los usuarios a no confiar en todos los sitios web que accedan, por último, que la aplicación sirva de herramienta complementaria para realizar el punto anterior.

1.5 Viabilidad

1.5.1 Punto de Vista Técnico.

Al analizar desde el punto de vista técnico, existen los medios técnicos tanto por la empresa que respalda el proyecto como el autor de este proyecto. Queda en evidencia la viabilidad del mismo. En caso de necesitar alguna recomendación o referencia, la empresa se compromete a facilitar la ayuda técnica necesaria.

1.5.2 Punto de Vista Operativo.

Desde el punto operativo, la investigación es viable, ya que no entorpece ni altera las tareas del día a día en la empresa de soporte. El proyecto se planea realizar en su gran mayoría en horario de fines de semana y con acompañamiento o reuniones esporádicas con la contraparte de la empresa Zimplifica SA. Lo cual deja en evidencia la viabilidad del punto operativo.

1.5.3 Punto de Vista Económico.

El punto de vista económico no está ligado a un gasto por parte de la empresa Zimplifica SA, ya que las herramientas y equipo son propiedad del investigador, así también como el “costo teórico”, es por eso que se hace la salvedad, para que la empresa esté consciente de ello. En el momento que se necesite alguna licencia o software de pago, se evaluará entre ambas partes (empresa e investigador) para sufragar las mismas.

1.6 Objetivos

Se decide utilizar la taxonomía de Bloom revisada ya que proporciona una buena colección de verbos, que, en esta versión revisada, los sustantivos han cambiado por verbos que ayudan a dar un mejor enfoque creativo (verbo “crear”, nuevo en la esta versión de Bloom revisada) para el proyecto de investigación. (Anderson & Krathwohl, 2001)

Por último, el uso de la taxonomía va de la mano en los dominios cognoscitivos de alto nivel a los que el investigador se verá inmerso.

1.6.1 Objetivo General.

Diseñar una aplicación móvil que permita el escaneo y análisis de direcciones electrónicas (URL), generando una respuesta de riesgo positiva o negativa de las mismas.

1.6.2 Objetivos Específicos.

1. Elaborar una interfaz que permita la captura de una dirección URL para su posterior análisis.
2. Aplicar una interfaz de programación de aplicaciones (API) para analizar todas las direcciones electrónicas.
3. Realizar un análisis comparativo de soluciones equivalentes.
4. Elaborar un prototipo funcional de escaneo de análisis de direcciones URL para la empresa Zimplifica S.A

1.6.3 Cronograma del proyecto

Para el plan del proyecto en curso, se trabaja con un cronograma que abarque 2 cuatrimestres, para un total de 30 semanas. En este caso el estudiante a cargo del proyecto es el único recurso encargado de realizar cada fase, para su revisión se contará con la ayuda del profesor tutor.

Fecha		Entregable	Etapa
Semana 1	8-Oct-18		
Semana 2	15-Oct-18	Investigación sobre las características de un sitio web sospechoso	INVESTIGACIÓN
Semana 3	22-Oct-18		
Semana 4	29-Oct-18	Investigación sobre el ambiente Android para su posterior desarrollo	

Semana 5	5-Nov-18		
Semana 6	12-Nov-18	Creación y corrección de objetivo general y específicos	
Semana 7	19-Nov-18		
Semana 8	26-Nov-18	Investigación de los servicios web existentes para posible análisis de sitios web	
Semana 9	3-Dec-18		
Semana 10	10-Dec-18		
Semana 11	17-Dec-18	Creación de ambiente de desarrollo Android	
Semana 12	31-Dec-18		
Semana 13	7-Ene-19	Creación de prototipo de aplicación móvil Android de escaneo	DISEÑO
Semana 14	14-Ene-19	Creación de cuadro comparativo entre aplicaciones del mismo índole	
Semana 15	21-Ene-19		
Semana 16	28-Ene-19	Pruebas de concepto para el consumo de servicios web	
Semana 17	4-Feb-19		
Semana 18	11-Feb-19		
Semana 19	18-Feb-19		
Semana 20	25-Feb-19	Desarrollo de aplicación móvil de escaneo	EJECUCIÓN
Semana 21	4-Mar-19		
Semana 22	11-Mar-19		
Semana 23	18-Mar-19		
Semana 24	25-Mar-19	Ejecución de pruebas	
Semana 25	1-Apr-19	Análisis de los resultados de la aplicación	
Semana 26	8-Apr-19	Revisión de documento	
Semana 27	15-Apr-19		
Semana 28	22-Apr-19	Edición del documento escrito	
Semana 29	1-May-19	Finalización del documento	PRESENTACIÓN
Semana 30	6-May-19	Revisión de documento	
Semana 31	13-May-19	Aplicar correcciones	
Semana 32	25-May-19	Envío documento a la Universidad	

Tabla 1 - Cronograma del Proyecto

1.7 Alcances y Limitaciones

1.7.1 Alcances.

Siguiendo los objetivos, se tiene como base la creación de una aplicación móvil (siendo un prototipo funcional) que centre su tarea en el escaneo de direcciones URL. Para luego interpretarlas como una dirección válida y posterior a eso, analizarlas contra un servicio web que ayudará a identificar si el sitio web

posee indicios de ser perjudicial para el usuario o no, esto por medio de un mensaje en pantalla al final del análisis.

1.7.2 Limitaciones.

Para la creación de la aplicación móvil, se delimita la creación del entorno en la plataforma Android. Además, en esta fase no se tiene contemplado subir la aplicación al repositorio de Play Store, mismo dónde el usuario accede para descargar cualquier aplicación.

1.9 Estado de la Cuestión

De manera escalonada se muestra el escenario actual donde los sitios web sospechosos cada día van en aumento, aunado también por el creciente número de accesos desde dispositivos móviles reflejan como cada pieza converge en la investigación de la mezcla entre poder dar uso a una aplicación móvil para la detección o alerta de un sitio web sospechoso.

Sitios web sospechosos. Existe una diferencia –muchas veces no percibida por el usuario final- entre un sitio web sospechoso o maligno a uno seguro. Este último es muy sencillo de describir ya que sería el escenario perfecto de navegación web, en donde podemos revisar noticias, ver videos o hacer compras electrónicas sin mayor dificultad. Pero el primer caso si nos lleva a un análisis un poco más profundo. Según Symantec Corporation un sitio web malicioso es "*un sitio que intenta instalar 'malware' en nuestro dispositivo. Algunas veces requiere acción por parte del usuario, en otros casos como el 'drive-by download' el sitio web puede instalar software en el equipo sin consentimiento del usuario*". (Symantec, 2018)

Dispositivos móviles. En el campo de la tecnología, siempre se ha apostado por llevar funcionalidad a dispositivos portátiles. Son muchas las versiones y funciones que estos dispositivos realizan. ¿Pero qué características debe reunir un aparato para ser catalogado como móvil?, para ello existen algunas características que lo definen, Jaime en su informe lo explica como "*1. De reducido tamaño, haciéndolo fácil de transportar. 2. Cuenta con cierta capacidad de computación y almacenamiento de datos. 3. Incorpora elementos de E/S básicos (pantalla, teclado)*" (Aranaz, 2009) y es con el ejemplo anterior que nos queda claro que un dispositivo móvil no necesariamente es un teléfono celular, sin embargo existe una relación muy arraigada.

Aplicaciones móviles. Las aplicaciones móviles, desde sus inicios han sido una extensión funcional de equipos no móviles que responden a ciertas tareas de la vida cotidiana, en sus formas más básicas se encuentran calculadoras, diccionarios, agendas, hasta juegos inclusive. Con el paso del tiempo han evolucionado hasta poder sugerir el pronóstico del tiempo, juegos de realidad aumentada, y hasta navegación GPS.

Las aplicaciones móviles las podemos clasificar en dos tipos, según el sitio Genexus, en aplicaciones Nativas y WebApps optimizadas. "*Las Aplicaciones Nativas son aquellas que se desarrollan para un determinado sistema operativo en el móvil. Se crean exclusivamente para teléfonos móviles, debiéndose crear una para iOS, otra para Android, las segundas son más sencillas de desarrollar y se manejan desde un ordenador. Los desarrolladores no usan diferentes lenguajes de programación; por el contrario, las desarrollan en lenguajes conocidos como JavaScript o el HTML.*" (Genexus, 2016)

Seguido de definir algunos aspectos importantes en la investigación nos apegamos a Biolchini. (2005) para realizar una adecuada revisión sistemática, al establecer así un adecuado estado de la cuestión referente a la identificación de sitios web sospechosos, pudiendo ser analizados desde una aplicación móvil.

1.9.1 Revisión sistemática

1.9.1.1 Formulación de las preguntas

Enfoque de la pregunta. Identificar las características que poseen los sitios web sospechosos que perjudican o afectan a la mayoría de la población internauta.

Calidad y amplitud de la pregunta

- **Problema**. Se necesita poder identificar cuándo un sitio web es potencialmente peligroso ante un usuario, o bien, cuales sitios web tienen falencias en seguridad que vayan a poner en riesgo la información del usuario.

- **Pregunta**. ¿Cuáles son las características de un sitio web sospechoso?

- **Palabras clave**. Website, malicious, application

- **Intervención**. Identificación de páginas web maliciosas

- **Control**. Ninguno

- **Efecto**. Solución de escaneo móvil de URL para personas con poca pericia en el uso de internet.

- **Medida de resultado**. A criterio del investigador

- **Población**. Artículos y publicaciones referentes a seguridad informática.

- **Aplicación**. Aplicaciones móviles

- **Diseño experimental**. Ninguno

1.9.1.2 Selección de fuentes

Definición de criterios de selección de fuentes. Los criterios para la selección de fuentes se basan en el uso de repositorios de información (tesis de maestría y doctorado) en el tema de la seguridad de la información. Además del uso de palabras clave previamente identificadas.

Lenguaje de estudio. Inglés.

Identificación de recursos

Métodos de búsqueda de recursos. Se utilizan motores de búsqueda de Internet.

String de búsqueda. Identifying+suspicious+websites

Lista de recursos. Google académico (scholar.google.es)

Selección de recursos después de la evaluación. La selección del motor de búsqueda comprende trabajos serios y bien fundamentados.

Revisión de referencia. Aprobado

1.9.1.3 Selección de estudios

Definición de estudios

- Definición de criterios de inclusión y exclusión de estudios. El análisis y estudios se realizarán con base en las características de los sitios web sospechosos o aquellos que presenten falencias en seguridad. Se excluyen de este estudio los resultados que tengan más de 2 años de antigüedad (a la fecha de publicación de este proyecto)

- **Definición de los tipos de estudios**. Los estudios relacionados con el área de CiberSeguridad.

- **Procedimiento para la selección de estudios.** Se procede en primera instancia con la ejecución en los distintos motores de búsqueda web. Luego se analizan los resultados contra los criterios de inclusión anteriormente definidos y por último se realiza el descarte de los que cumplen para ser incluidos.

Ejecución de la selección

- Selección inicial de estudios:

* Filter-based identification of malicious websites

* Detecting Malicious Web Links and Identifying Their Attack Types

* Efficient suspicious URL filtering based on reputation.

- Evaluación de la calidad de los estudios. Los análisis de los resultados obtenidos cumplen con los criterios de selección para la presente investigación, además cumplen también con el área de seguridad informática.

- Estudio Seleccionado. Detecting Malicious Web Links and Identifying Their Attack Types

Revisión de los estudios. Aprobado

1.9.1.4 Extracción de la información

Definición de criterios de inclusión y exclusión de la información. La información que se espera extraer debe contener criterios o características de sitios web sospechosos para ser posteriormente identificados con una aplicación web.

Formulación de extracción de datos. Para la extracción de datos se considera adecuado utilizar la siguiente plantilla

Estudio:
Tipo de Estudio:
Definición del problema:
Contexto:
Enfoque:
Método:
Confiabilidad del método:
Resultados:
Conclusiones:

Extracción de resultados objetivos

1.9.1.5 Resumen de los resultados

Los resultados se pueden observar en la siguiente tabla:

Estudio. Detecting Malicious Web Links and Identifying Their Attack Types
Tipo de Estudio. Análisis
Definición del problema. La proliferación de sitios web maliciosos, cómo se pueden identificar y sus distintos tipos de ataques.
Contexto. El contexto de la investigación se basa en los sitios web sospechosos, y que son perjudiciales para los usuarios inexpertos al uso de la tecnología.

Enfoque. El enfoque de la investigación radica en ofrecer un control compensatorio a la hora de analizar si un sitio web es sospechoso mediante la ayuda de una aplicación móvil de escaneo.
Método. El estudio e investigación a través de los últimos 8 años sobre los tipos de ataques y falencias de los sitios web, son buenos insumos para determinar una lista de las características más comunes en los sitios web que los hacen ser sospechosos y poco confiables.
Confiabilidad del método. Se confía en el método utilizado por los vastos trabajos de investigación encontrados en repositorios como Google Académico.
Resultados. Se evalúan los resultados para la presente investigación y se genera una lista de las carencias principales de un sitio web que lo hace sospechoso.
Conclusiones. Luego de la investigación y análisis se logra obtener las siguientes características de un sitio web sospechoso: • Sitios web que no utilicen cifrado o certificados • Sitios web que implementan scripts maliciosos • Sitios web en dominios de lista negra • Sitios web con enlaces rotos y faltas ortográficas. • Sitios web de descargas drive-by.

Tabla 2 - Extracción de datos para estudio de detección de URLs sospechosos

Número de estudios: 3 sitios consultados y revisados, 1 seleccionado.

1.9.1.6 Comentarios finales

Los diferentes resultados encontrados, tratan de la identificación y análisis de sitios web catalogados como phishing. Sin embargo, se escoge el resultado que abarca más clasificaciones de amenazas contra el usuario final.

Capítulo 2. Marco Teórico

A diferencia de los años noventa, dónde el día a día de una persona no involucraba tanto el uso de Internet, hoy día se puede decir que es un recurso imprescindible. Tanto para cuestiones laborales, de estudio o simplemente ocio, es un hecho que su uso va en aumento, a raíz de esto la proliferación de sitios web ha hecho de nuestras vidas una herramienta de consulta diaria. Es por esto que la correcta identificación de sitios web de confianza versus aquellos que son dañinos, nos puede ahorrar dolores de cabeza a la hora de frecuentar un sitio web en particular.

Para lograr esto, muchas veces se necesita de cierta pericia técnica al revisar ya sea a simple vista; si el sitio web utiliza cifrado, si maneja certificados, o bien, al utilizar extensiones en el navegador que impidan o alerten la ejecución de scripts, por otro lado también, utilizar sitios web de compañías que provean servicios de seguridad como revisión de URLs. Todo esto solamente para estar seguros de que el sitio web cumple con ciertos filtros que nos garantizarán un poco la seguridad.

Las recomendaciones anteriormente descritas, son en muchos casos desconocidas por los usuarios no técnicos (adultos mayores, padres de familia, personas con poco grado de escolaridad) y que tienen acceso a Internet en cualquier dispositivo. Por esta razón que surge la necesidad de crear una herramienta que sea capaz de escanear un link de un sitio web y generar un resultado que ayude al usuario a tomar una decisión de si continúa o no con el acceso o transacción del sitio. Para poder tener un panorama más amplio sobre las características de los sitios web sospechosos y la relación del cómo se puede revisar mediante una aplicación móvil se definen los siguientes apartados.

2.1 Características de sitios web sospechosos

La diferencia más notoria entre un sitio web sospechoso ante uno de confianza es la manera en que se comporta el equipo una vez se accede a dicho sitio, es una señal que en muchos casos el usuario lo nota, sin embargo, con el paso del tiempo y la evolución de las páginas web, existen muchos sitios a los cuales ingresamos y de manera silenciosa nos vemos expuestos a distintos ataques que son imperceptibles por el usuario. A la hora de analizar y revisar las características de un sitio web sospechoso tenemos varios factores que juegan un papel importante que nos pueden hacer dudar, entre los más comunes tenemos los siguientes.

2.1.1 Sitios web que no utilicen cifrado o certificados

Ante la evolución de los sitios web, ha surgido la necesidad de poder garantizar “la identidad” de los mismos, por ejemplo, un pasaporte que identifica una persona cuando viaja sería una buena analogía. Por otro lado, también tenemos la información que viaja a través de los equipos entre los usuarios y los servidores, misma que debe ser segura y libre de interrupciones o modificaciones malintencionadas. Es por eso que nacen los certificados de seguridad, tal como lo menciona el sitio Certsuperior “Los *certificados de seguridad son una medida de confianza adicional para las personas que visitan y hacen transacciones en su página web, le permite cifrar los datos entre el ordenador del cliente y el servidor que representa a la página.*” (Certsuperior, 2016)

Pero, ¿Cómo se sabe si el sitio web utiliza certificados de seguridad?, basta con revisar la dirección electrónica -dirección URL- y ver que comienza con HTTPS,

en vez de su sucesor, el clásico HTTP. Este primero no es más que un protocolo que utiliza cifrado SSL (Secure Socket Layer) y TLS (Transport Layer Security) basándose en su predecesor el HTTP.

Por lo cual, se hace la mención en este apartado sobre la importancia de ingresar a sitios web “certificados”, ya que es la misma evolución digital que nos obliga a estar cada vez más seguros. Tanto es así que Google está comenzando una campaña de seguridad para marcar o resaltar todos aquellos sitios que no estén cifrados con HTTPS (Schechter, 2018)

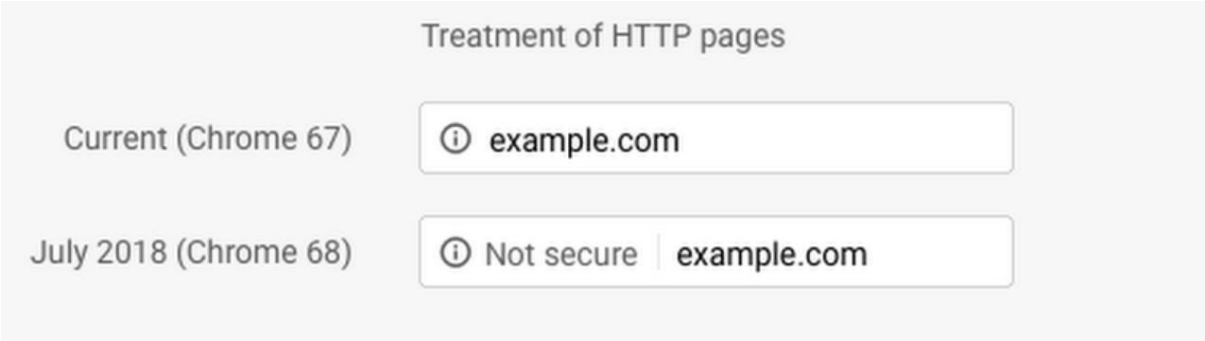


Imagen 1 - Amenaza de página HTTP (Schechter, 2018)

2.1.2 Sitios web que implementan scripts maliciosos

Las amenazas informáticas, entre ellas virus, que en sus inicios comenzaban su propagación -hace algún tiempo atrás, entre los años ochenta y noventa- por medios extraíbles como disquetes, discos compactos, entornos de red, entre otros, comenzaron atormentando a los usuarios dañando sus archivos, equipos e imagen. Hoy día, estas amenazas han mutado para convertirse en malware, y han llegado hasta páginas web para alojarse de forma silenciosa por medio de scripts, que posteriormente serán ejecutados cuando un usuario ingrese desde su equipo.

El funcionamiento de un script malicioso, según lo describe Josep en el sitio Welivesecurity, es cuando “*los delincuentes pueden ejecutar código malicioso en los sistemas de los usuarios aprovechando alguna de las múltiples vulnerabilidades que*

pueden tener, tanto en los navegadores como en el propio sistema o en aplicaciones de terceros." (Albors, 2016) No importa si el sitio al cual frecuentamos a menudo es de confianza, si el mismo fue blanco de un ataque horas antes que ingresamos, nos vamos a ver en aprietos con la ejecución en nuestros equipos de rutinas indeseables que muchas veces desencadena en: secuestro de nuestros datos (ransomware), re direccionamiento a otros sitios web o hasta minado de criptomonedas. Ahora bien, a pesar que no existe sitio web que garantice la seguridad al 100%, podemos contar con planes y medidas de mitigación, como por ejemplo, el uso de antivirus, herramientas de revisión de scripts, plugins del navegador que nos bloqueen la ejecución de estos bloques de código o inclusive, la simple actualización del sistema operativo puede ayudar a contener un poco este tipo de amenaza.

2.1.3 Sitios web en dominios de lista negra

Un punto que juega un papel importante en el entorno de los sitios web es la relación que existe entre una dirección IP y el dominio. El protocolo DNS (Domain Name System), por sus siglas en Inglés, es el encargado de realizar la vinculación entre la dirección web y la dirección IP. Es una labor muy útil, ya que es mucho más fácil recordar el nombre de un sitio web, que una cadena de números separados por punto.

Los dominios, al tener la facilidad de manipular distintos sitios web, pueden verse involucrados por completo con aquellos sitios que presentes fallas de seguridad. Debido a esto es que existen los DNSBL (Domain Name System Blacklists) que según la explicación del sitio web dnsbl.info son "*listas de bloqueo de spam que permiten a un administrador de un sitio web bloquear los mensajes de un*

sistema en específico que tiene historial de envío de spam". (DNSBL, s.f.) pero en la práctica, que un dominio esté marcado en una lista negra no necesariamente se deba a que maneje sitios web vinculados a envío masivo de spam, sino que pueden existir también sitios web que ofrezcan descargas de archivos multimedia que incumplan derechos de autor, por mencionar un caso más.

De esta forma, si un sitio web está realizando prácticas sospechosas como el envío de spam, puede comprometer perfectamente a los demás sitios web que pertenezcan al dominio. Una empresa que posea un sitio web como herramienta y sea catalogado en lista negra de dominio puede desencadenar en pérdida de posicionamiento web, pérdida de imagen y hasta ser visto como una posible amenaza.

2.1.4 Sitios web con enlaces rotos y faltas ortográficas.

Al igual que en la lectura, es gratificante encontrarse con textos que estén redactados de una manera correcta, ya que nos genera seguridad e interés. Lo mismo ocurre en un sitio web, si encontramos textos con faltas ortográficas o gramaticales nos hace dudar de la seriedad del mismo. Existen muchas páginas web que dan sospechas de ser sitios web falsos o de fines poco confiables, lo curioso del caso es que en su gran mayoría todos estos sitios tienen en común las faltas ortográficas.

Otro punto relacionado al anterior, son los enlaces rotos que pueden existir en los sitios web. Estos también restan credibilidad y generan sospecha del sitio al que se está frecuentando. Los motores de búsqueda como Google pueden restar posicionamiento de la página en las búsquedas y catalogar estos sitios como poco serios. Es aquí donde se conjugan ambas características para despertar la malicia

del usuario, quién en su perfil de internauta puede sospechar que una página seria y profesional no puede escatimar en este tipo de detalles.

2.1.5 Sitios web de descargas drive-by.

Luego de haber revisado el comportamiento de los sitios web que ejecutan scripts maliciosos, hay uno en especial que tiene un modo de operar más agresivo y perjudicial. Se trata de los sitios que implementan las descargas “drive-by”, que según el sitio oficial de Kaspersky “*una descarga drive-by hace referencia a una descarga involuntaria de código malicioso a su computadora o dispositivo móvil que deja al usuario a merced de un ciberataque*”. (Kaspersky, s.f.)

Este malware se adapta muy bien en forma de algunas líneas de código, para poder pasar inadvertido por aplicaciones de defensa en seguridad, basta con abrir el enlace web para que se dispare la ejecución por parte del código malicioso. El mismo ejecutará las acciones de descarga (muchas veces de sitios web alternos), sin autorización del usuario para alojar software que podría parecer benigno, pero que en el fondo contiene malware. Es así como los ciberdelincuentes toman control de nuestras terminales, ya sean teléfonos o computadoras para ejecutar el ataque.

Por eso siempre es importante mantener los equipos con los sistemas operativos actualizados, también un software de protección en toda la red de la empresa y por último, desconfiar de correos electrónicos o abrir enlaces de sitios web desconocidos.

2.2 Plataforma Android

Los inicios de Android se empiezan a gestar desde el año 2003, cuando la compañía homónima Android Inc, comienza a dar los primeros pasos en la creación del cuál sería el Sistema Operativo (S.O) más usado en la actualidad (El Universal, 2018). Este versátil S.O está basado en arquitectura Linux, la cual se compone de algunas capas que se exponen a continuación:

- **Aplicaciones o Apps del sistema**. Son las aplicaciones que conocemos al utilizar el S.O del celular. Se caracterizan por realizar las operaciones básicas del teléfono como envío de mensajes de texto, captura de fotografías (en caso de la cámara), y cualquier otra aplicación que esté disponible en la tienda “Play store” para descarga ya sea de pago o gratuita.
- **Framework API de Java**. Son todas las funciones del S.O Android mediante una API escrita en Java. Estas funciones están a la disposición de los desarrolladores para poder implementarlas en la creación de aplicaciones. Entre algunos ejemplos se tiene un administrador de notificaciones, que permite a las aplicaciones mostrar alertas en la barra de estado. Proveedores de contenido, permite a las aplicaciones acceder datos de otras, como por ejemplo registro de llamadas, mensajes, contactos.
- **Bibliotecas nativas de C y C++**. Además de las aplicaciones del API de Java, muchos componentes del S.O Android se basa en bibliotecas nativas escritas en código C/C++. Por ejemplo, si alguna aplicación que se esté desarrollando necesite utilizar gráficos en 2D y 3D, se puede utilizar la aplicación del API del framework de Java llamada “JavaOpenGL” que a

su vez se comunica con “OpenGL ES” perteneciente a esta capa de bibliotecas nativas.

- **Android Runtime (ART).** Tiempo de ejecución de Android o ART (por sus siglas en Inglés) es el responsable de manejar el tiempo de ejecución de las aplicaciones. Su predecesor llamado “Dalvik” fue el que realizaba esta misma función desde que inició el proyecto de este S.O. Entre sus principales funciones están; la compilación AOT y JIT, recolección de elementos no usados (GC), mejor compatibilidad con la depuración y la capacidad de establecer puntos de control.
- **Hardware Abstraction Layer**. La capa de abstracción de hardware es la encargada de ofrecer una interfaz de comunicación con la capa de API del framework de nivel más alto. Su trabajo se basa en brindar interfaces estándares a las peticiones del API Framework, esto se logra con ayuda del sistema al cargar los módulos de la biblioteca que se necesitan de forma específica.
- **Kernel de Linux**. La última capa y el núcleo del sistema es el Kernel de Linux, mismo que implementa el uso del ART, administración de recursos como la memoria y subprocesos. (Android, 2018)

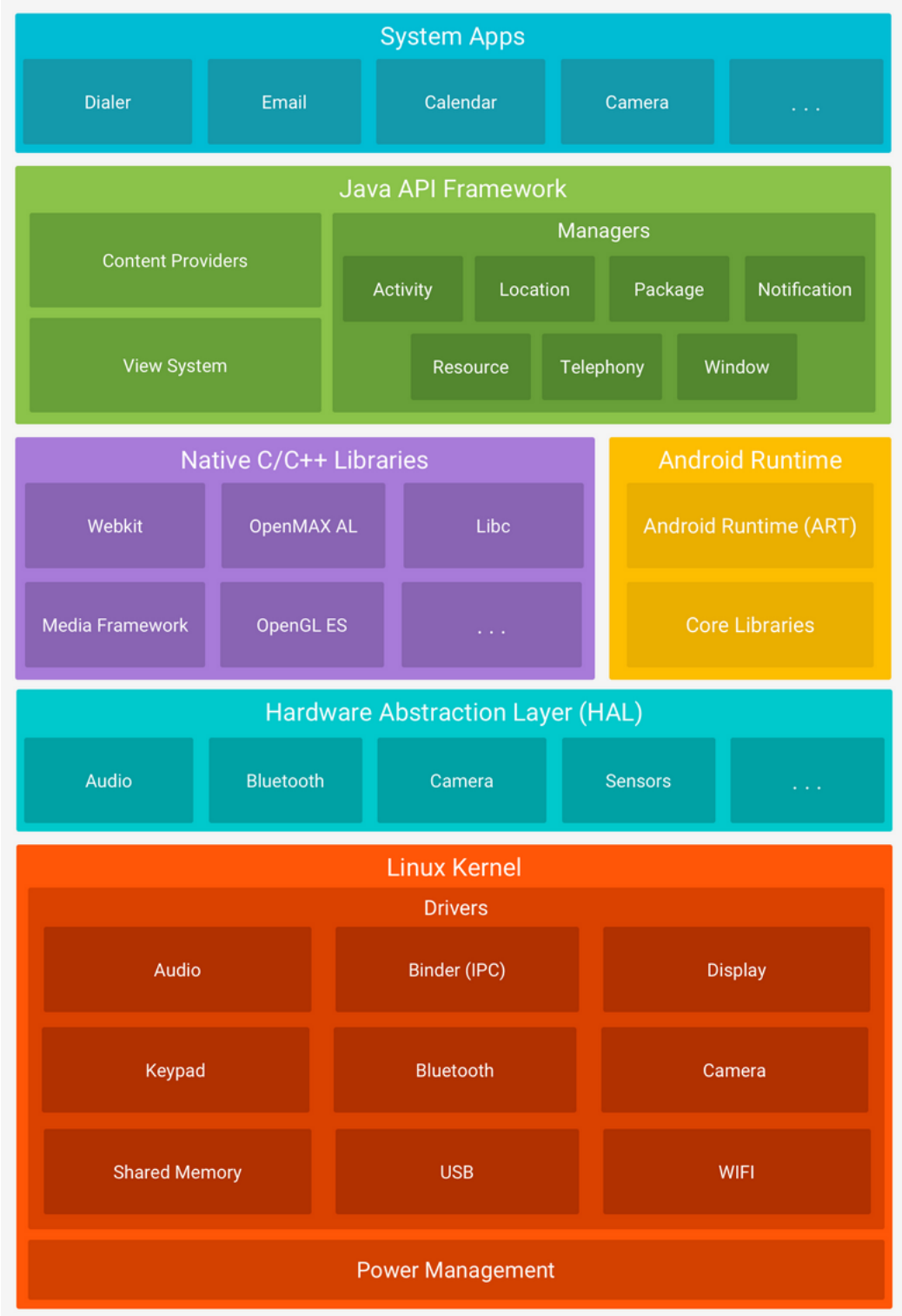


Imagen 2 - Arquitectura Android (Android, 2018)

La comunidad de desarrolladores Android cada día gana más adeptos, y no es para menos, si la cantidad de aplicaciones Android superan los 3 millones en PlayStore. Las mismas tienen una clasificación que vale la pena mencionar:

Aplicaciones Nativas. Se entiende por aplicación nativa a todas aquellas que han sido creadas en el lenguaje base, en este caso Java. Para entornos como iOS se utilizaría Objetive C y por último .NET para Windows Phone.

Aplicaciones Híbridas. En este caso se clasifican como aplicaciones Híbridas a las que implementan HTML5, Javascript y CSS, son desplegadas dentro de contenedores nativos como Cordova y desde donde acceden a las funciones del sistema operativo en el cual se hospedan.

Aplicaciones Generadas. Se les da el nombre de aplicaciones generadas a las que utilizan herramientas de terceros para acelerar o facilitar el desarrollo de las mismas. Herramientas como Xamarin o Genexus ofrecen un entorno de creación e incorporación con diferentes lenguajes de programación para finalmente generar la App en el lenguaje de la plataforma destino. (InnovaAge, s.f.)

2.2.1 Android SDK

Del Inglés SDK, Software Development Kit o Kit de desarrollo de software, es un conjunto de funciones o recursos que cierto proveedor pone a disposición de los programadores (por lo general son los usuarios técnicos que lo utilizan) para ser utilizado en la creación de nuevo código, programas, soluciones de software.

Ahora bien, según el sitio web techopedia (Techopedia, 2019), el SDK de Android incluye:

- Emulador

- Debugger
- Documentación referente a la interface de programación de aplicación
- Ejemplos de código fuente
- Librerías requeridas.

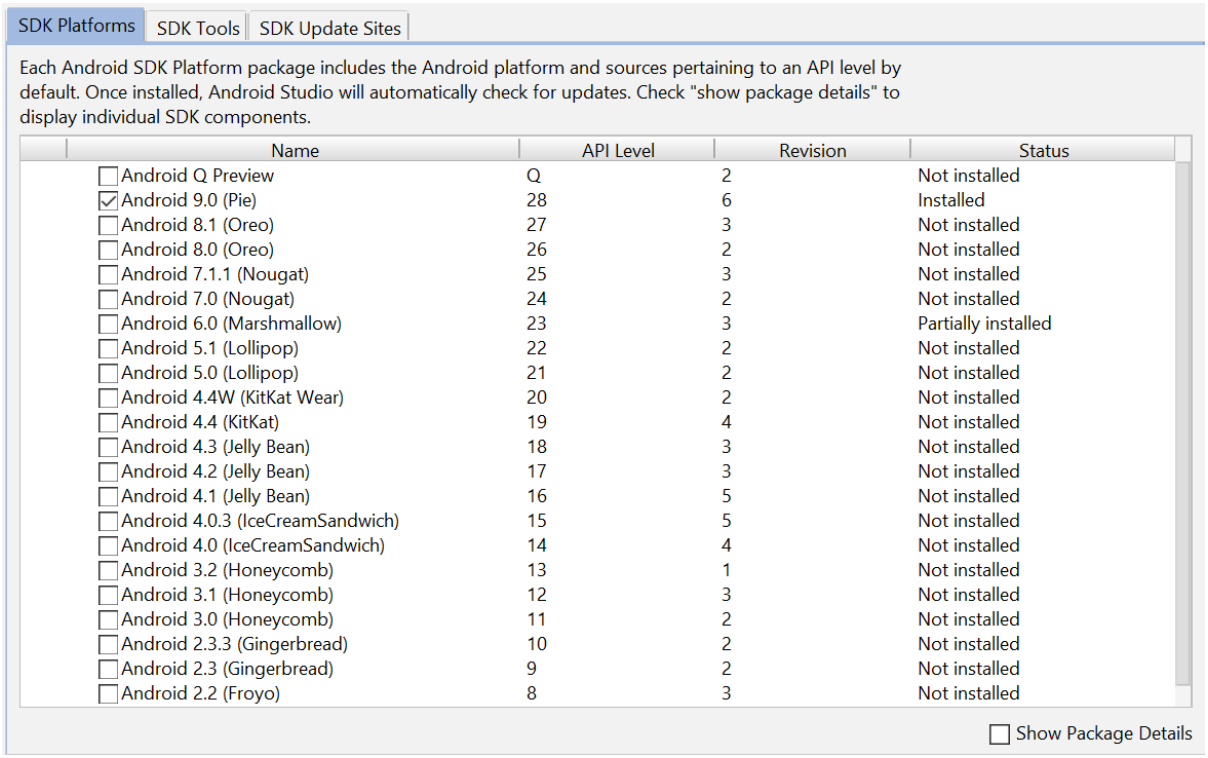


Imagen 3 - Ejemplo de interfaz SDK Android. Fuente: Elaboración propia

Para el proyecto en curso, se utiliza el SDK de Android para el desarrollo del prototipo funcional, aunado a esto el IDE (Integrated Development Environment) Android Studio para el desarrollo del aplicativo.

Cabe mencionar también la utilización de la funcionalidad AVD (Android Virtual Device), que permite crear diferentes interfaces emuladas de acuerdo con las necesidades de las distintas versiones del Sistema Operativo Android.

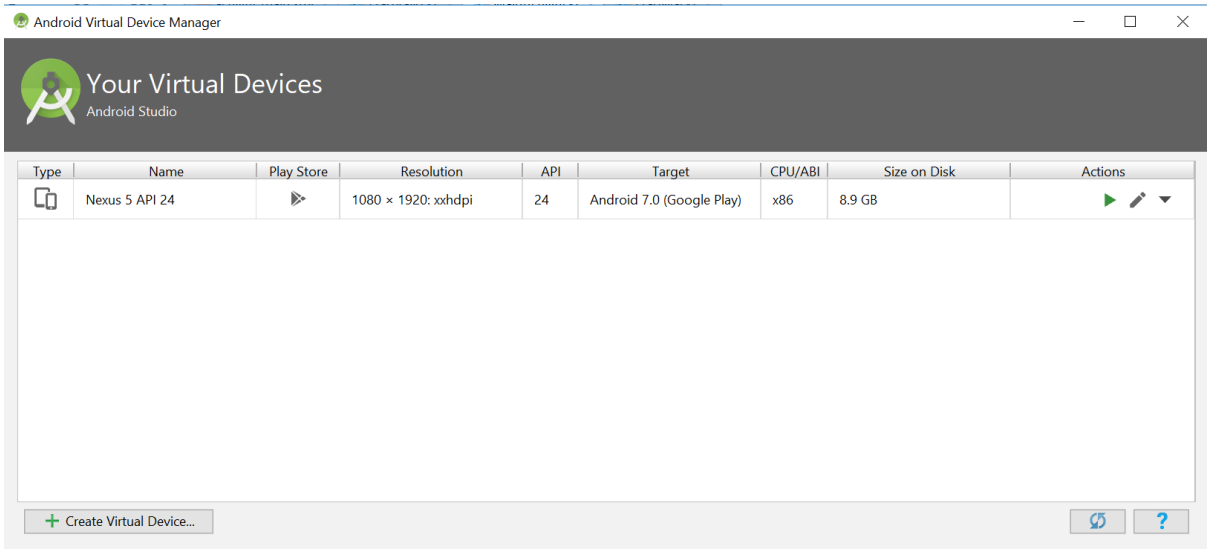


Imagen 4 - Agente virtual de dispositivos Android. Fuente: Elaboración propia

Una ventaja del IDE es ofrecer entre las opciones de ejecución de código fuente el sistema operativo Android para ser utilizado en aquellos dispositivos conectados por cable USB. La siguiente imagen resume muy bien la idea.

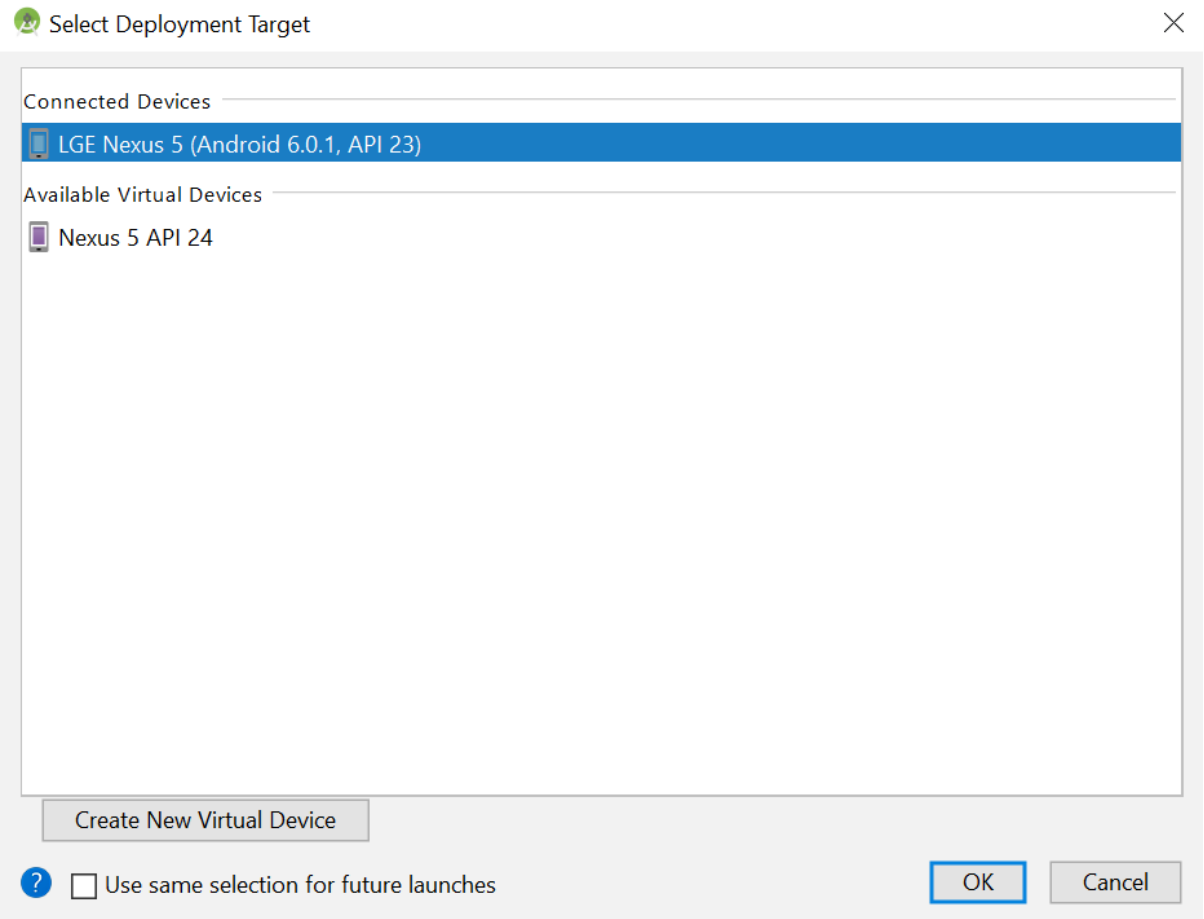


Imagen 5 - Dispositivo destino de ejecución. Fuente: Elaboración propia

2.2.2 Empaquetado Aplicación Android

Todas las aplicaciones que sean desarrolladas para la plataforma Android, comparten el mismo proceso de empaquetado o liberación del producto. Para dicho producto final, se genera un archivo con la extensión .apk (Android Application Package) que contiene todos los recursos necesarios para su correcto funcionamiento en las terminales donde se instale.

En la publicación realizada en el sitio de Github, David Griffiths explica de manera muy sencilla los pasos en como las aplicaciones Android son construidas desde la programación a la liberación. A continuación, se detalla (Griffiths, 2017):

- Compilación Java. Es necesario poder traducir el código java de la aplicación móvil al de un ensamblado java. Esto se logra con ayuda de un compilador y así generar archivos de clase.
- Conversion a Dalvik Bytecodes. Android cuenta con su propio formato de código de bytes llamado Dalvik. Para este paso se necesitan los archivos de clase del punto anterior junto con cualquier archivo de Java, para ser convertidos a formato Dalvik (dex).
- Colocar el archivo classes.dex y los archivos de recurso en un archivo de tipo paquete. Con ayuda del AAPT (herramienta Android de empaquetado de activos), se toman los archivos .dex del punto anterior y cualquier otro archivo de recurso como imágenes, sonidos, plantillas para ser comprimidas y generar así el archivo “apk”.
- Firmar el archivo .apk
- El archivo apk es transferido e instalado en el dispositivo.

El siguiente diagrama resume de una mejor manera la idea

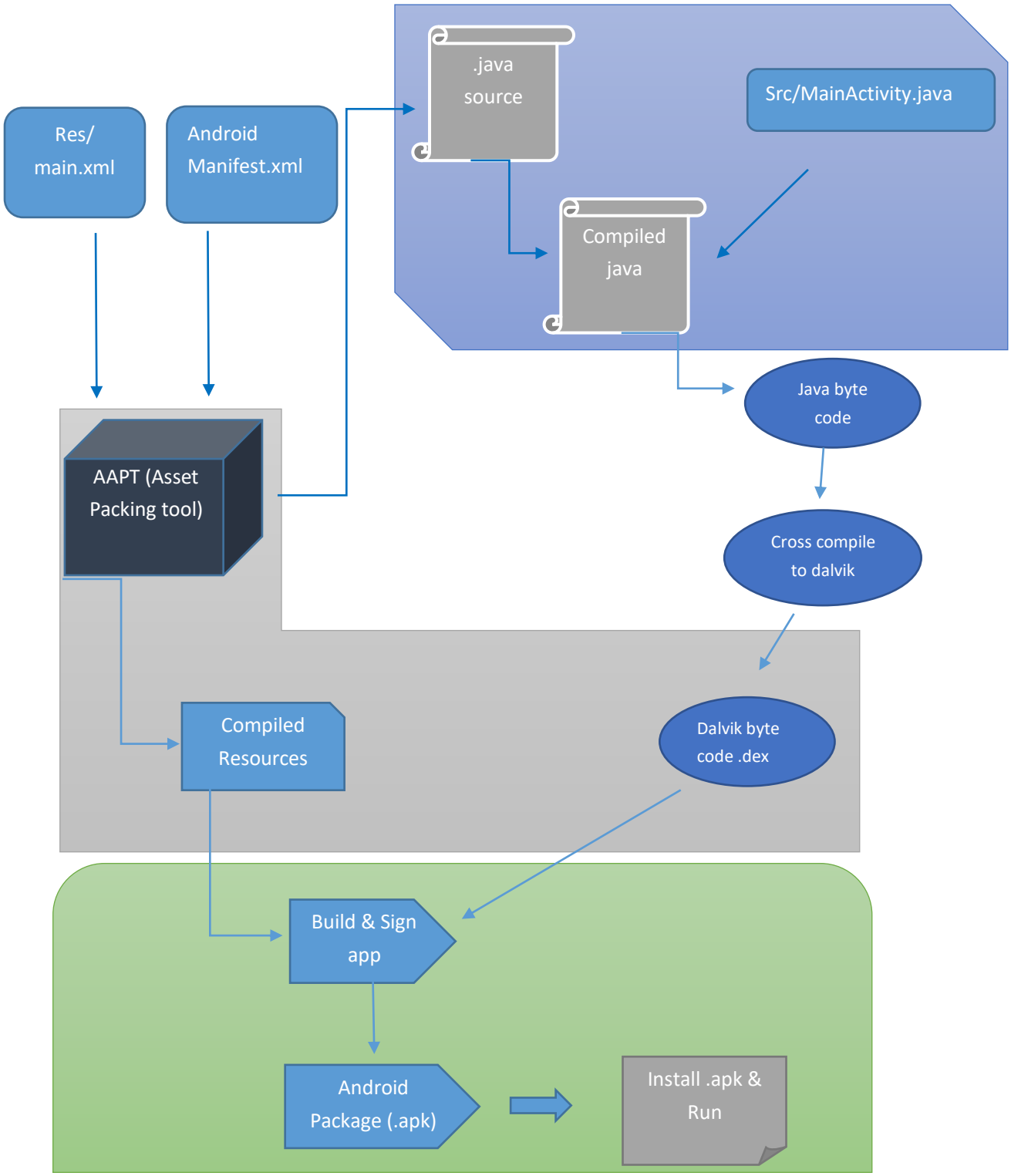


Gráfico 1 - Empaquetado Android (Garud, 2017)

2.3 Servicios Web

En el entorno tecnológico y especialmente de programación, las integraciones son un proceso muy útil y necesario para la comunicación entre 2 o más sistemas. Los servicios web han venido como una solución a la intercomunicación de los diferentes sistemas. Según W3C (World Wide Web Consortium) define un servicio web "*como un sistema de software designado para dar soporte a la interacción de máquina a máquina interoperativa a través de una red.*" (IBM, 2014)

Entre las variantes a la hora de escoger un servicio web se tienen dos grandes aristas; **SOAP**, que de sus siglas (Simple Object Access Protocol) es un protocolo dedicado a intercambiar mensajes vía HTTP, se utiliza XML para ordenar los mensajes que se van a enviar y recibir. Luego **REST** (Representational State Transfer) su arquitectura se amolda más a sistemas distribuidos como es la web, con una colección de principios se acopla a las arquitecturas de red. La elección entre uno y el otro es tema de debate por las compañías, se recomienda poner sobre la mesa cuáles son las necesidades de la empresa y revisar lo que ofrece cada una para tomar la mejor decisión.

2.4 Lenguaje de programación Kotlin

Desde los inicios de la existencia del sistema operativo Android, se ha visto un fuerte vínculo con el lenguaje de programación Java, que cuenta con adeptos en la comunidad de desarrolladores.

Sin embargo, con el paso del tiempo y la automatización en procesos, ha surgido un nuevo lenguaje de programación que se amolda muy bien por su versatilidad e interoperabilidad con Java, este lenguaje llamado Kotlin permite

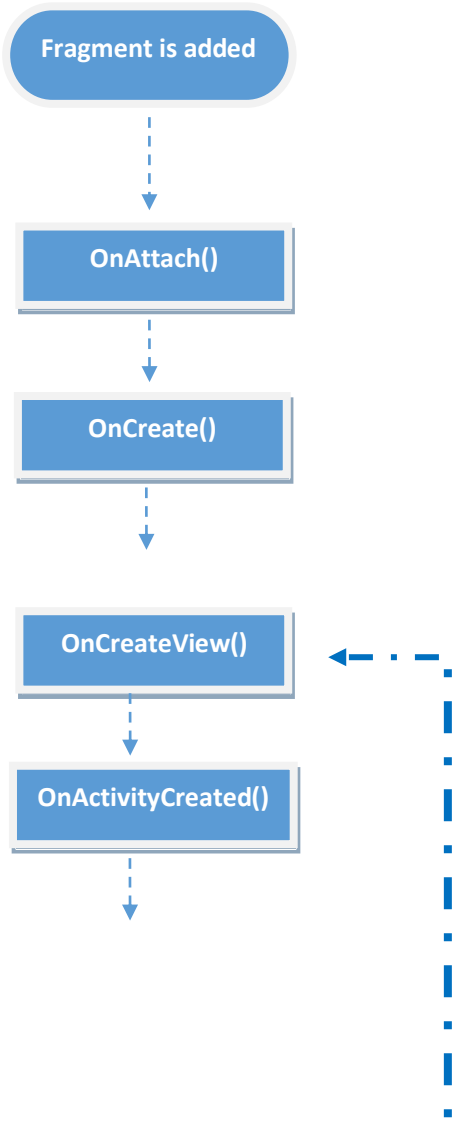
proyectos de desarrollo con código mixto (Java y Kotlin). En la página oficial se detalla además ciertos casos de uso que vale la pena mencionar; el primero, Kotlin es ideal para desarrollos basados en la máquina virtual de Java, segundo, posee gran aceptación por parte de desarrolladores y, por último, aumenta la productividad a la hora de desarrollo, se hace más con menos código. (Kotlin, 2019)

Cada aplicación Android posee componentes que se pueden ver como bloques que interactúan tanto con el sistema como con el usuario. Los principales componentes según la guía de documentación Android (Android, 2018) son:

- **Actividades**. Una actividad es una visualización en pantalla que muestra al usuario una porción de funcionalidad. Se puede decir a modo de ejemplo que la interfaz para redactar un mensaje SMS es una actividad. Luego, otra actividad es una consulta en pantalla que despliega la lista de los contactos del teléfono. Que si bien, toda la funcionalidad parece venir de una misma aplicación, en el fondo son muchas actividades trabajando en conjunto que dan esa noción.
- **Servicios**. Los servicios a diferencia de las actividades no cuentan con interfaz al usuario. Son como su palabra lo indica “servicios” que se ejecutan por lo general en segundo plano. Como por ejemplo la descarga de un archivo mientras se navega por Internet.
- **Proveedores de contenidos.** Es un mancomunado compartido de datos. Que bien las aplicaciones pueden acceder con los permisos adecuados a dichos datos. Un ejemplo es la aplicación Bloc de Notas, que utiliza el proveedor de contenido para crear y editar notas.
- **Receptores de mensajes**. El sistema Android envía mensajes al ocurrir ciertos eventos, a lo cual el receptor de mensajes responde a

los anuncios de estos mensajes. El sistema puede enviar un mensaje cuando la batería tiene poca carga, o bien cuando se enciende la pantalla. El receptor de mensajes tampoco cuenta con una interfaz, pero si pueden ser canalizados a la barra de estado para alerta del usuario.

- **Fragmentos**. Son pequeños módulos que heredan las funciones de una actividad. La ventaja en este caso es que se pueden combinar varios fragmentos en una sola actividad y así crear una experiencia de multi-función al usuario. Tienen ciclos de vida propios y para efectos de la investigación en curso han sido muy útiles para crear el prototipo funcional. Al ser de gran utilidad para el desarrollo del prototipo, se explica un poco más el ciclo de vida del fragmento.



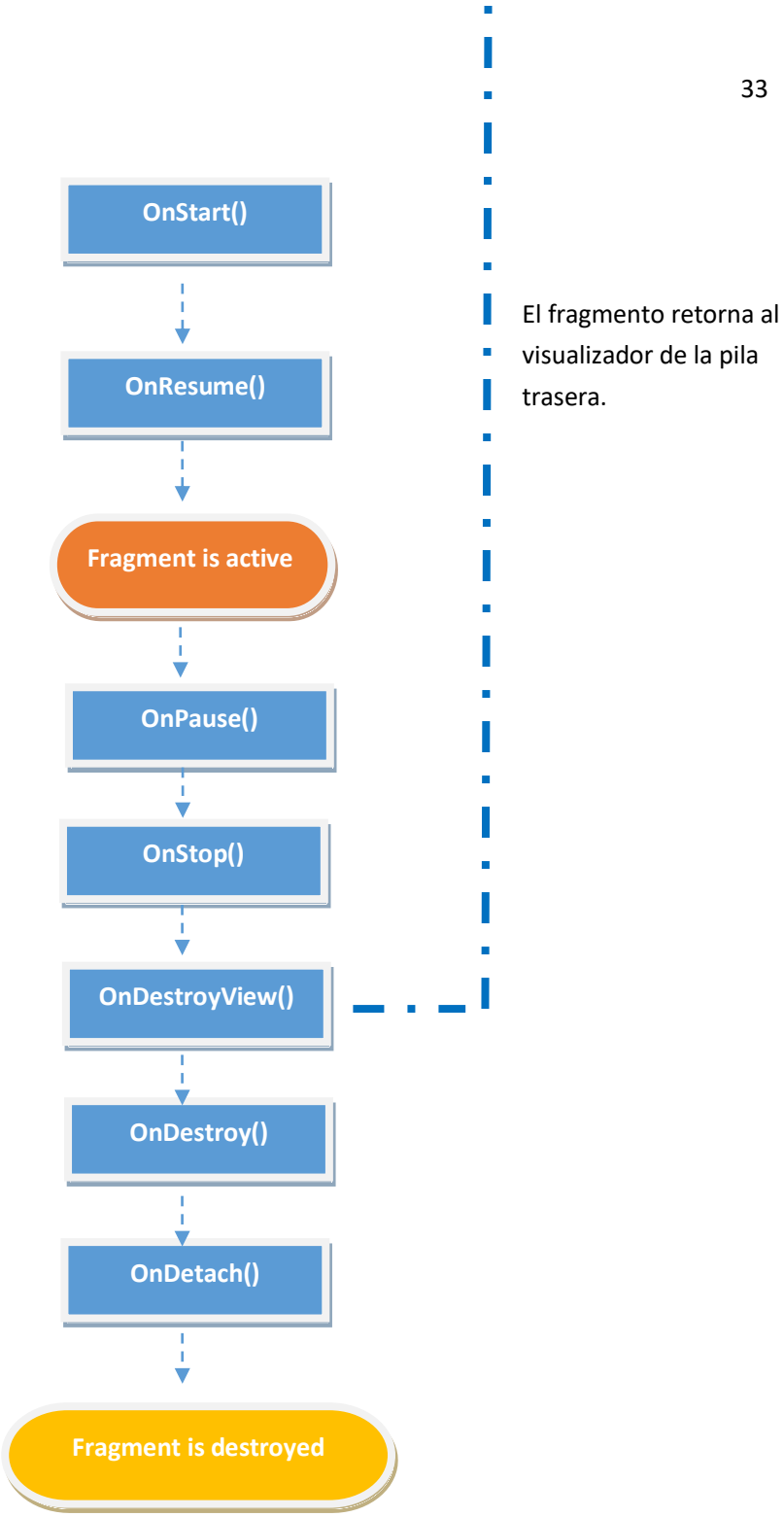


Gráfico 2- Ciclo de vida de un Fragmento (Android, 2018)

Cada proceso en el recuadro es un evento de la aplicación, de los cuales hay 3 que se caracterizan por ser los más utilizados; "**onCreate**", el sistema llama a este método cuando se crea el fragmento, se inicializan componentes que serán utilizados a lo largo del fragmento, "**onCreateView**" este método es llamado por el

sistema para diseñar la interfaz de usuario, y "**onDetach**", el sistema llama este método cuando el fragmento será desvinculado de la vista del usuario en la interfaz, por lo general se terminan procesos o se reestablecen valores en este punto.

2.5 Reconocimiento óptico de caracteres (OCR)

El reconocimiento óptico de caracteres u OCR (por sus siglas en Inglés) es la capacidad que tiene el software de distinguir mediante algoritmos los patrones correspondientes al alfabeto en una impresión y así convertirlo en texto legible y editable de forma digital. El sitio web **definicion.com**, lo definen como "*La noción se utiliza en la informática para nombrar a un procedimiento que permite digitalizar un texto a través de un escáner*." (Definicion, 2019)

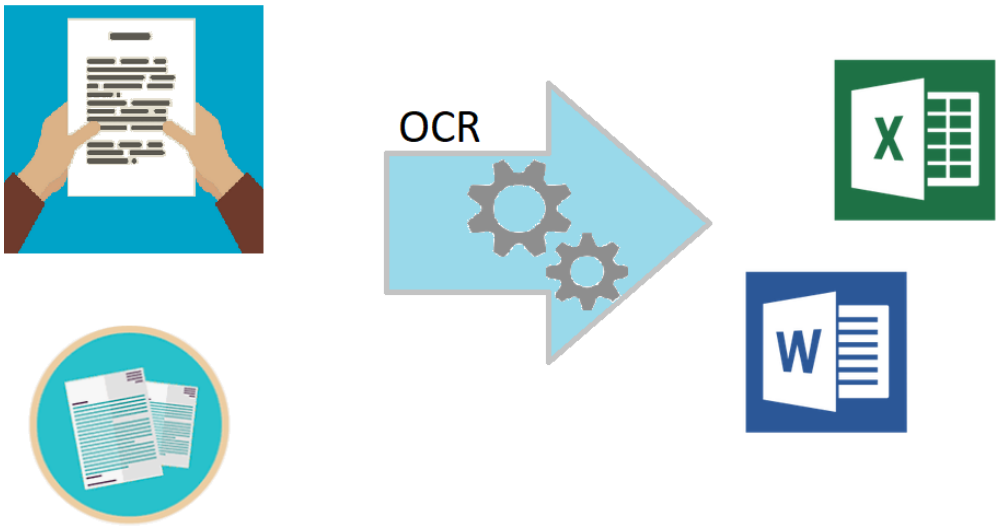


Imagen 6 - Proceso OCR. Fuente: Elaboración propia

Al final lo que se necesita es tener una imagen base, que sirve de fuente para aplicar la función de reconocimiento. Para efectos del proyecto en curso, se

pretende utilizar la cámara de un teléfono inteligente como medio de captura de imagen, y así obtener una dirección web URL.

Es importante destacar también la disposición de poder utilizar el API de Google, que está a la mano de los desarrolladores mediante las herramientas del SDK, que con las librerías necesarias se puede implementar el reconocimiento de texto de una forma programada. Para una mejor referencia, la dependencia es la que se muestra en la siguiente imagen.

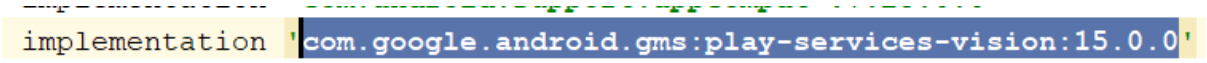


Imagen 7 - Dependencia del API de Google. Fuente: Elaboración propia

2.6 API de VirusTotal

Gracias a la existencia y disponibilidad de las interfaces de programación de aplicaciones (API), se brinda a los desarrolladores la oportunidad de consumir utilizar los recursos que el dueño del API así lo diseñe.

VirusTotal, un servicio que se consulta vía web, es de origen español y creado por Hispasec Sistemas (luego adquirida por Google). Su función principal, como lo muestra en su sitio web es "*analiza archivos y URLs sospechosas facilitando la rápida detección de virus, gusanos, troyanos y todo tipo de malware.*" (VirusTotal, 2019).

Además, cuenta también con un API, que está a disposición para ser utilizado integrándolo en distintas aplicaciones cliente. Entre sus servicios para la versión 2.0 se tiene:

- Envío y escaneo de archivos
- Re escaneo de archivos previamente subidos
- Obtención de reportes de los archivos analizados
- Envío y escaneo de direcciones web URLs
- Obtención de reportes de URLs escaneadas
- Obtención de reportes de direcciones IP
- Obtención de reportes de dominio
- Realizar comentarios sobre IPs y direcciones URL

El sitio web, al que se puede ingresar por medio de la dirección www.virustotal.com muestra una interfaz muy simple pero a la vez útil para los usuarios que analicen malware, o para todo aquel que tenga duda con la procedencia de alguna dirección web.

Imagen 8 – Sitio Web virus total. Fuente: Elaboración propia

Una de sus grandes ventajas, es que cuenta con una base de consulta de 66 antivirus que ayudan a detectar irregularidades o amenazas. Entre los más conocidos se tienen: Kaspersky, Malwarebytes, Sophos, Fortinet, ESET, BitDefender, Avira, entre otros. (VirusTotal, 2019) Por otro lado, cuenta también con una comunidad de usuarios dedicados al estudio de malware que por medio de comentarios en el sitio realizan aportes y experiencias que han tenido con los archivos analizados o sitios web.

El API se encuentra a la disposición mediante una dirección electrónica a la cual se envían o reciben las peticiones, esto por ser un servicio web. La dirección es **https://www.virustotal.com/vtapi/v2** donde, el link anterior es la dirección base y para utilizar los diferentes servicios solo se le añaden los sufijos. Por ejemplo, para escaneo de archivos se utiliza el sufijo "../file/scan", para obtener el reporte del archivo escaneado "../file/report". Por otro lado, para poder escanear una URL y saber si es sospechosa o no, se debería utilizar la siguiente dirección con su sufijo correspondiente "https://www.virustotal.com/vtapi/v2/url/scan". La siguiente imagen ejemplifica una petición hacia el servidor (en el lenguaje de programación Python) de cómo analizar una dirección Url, que como vemos, no demanda una gran cantidad de líneas de código.

```
import requests
params = {'apikey': '-YOUR API KEY HERE-', 'url':'http://www.ejemplo.com'}
response = requests.post('https://www.virustotal.com/vtapi/v2/url/scan', data=params)
json_response = response.json()
```

Imagen 9 - Ejemplo petición escaneo Url. Fuente: (VirusTotal, 2019)

Capítulo 3. Marco Metodológico

3.1 Tipo de Investigación

Siguiendo la línea de la investigación en curso, el estudio se centra en el uso de la metodología de investigación aplicada, puesto que no se genera conocimiento per se, sino más bien se basa en el existente de la investigación básica. El aprovechamiento del conocimiento en el área de desarrollo de software por parte del investigador, y el reconocimiento en la necesidad de un sector de la población que utiliza Internet para navegar por distintos sitios web, hacen que se aprovechen de las diferentes piezas para crear una solución móvil y así justificar la escogencia de este tipo de investigación. El siguiente diagrama tomado del sitio douc.cl ejemplifica de forma clara la idea.

Imagen 10 - Investigación Aplicada. Fuente (UC, 2019)

3.2 Alcance investigativo

Debido al tipo de investigación que se realiza, y el acercamiento para poder conocer el comportamiento de un grupo de personas que son usuarios de Internet, tanto para realizar transacciones, revisar correo electrónico, comercio electrónico, revisión de estados de cuenta bancarias, entre otros, es que se define el alcance de la investigación de tipo descriptivo, éste, como lo explica Danhke, 1989 (citado por Hernández, Fernández y Baptista, 2006) “Los estudios descriptivos buscan

especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis" (Hernández, Fernández y Baptista 2006)

3.3 Enfoque

Con base al objetivo general y los objetivos específicos de este proyecto, involucran un trabajo por realizar al estudio de un grupo de personas, que generará así una base e insumos para poder dar forma al prototipo funcional de la aplicación móvil, el enfoque que se adapta más es la investigación cuantitativa, que tiene como base el paradigma positivista. Este paradigma posee algunas características que como lo menciona Pedro Zayas vale la pena mencionar, "…*la formulación de hipótesis, su verificación y la predicción a partir de las mismas, la sobrevaloración del experimento, el empleo de métodos cuantitativos y de técnicas estadísticas para el procesamiento de la información, así como niega o trata de eliminar el papel de la subjetividad del investigador*…" (Agüero, 2010). De esta manera es que nace una hipótesis, que indica que gran parte de los usuarios de sitios web no revisa los links o incluso desconoce que existen herramientas para realizar esta labor.

Volviendo a la idea principal del enfoque cuantitativo, es hacer uso de alguna técnica para procesar información, para luego analizarla y exponer resultados, al dar así un criterio más sólido ante la hipótesis planteada.

3.4 Diseño

De acuerdo con el estudio cuantitativo que se hace mención en el enfoque, es necesario en este diseño definir las variables, que ayudan a entender la información que se desea recolectar.

3.4.1 Variable 1:

Las tendencias de los usuarios ante el uso de dispositivos para navegar en Internet.

Definición conceptual:

La elección del dispositivo de navegación web por parte de los usuarios al depender de las transacciones que realicen.

Definición instrumental:

De la encuesta aplicada, se considera el ítem número 5.

Definición operacional:

Si las respuestas seleccionadas corresponden a “Computadora”, los usuarios prefieren el uso de una laptop o equipo de escritorio para realizar transacciones. Si por el contrario las respuestas pertenecen al rubro “Celular”, los usuarios son más propensos a utilizar más el teléfono para navegar y realizar transacciones.

3.4.2 Variable 2:

La importancia que los usuarios de Internet sepan de las amenazas que poseen ciertos sitios web.

Definición conceptual:

Mecanismo que permita a los usuarios de Internet tener un criterio de discernimiento ante un sitio web, basado en si muestra algún tipo de amenaza.

Definición instrumental:

De la encuesta aplicada, se consideran los ítemes 9 y 12.

Definición operacional:

Con límites a las preguntas cerradas Sí o No, aquellos que respondan de forma afirmativa poseen los conocimientos o tienen la voluntad de aplicar los mismos ante una eventual revisión electrónica de un sitio web. De lo contrario, si responden de forma negativa, se tiene una falencia que denota ignorancia o falta de cuidado ante la navegación web.

3.5 Población y muestreo

La población se conforma por personas usuarios de Internet.

	Valor absoluto	Valor relativo
Población	30	100%
Muestra	27	90%

3.6 Instrumento recolección de datos

La presente investigación será realizada por medio del enfoque cuantitativo, y de forma intrínseca se abarca el paradigma positivista. Debido a esto se procede a realizar el análisis numérico de los datos.

Se aplica un instrumento para la recolección de datos, la encuesta, que cuenta con 14 preguntas, que en su mayoría son preguntas cerradas, en donde el

encuestado debe responder: Sí o No. Además, se toman datos personales como edad, grado académico, entre otros. Este instrumento se utiliza para conocer el comportamiento de los usuarios respecto de la navegación segura y manipulación de las direcciones web.

3.7 Técnicas de análisis de información

Con base a la información recolectada en el punto anterior, se representa por medio de una espina de Ishikawa las causas que generan el problema. Esta herramienta es muy útil para explicar en profundidad el entendimiento de ciertas causas generadoras de un problema.

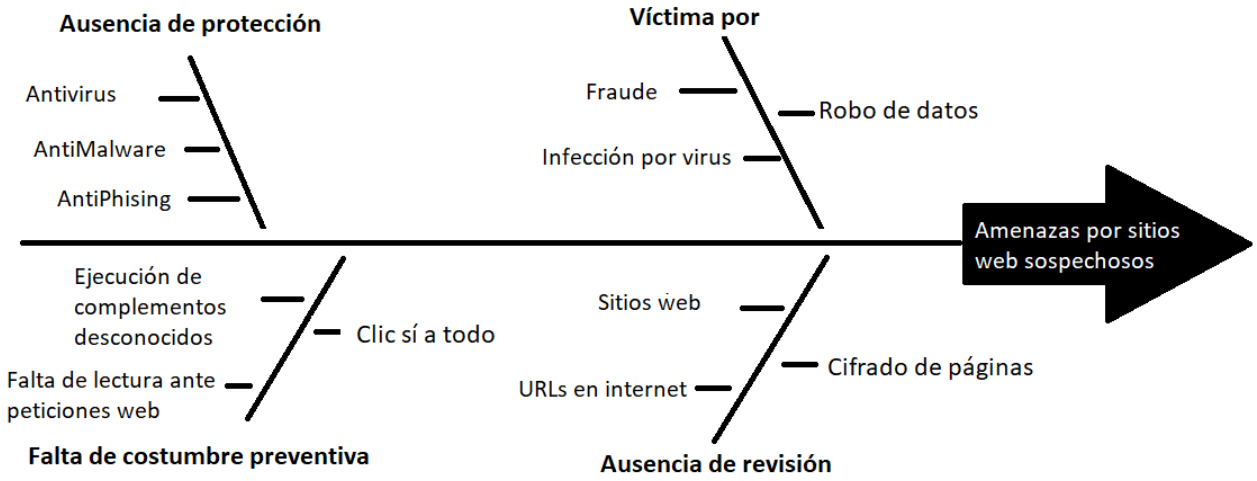


Imagen 11 - Espina de Ishikawa. Fuente: Elaboración propia

Se observa en el diagrama causa y efecto, las variables del comportamiento presentado por el usuario, donde, la ausencia de revisión al navegar, falta de costumbre preventiva, haber sido víctima de delincuentes informáticos y ausencia de protección en sus equipos es que se desencadenan las amenazas y posibles ataques a sus equipos desde sitios web.

Capítulo 4. Análisis del Diagnóstico

Para efectos del capítulo, se procede a realizar un análisis cuantitativo del instrumento utilizado. En este caso la encuesta- a la muestra de 27 usuarios de Internet, y, por ende, de navegadores web. Dicho instrumento se aplica con el fin de conocer el comportamiento de los usuarios ante la revisión de la seguridad al visitar un sitio web.

A continuación, se analizan las preguntas más representativas de la encuesta aplicada:

Pregunta número 3, ¿Nivel académico?

Respuesta	Porcentaje	Cantidad
Primaria completa	0.00%	0
Secundaria completa	0.00%	0
Secundaria incompleta	3.70%	1
Universitaria incompleta	37.04%	10
Universitaria completa	59.26%	16
	Total de respuestas	27

Cuadro 1 - Pregunta # 3. Fuente: Elaboración propia

De los entrevistados, la mayoría corresponde al 59.3%, lo cual pronostica que muy posiblemente la población encuestada cuente con buenos conocimientos en la navegación web. Aun así, el porcentaje de aquellos que no terminaron estudios universitarios es del 37%. Por último, solamente un 3.7% no cuenta con la secundaria completa. Las casillas de primaria completa y secundaria completa no fueron marcadas por ninguna persona.

Pregunta número 4, ¿En qué dispositivo suele navegar más en internet?

Respuesta	Porcentaje	Cantidad
Computadora	22.22%	6
Tablet	0.00%	0
Teléfono Inteligente	77.78%	21
	Total de respuestas	27

Cuadro 2 - Pregunta # 4. Fuente: Elaboración Propia

La casilla referente al uso de Tablet no fue seleccionada por ningún encuestado, por otro lado, se observa que la mayoría de usuarios utiliza el teléfono inteligente (Smartphone) para navegar por Internet, siendo representado por el 77.8%. Mientras que un 22.2% indicó que navega utilizando la computadora como dispositivo más frecuente.

Pregunta número 5, ¿Para realizar transacciones web delicadas o seguras, que dispositivo utiliza más?

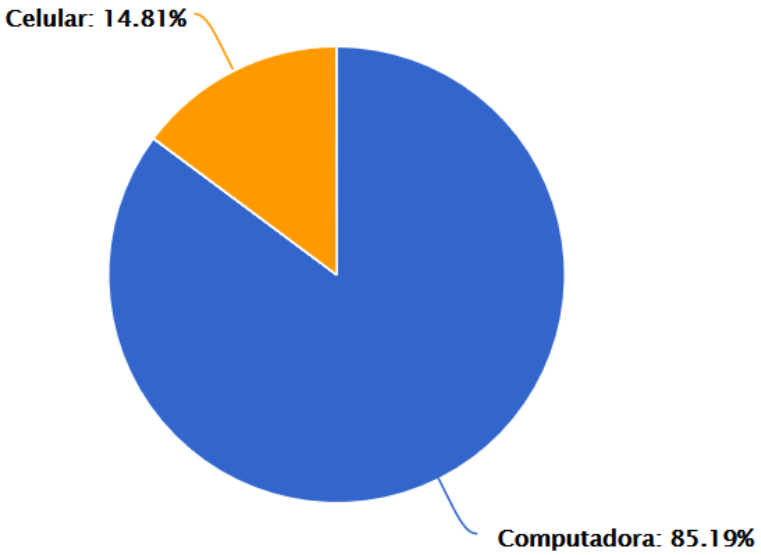
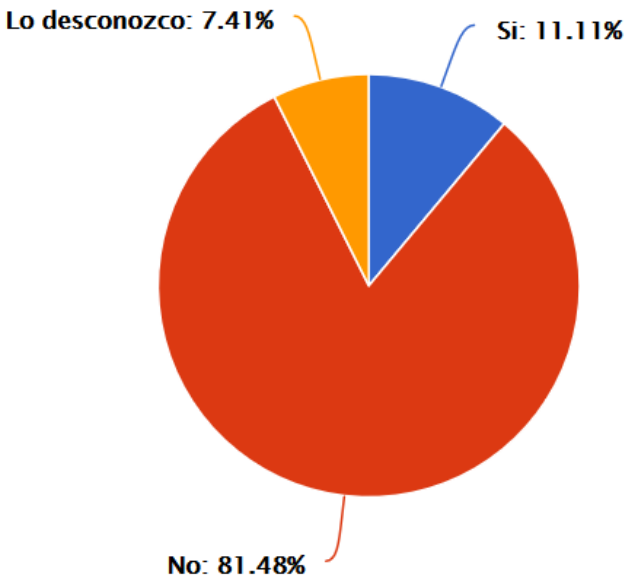


Gráfico 3 - Pregunta # 5. Fuente: Elaboración Propia

La casilla referente al uso de Tablet, no tuvo ninguna marca, mientras que 23 usuarios indicaron que prefieren utilizar la computadora como medio o dispositivo más seguro al realizar transacciones delicadas o de mayor cuidado. Por último, solamente 4 personas indicaron que también utilizan el Smartphone para realizar transacciones delicadas.

Pregunta número 6, ¿Ha sido víctima de algún fraude por el uso de internet en el último año?



Cuadro 3 - Pregunta # 6. Fuente: Elaboración Propia

La casilla correspondiente a que no han sido víctimas de fraude por el uso de Internet comprende la mayor de las respuestas con un 81.4%, mientras que un 18.6% se dividen que sí, o que lo desconocen. Siendo un porcentaje pequeño, pero en relación con la muestra son 5 de cada 27 usuarios.

Pregunta número 7, ¿Ha sido víctima de infección de virus en su equipo de navegación web en el último año?

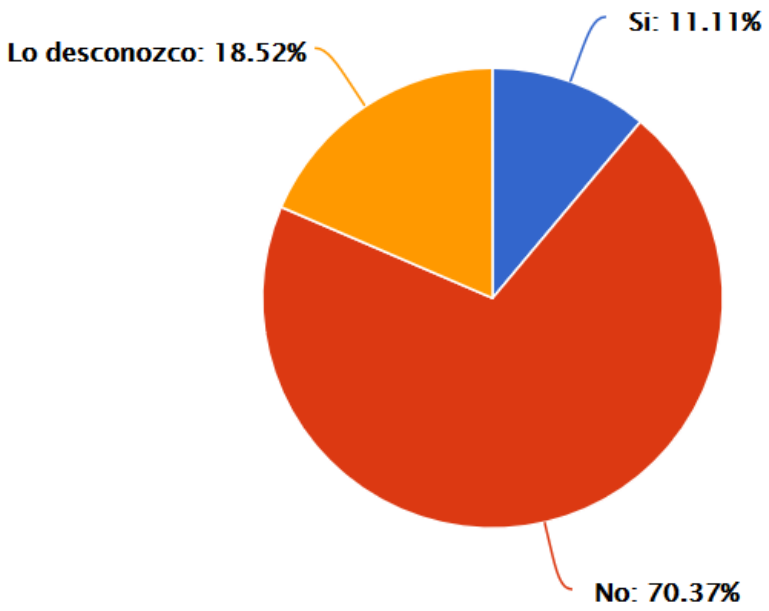


Gráfico 4 - Pregunta # 7. Fuente: Elaboración Propia

La casilla correspondiente a que no han sido víctimas de virus o malware en los equipos de navegación comprenden un 70.3%. Luego un 18.5% no sabe si han sido infectados o corren algún riesgo de infección y por último un 11.1% indican que sí han corrido algún riesgo.

Pregunta número 8, ¿Qué tipo de protección virtual (anti malware, antivirus, etc) utiliza para sus equipos?

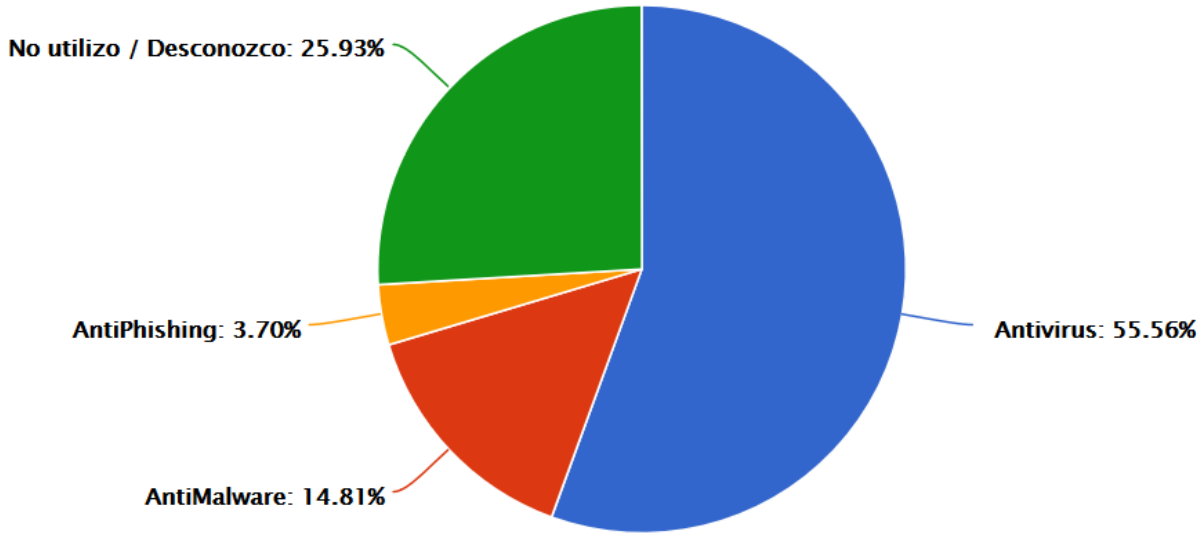


Gráfico 5 - Pregunta # 8. Fuente: Elaboración Propia

Para esta pregunta vemos que un 55.5% utiliza el antivirus como forma de protección virtual, luego la segunda gran área nos muestra que un 25.9% desconoce o no utiliza ningún tipo de protección. Por último, las 2 áreas restantes muestran que un 14.8% utiliza AntiMalware y un 3.7% AntiPhishing.

Pregunta número 9, ¿Conoce de herramientas en línea que permitan identificar si un sitio web es sospechoso o confiable?

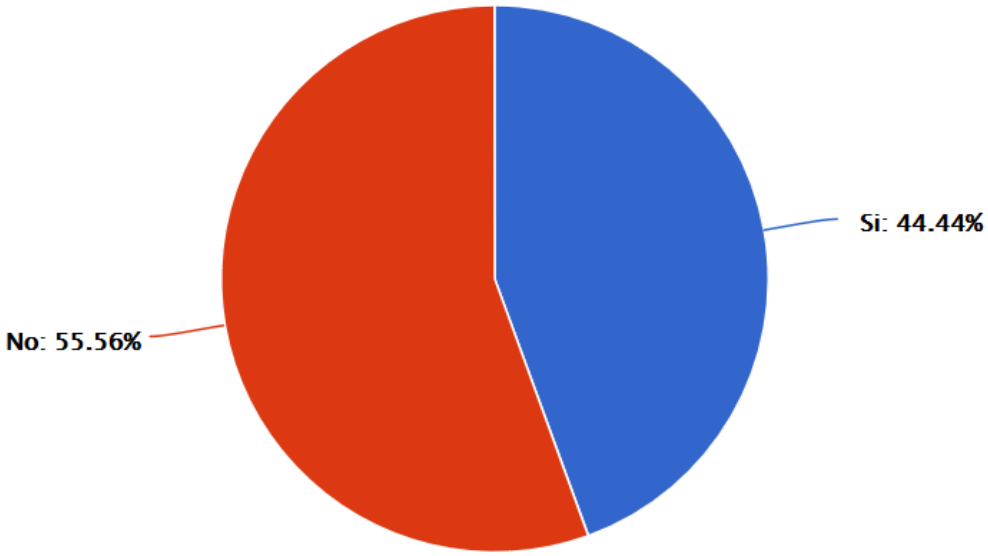


Gráfico 6 - Pregunta # 9. Fuente: Elaboración Propia

Con base en el gráfico anterior, un 55.56% no conocen de herramientas que permitan identificar si un sitio web es perjudicial o sospechoso ante su navegación o visita. Por otro lado, un 44.44% indicó saber de la existencia de este tipo de herramientas.

Pregunta número 10, Si la respuesta anterior fue afirmativa, indique cuáles.

Respuesta	Porcentaje	Cantidad
VirusTotal	16.67%	2
HybridAnalysis	16.67%	2
TrendMicro	41.67%	5
Symantec	75.00%	9
Otro	25.00%	3
	Total de respuestas	12

Cuadro 4 - Pregunta # 10. Fuente: Elaboración Propia

Los 12 usuarios que respondieron de forma afirmativa en la pregunta número 9, se dividen en 4 grupos. Un 75% indicaron conocer Symantec como medio de identificación ante sitios web sospechosos. Un 41.67% reconocen a TrendMicro, mientras que un 16.67% conocen las herramientas VirusTotal y otro 16.67% HybridAnalysis. Por último, un 25% muestra conocimiento en otra herramienta.

Pregunta número 11, ¿Tiene usted la costumbre de validar la confiabilidad o seguridad de los sitios web antes de ingresar a ellos?

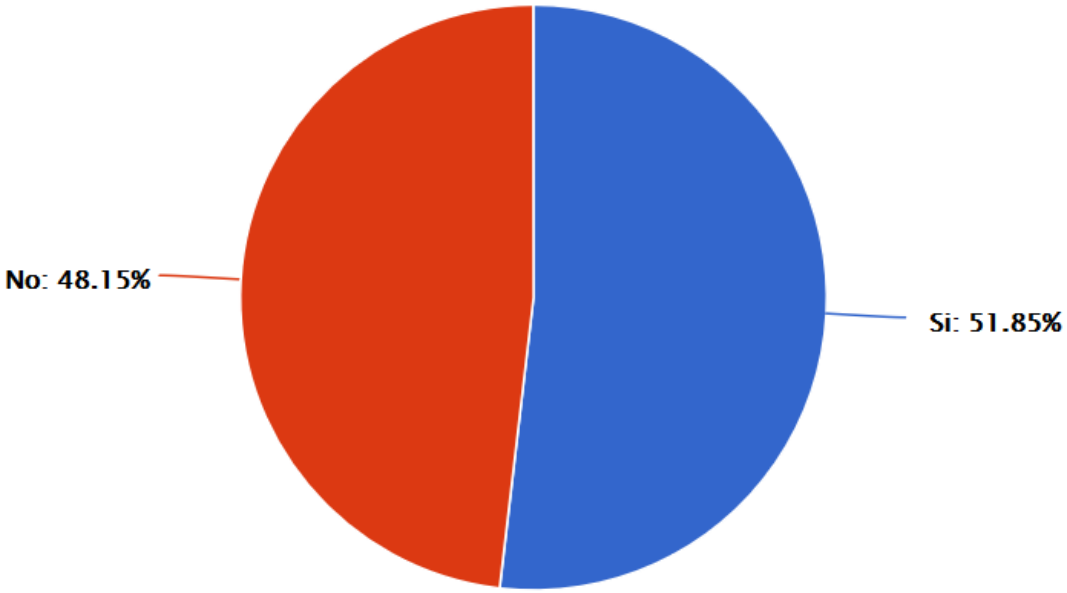


Gráfico 7 - Pregunta # 11. Fuente: Elaboración Propia

De los resultados anteriores, se evidencia que la costumbre es casi de 50/50, donde un 51.85% de los usuarios indicaron que sí revisan o son cuidados con las direcciones webs antes de visitarlas. Por otro lado, un 48.15% indicó que no revisa o no tiene cuidado ante un eventual sitio web sospechoso.

Pregunta número 12, conociendo un medio de análisis de seguridad de sitios web que advierta si el sitio es sospechoso o inseguro. ¿Lo utilizaría?

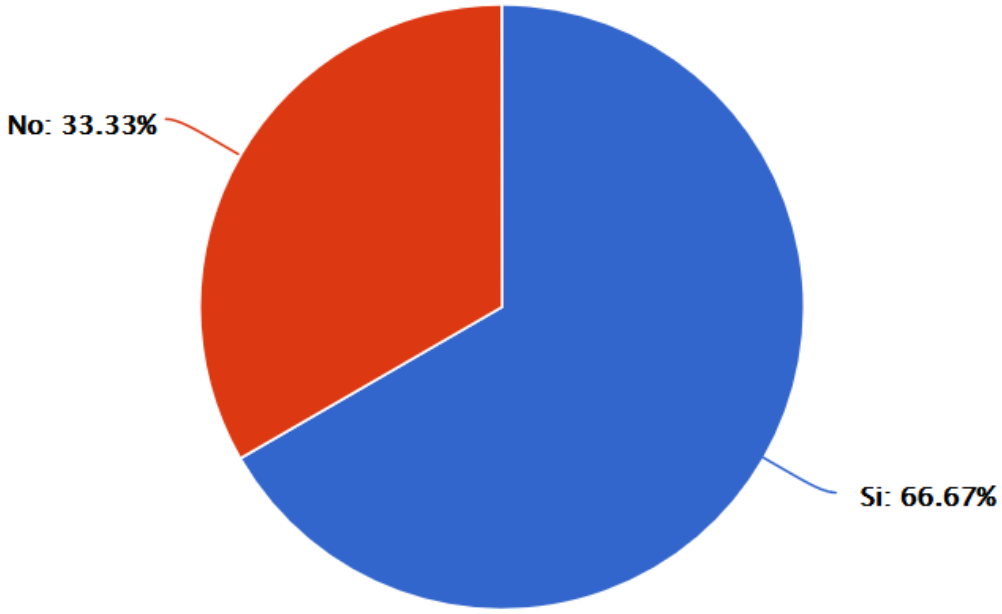


Gráfico 8 - Pregunta # 12. Fuente: Elaboración Propia

De acuerdo con la última pregunta, un 66.67 % indica que sí utilizaría un medio o vía para analizar y revisar si un sitio web es sospechoso o no. Mientras un 33.33% indica que aun así no lo utilizaría.

Capítulo 5. Propuesta de Solución

Siguiendo con el hilo de la investigación, y con el fin de revisar un poco mejor el escenario que dio como respuesta a la creación del prototipo funcional, se abarcan los siguientes 4 casos:

Una población vulnerable

En el manejo de la tecnología existen usuarios de todas las edades, desde aprendices a expertos. Y no es más que con la práctica que día a día se logra obtener más habilidades ante este mundo digital tan cambiante, claro, bajo esta premisa es que volvemos a tener dos grupos de usuarios, los que por alguna necesidad o simple gusto desean adquirir de nuevo conocimiento, o aquellos que se conforman con lo básico.

Este último grupo, es el que se convierte en foco más vulnerable ante situaciones que comprometen su seguridad en la navegación y uso de la tecnología. La noticia publicada por Fortune.com en el 2017 nos alerta el riesgo que existe en este campo, donde una estafa masiva de phishing engañó a los departamentos de contabilidad de Google y Facebook para que transfirieran entre distintos usuarios la módica suma de 100 millones de dólares a una cuenta propiedad de un hacker. (John, 2017)

Por otro lado, se tiene como evidencia también la investigación realizada, que por medio de la encuesta, reflejó que muchos usuarios de Internet no tienen la costumbre de validar la confiabilidad o seguridad de los sitios web antes de ingresar a ellos. Esto genera sin lugar a dudas, una brecha de seguridad, que es

aprovechada por los ciber delincuentes a la hora de crear los mecanismos de ejecución de ataque.

Casos de amenazas materializadas

Es importante hacer mención de algunos escenarios en los cuales por algún descuido o falta de experiencia, los usuarios que navegan en Internet han sido víctima de ataques virtuales o pérdida de activos llámese datos, dinero, entre otros. Los siguientes ejemplos ilustran amenazas materializadas en donde la seguridad de uno o varios usuarios ha sido comprometida.

Caso 1:

Hackers convierten sitio web de embajada Bangladesh en esquema de criptominado. Delincuentes cibernéticos toman el sitio web de la embajada de Bangladesh –mismo en que se tramitan visas y consultas de usuarios- y sacan provecho para realizar minado de criptomonedas. Con solo ingresar al sitio basta para que el equipo del usuario final se descargue un archivo malicioso y así sea parte de la red que realiza esta ilícita acción. Como punto interesante en la nota, se indica que "*solamente 3 de 69 motores de antivirus, detectaron el sitio infectado como malicioso*" (Lyngaas, 2019) lo cual nos llama a ser muy cuidadosos y no confiar aún en sitios web de confianza.

Caso 2:

Nueva campaña de phishing ayuda a Microsoft Azure Blob Storage a robar las credenciales de cuentas Microsoft. Se encuentra el escenario en donde se aplican 2 campañas de phishing, la primera, sentido de urgencia para actualizar

información de cuentas Office365 que aparentemente posee información desactualizada. La segunda, apunta a robar credenciales Microsoft de la plataforma Facebook Workplace, enviando una “Notificación de Facebook” vía correo que sirve como el anzuelo para que se ejecute el ataque. Para este caso, la plataforma Azure Blob Storage añade legitimidad tanto en la creación del sitio web para el phishing, como también un certificado digital firmado por Microsoft (Stewart, 2019). Al tener esto en mente, el producto final se visualiza como una trampa casi imperceptible al usuario, que de forma lamentable ingresa sus datos para luego ser robados. Se tiene que tener claro que el caso anterior descrito es una campaña, sin embargo, funciona muy similar en la vida real del ambiente laboral.

Soluciones existentes

Habiendo conocido los casos anteriores, son muchas las dudas que surgen respecto al resguardo de la seguridad de la información y su famosa triada (Disponibilidad, Integridad y Confidencialidad). Así como también, a cuánta seguridad estamos apostando para sentirnos seguros a la exposición del mundo de Internet.

Para nuestra dicha existen empresas dedicadas a la ciberseguridad que brindan mucho empeño en analizar todo tipo de vulnerabilidades, malware, y actividades sospechosas. Además, ponen a la disposición de los usuarios herramientas para el análisis tanto de equipos físicos, o bien, servicios en la nube. Y son algunos de estos servicios los que se tratarán de explicar de una forma sencilla a continuación.

HybridAnalysis, es un servicio gratuito para el análisis de malware. Cuenta además de un SandBox (Caja de arena) donde se analiza todo tipo de malware o amenaza en un entorno controlado, con la particularidad de simular un ambiente de trabajo de un usuario común. La siguiente imagen ilustra la página de inicio del sitio web.

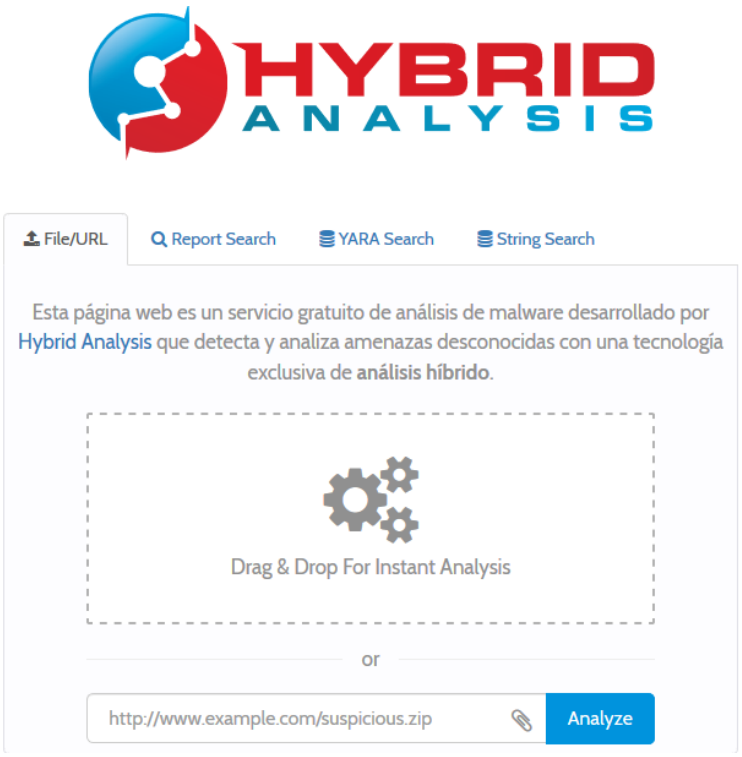


Imagen 12 - Sitio web Hybrid Analysis. Fuente: Elaboración propia

Sucuri, por otro lado, ofrece una gran variedad de productos relacionados con la garantía de seguridad de la información. Entre ellos Muro corta fuegos de sitios web (Website Firewall) como también una plataforma de seguridad a sitios web, al apostar por un mercado meramente de navegación de internet. La siguiente imagen muestra el servicio ofrecido por la empresa para lo que es el análisis de direcciones URL.

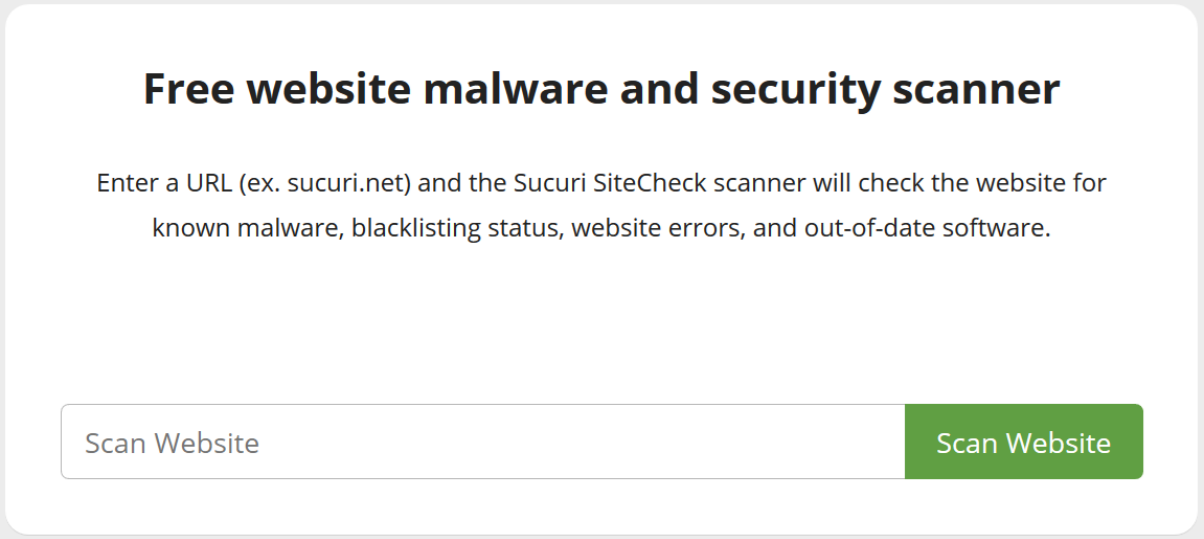


Imagen 13 - Sitio web Sucuri. Fuente: Elaboración propia

Symantec, una de las compañías líderes en seguridad informática, pone también a la disposición de los usuarios una página web para poder validar la reputación o confianza de las direcciones URL o bien, sitios web.

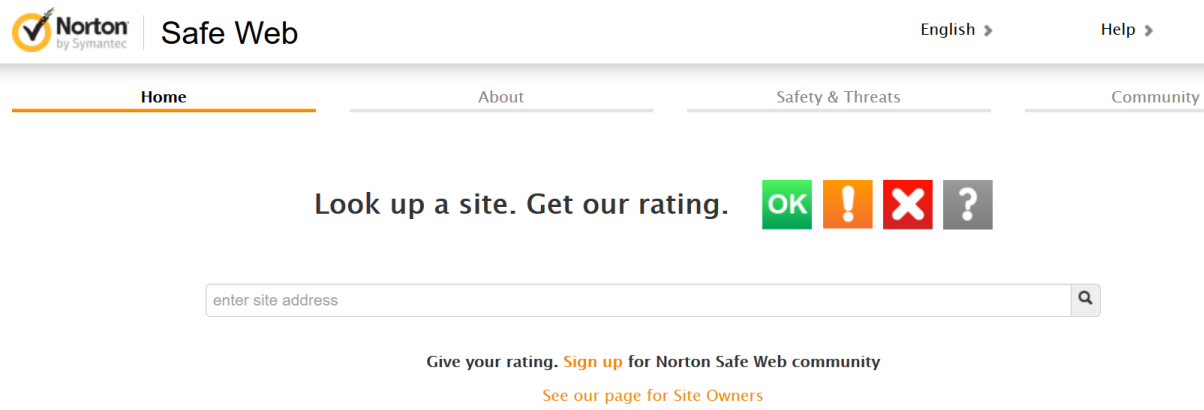


Imagen 14 - Servicio escaneo URL de Symantec. Fuente: Elaboración Propia

Para finalizar este apartado, se realizó una comparativa con herramientas actuales que brinden el servicio de analizar direcciones URL, bondades que ofrecen y sus

diferentes formas de análisis. Es así que se crea la siguiente tabla con el fin de mostrar valores como la fuente u origen del servicio, tiempos de carga-análisis y la plataforma en que se ejecuta.

Tabla Comparativa

Servicio por	Fuente	Movilidad	Plataforma	Tiempo análisis	Tiempo carga	Captura de Url
URL Scanner	Elaboración propia	Si	Android (Móvil)	3 segundos	1 segundo	Cámara (escáner)
Symantec	https://safeweb.norton.com	No	Web	1 segundo	2 segundos	Caja de texto
HybridAnalysis	https://www.hybrid-analysis.com	No	Web	6 minutos	2 segundos	Caja de texto
Virus total	https://www.virustotal.com	Si	Web/Móvil	2 segundos	1 segundo	Caja de texto
Trend Micro	https://global.sitesafety.trendmicro.com	Si	Web	2 segundos	3 segundos	Caja de texto
URLVoid	https://www.urlvoid.com	No	Web	3 segundos	2 segundos	Caja de texto
WebInspector	https://app.webinspector.com	No	Web	NA	3 segundos	Caja de texto
Sucuri	https://sitecheck.sucuri.net	No	Web	2 segundos	2 segundos	Caja de texto
Kaspersky VirusDesk	https://virusdesk.kaspersky.com	Si	Web/Móvil	4 segundos	2 segundos	Caja de texto

Tabla 3 - Comparativa entre servicios de seguridad. Fuente: Elaboración propia

Solución propuesta

La aplicación de escaneo de sitios web sospechosos, se presenta como una solución ante la incertidumbre o desconocimiento por parte de los usuarios de Internet que sufren muchas veces de dudas, infecciones en sus equipos o robo de información por medio de ataques como el phishing. Y no solamente eso, tal como refleja la investigación en curso, existen sitios web sospechosos que toman ventaja de los equipos de los usuarios, éstos sin estar conscientes.

De este modo, es que se propone la creación de un prototipo de aplicación móvil que cubra la necesidad de forma inicial, de poder identificar el grado de

amenaza de las direcciones web que nos encontramos, ya sea por medio de algún correo electrónico, o bien, aquellas que aparezcan en un sitio web o medio impreso. Un punto que vale la pena mencionar es la utilización del teléfono inteligente como medio de escaneo (utilizando la cámara), así se le evita al usuario la opción de ingresar a la dirección URL en su navegador, al ganar ventaja para la ejecución de un análisis previo a la visita. Una vez el sitio web ha sido analizado, se le informa al usuario para que éste tome la decisión final.

La siguiente infografía detalla de una buena manera la propuesta:

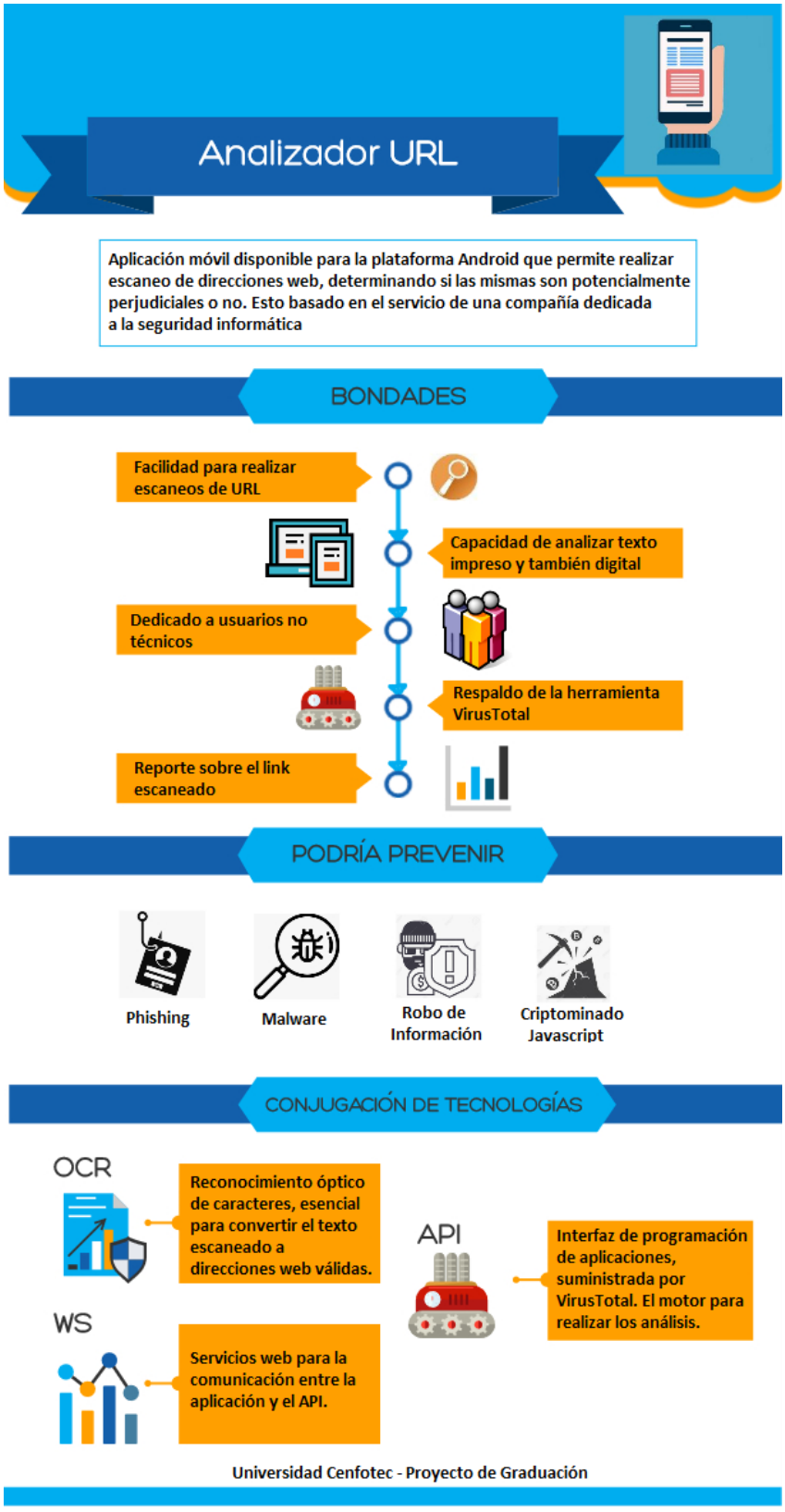


Imagen 15 - Infografía analizador URL. Fuente: Elaboración propia

La aplicación se pretende desarrollar para ser ejecutada en el sistema operativo Android en su fase inicial, para escanear direcciones URLs que luego el sistema generará una respuesta ante la dirección escaneada de si el sitio es sospechoso o no. Cabe mencionar que esta herramienta se puede ver como un tipo de control compensatorio a la hora de tomar una decisión de si continuamos trabajando con esa dirección electrónica que la aplicación nos indica como poco confiable. El siguiente diagrama de flujo muestra el proceso de la aplicación:

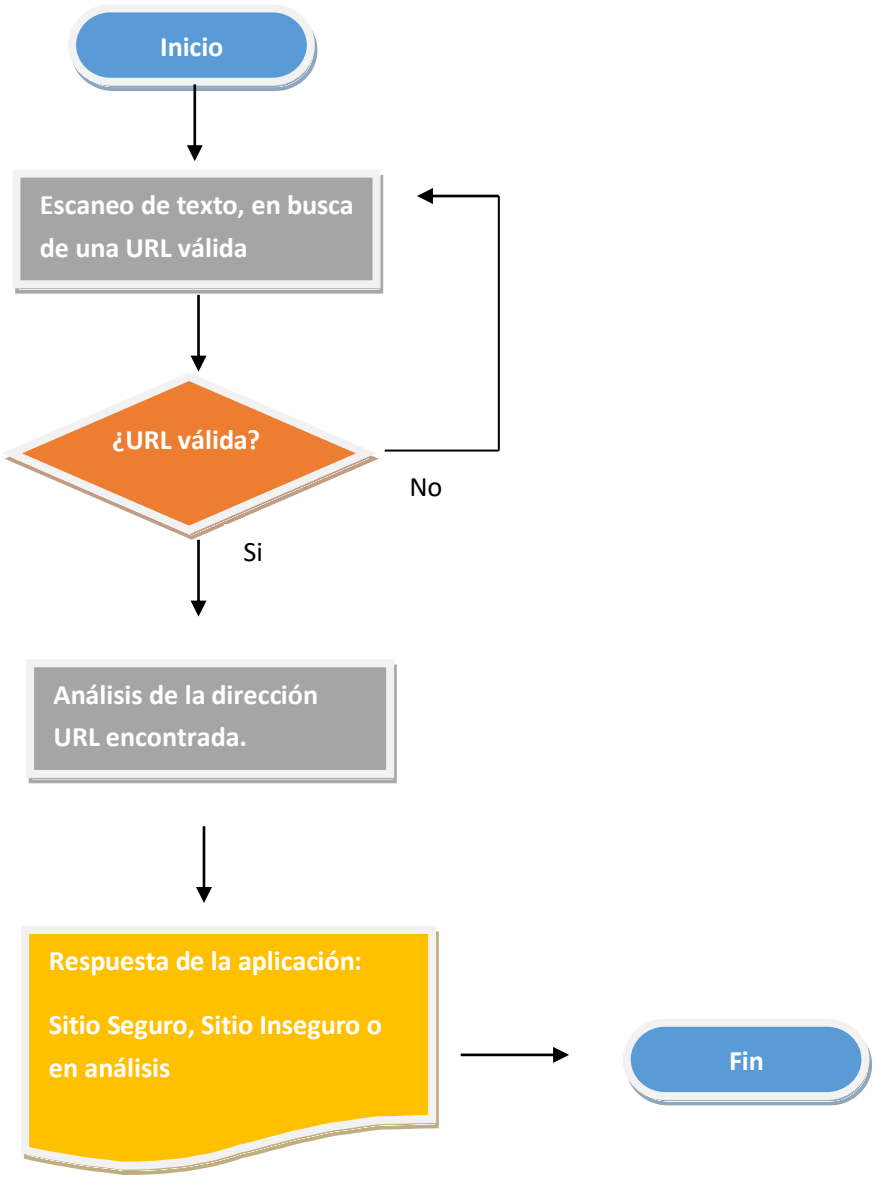


Gráfico 9 - Diagrama de flujo del prototipo de aplicación

Como información adicional, se puede encontrar en el Anexo # 2, toda la funcionalidad con una demostración paso a paso del prototipo desarrollado.

Por último, para la distribución de la aplicación en primera instancia se puede recurrir a la generación de un archivo en formato “apk” para ser instalado en los equipos donde se vaya a utilizar la aplicación de escaneo. En futuras versiones se tiene planeado subir la aplicación a Play Store para que pueda ser descargada por todos los usuarios de Android.

Capítulo 6. Conclusiones y Recomendaciones

6.1 Conclusiones

Una vez analizados los datos que se recabaron en la investigación, se tiene como conclusiones:

1. Con ayuda de la tecnología de reconocimiento óptico de caracteres, se puede capturar texto explícito en medios físicos o digitales, y delimitar su transformación en direcciones URL válidas para su análisis. Evitando que el usuario tenga que digitar o accidentalmente cargar en su equipo direcciones sospechosas. Gracias a la creación del prototipo de escaneo de URLs, se facilita la captura y análisis de direcciones en sitios web.
2. Poder consultar una Interfaz de Desarrollo de Aplicaciones (API) con respaldo de múltiples antivirus y poder incorporarla en aplicaciones cliente hace que el acercamiento a un usuario de internet promedio sea de gran utilidad, ya que al usar su teléfono inteligente se puede ver alerta en caso de un sitio web sospechoso.
3. Se analizan distintas herramientas que ofrezcan servicios de análisis de direcciones URL, tanto en plataforma web, como de dispositivos móvil. Además, se realiza una comparativa entre el tiempo de la respuesta al usuario, como la reputación de las fuentes.
4. Se realiza un prototipo funcional de escaneo de direcciones URL, donde una vez la dirección es reconocida por la aplicación, se analiza y en cuestión de segundos se muestra una respuesta al usuario, donde las 3 posibles respuestas son: Sitio Seguro, Sitio Inseguro y Sitio en Revisión.

6.2 Recomendaciones

El hecho de contar con una mayor experiencia en el área de programación móvil, facilitará de una mejor manera la escalabilidad de la aplicación, tanto en términos de diseño como de funcionalidad.

Es recomendable estudiar los servicios y aplicaciones actuales de seguridad que ayudan a los usuarios a evitar las amenazas o ser víctimas de fraude, virus, robo de información. Esto con el fin de poder mejorar los servicios o aplicaciones que se piensen desarrollar.

Por último, se sugiere el estudio de otras vías de captura de información. En la versión actual se utiliza la cámara del teléfono inteligente para capturar una dirección URL y su análisis, pero en términos de seguridad nunca es suficiente. Se puede revisar eventualmente cualquier tipo de información que tenga interacción con el teléfono inteligente (entrada y salida), con tal de resguardar los datos del usuario de una mejor manera.

Capítulo 7. Trabajos de Futuro

La creación del prototipo y la investigación que se desarrolló en este proyecto, es apenas la fase inicial de una aplicación móvil que ayude en la seguridad a los usuarios que navegan por Internet y se exponen muchas veces a riesgos y amenazas que en su mayoría pueden no conocer.

Existen varios puntos de mejora, que vendrían muy bien ser incorporadas en el prototipo de la aplicación desarrollada, a continuación, se mencionan algunas (pero no limitadas a ellas):

- Diversificar motor de análisis. La aplicación cuenta actualmente con el API de VirusTotal. Puede escalar a la incorporación de 2 o más motores de análisis, con el fin de buscar analizar más a fondo las direcciones web, o bien, inconsistencias que se conviertan en amenazas para el usuario.
- Analizar imágenes con direcciones URL. Una funcionalidad que resultaría de utilidad, es el modo en que sea realiza la captura de las direcciones URL, actualmente se realiza por medio de la cámara, la mejora viene en añadir un botón u opción de menú que permita seleccionar imágenes almacenadas en el celular en busca de direcciones URL.
- Nuevo diseño de algoritmo. Como mejora en el análisis de seguridad del prototipo desarrollado, existe la posibilidad de crear un algoritmo o función que evalúe si las páginas web a consultar poseen certificados de seguridad válidos, vigentes y acorde con lo que se solicita. A esto también una correcta revisión sobre el cifrado que se maneja.

- Histórico de sitios analizados. El prototipo actual no guarda en ningún sitio las revisiones de direcciones web analizadas. Sería de utilidad crear una función de menú que esté ligada a un archivo o log que maneja al menos las últimas 10 direcciones analizadas. De esta forma se gana tiempo en revisiones recurrentes o simplemente se tiene a la mano aquellas direcciones que resultaron sospechosas.

Tabla de Acrónimos

API	Application Programming Interface proveniente del inglés. En español se traduce como Interfaz de Desarrollo de Aplicación.
IDE	Integrated Development Environment proveniente del inglés. En español se traduce como Entorno de Desarrollo Integrado
SDK	Software Development Kit proveniente del inglés. En español se traduce como Kit de Desarrollo de Software.
DNSBL	Domain Name System Blacklists proveniente del Inglés. En español se traduce como nombre de sistema de dominio en lista negra.
URL	Uniform Resource Locator del Inglés. En español se traduce como localizador uniforme de recursos.

Referencias

Agüero, P. Z. (2010). *El Rombo de las Investigaciones de las Ciencias Sociales.* Cuba.

Albors, J. (27 de Junio de 2016). *Welivesecurity.* Obtenido de https://www.welivesecurity.com/la-es/2016/06/27/peligro-scripts-maliciosos-como-protegerte/

Anderson, L. W. (2001). *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives.* Boston, MA: Pearson Education Group.

Android. (25 de Abril de 2018). *Developers.Android.com*. Obtenido de https://developer.android.com/guide/platform/?hl=es-419#art

Aranaz, J. (Enero de 2009). Desarrollo de aplicaciones para dispositivos móviles sobre plataforma Google. *Desarrollo de aplicaciones para dispositivos móviles sobre plataforma Google*. Madrid, España.

Certsuperior. (2016). *Certsuperior.* Obtenido de https://www.certsuperior.com/CertificadosSeguridad.aspx

Definicion. (20 de 04 de 2019). *Definicion*. Obtenido de https://definicion.de/ocr/

DNSBL. (s.f.). *dnsbl*. Obtenido de dnsbl: https://www.dnsbl.info

El Universal. (18 de 07 de 2018). *ElUniversal.com.mx*. Obtenido de http://www.eluniversal.com.mx/cartera/telecom/android-lider-en-sistemas-operativos-para-dispositivos-moviles

Garud, S. (2 de Oct de 2017). *Quora*. Obtenido de https://www.quora.com/What-exactly-happens-during-an-Android-APK-creation-build-process

Genexus. (06 de enero de 2016). 3 tipos de aplicaciones móviles. *3 tipos de aplicaciones móviles: ventajas y desventajas que deberías conocer*.

Griffiths, D. (28 de Enero de 2017). *GitHub*. Obtenido de GitHun: https://github.com/dogriffiths/HeadFirstAndroid/wiki/How-Android-Apps-are-Built-and-Run

IBM. (25 de 04 de 2014). *ibm.com*. Obtenido de ibm.com: https://www.ibm.com/support/knowledgecenter/es/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55710_.htm

InnovaAge. (s.f.). *innovaage.com*. Obtenido de innovaage.com: https://www.innovaportal.com/innovaportal/v/696/1/innova.front/apps-hibridas-vs-nativas-vs-generadas-que-decision-tomar

John, J. (27 de April de 2017). *Fortune.com*. Obtenido de Fortune.com: http://fortune.com/2017/04/27/facebook-google-rimasauskas/

Kaspersky. (s.f.). *Kaspersky* . Obtenido de Kaspersky : https://www.kaspersky.com/resource-center/definitions/drive-by-download

Kotlin. (30 de 03 de 2019). *Kotlin*. Obtenido de https://kotlin.es/sobre-kotlin/

Lyngaas, S. (27 de Feb de 2019). *Cyberscoop*. Obtenido de https://www.cyberscoop.com/hackers-turn-bangladeshi-embassy-website-into-cryptomining-scheme/

Roberto Hernández, C. F. (2006). *Metodología de la investigación.* México DF: McGraw-Hill Interamericana.

Schechter, E. (24 de Julio de 2018). *Google.* Obtenido de Google: https://www.blog.google/products/chrome/milestone-chrome-security-marking-http-not-secure/

Stewart, R. (28 de Feb de 2019). *Cyware*. Obtenido de https://cyware.com/news/a-new-phishing-campaign-leverages-microsofts-azure-blob-storage-to-steal-users-microsoft-account-credentials-f74dfe3a

Symantec. (1 de 12 de 2018). *Norton.* Obtenido de Norton: https://us.norton.com/internetsecurity-malware-what-are-malicious-websites.html

Techopedia. (23 de 03 de 2019). *techopedia*. Obtenido de https://www.techopedia.com/definition/4220/android-sdk

UC, D. (30 de 03 de 2019). *Duoc.cl*. Obtenido de http://www.duoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

VirusTotal. (20 de Febrero de 2019). *Virustotal*. Obtenido de https://www.virustotal.com/es/

Anexos

Anexo # 1

A continuación, se presenta la lista de preguntas utilizadas en el instrumento de recolección de datos:

1. ¿Cuál es su rango de edad?
2. ¿Cuál es su género?
3. ¿Nivel Académico?
4. ¿En qué área se enfocan sus estudios actuales o previos?
5. ¿En qué área profesional se desempeña?
6. ¿En qué dispositivo suele navegar más en Internet?
7. ¿Para realizar transacciones web delicadas o seguras, qué dispositivo utiliza más?
8. ¿Ha sido víctima de algún fraude por el uso de Internet en el último año?
9. ¿Ha sido víctima de infección de virus en su equipo de navegación web en el último año?
10. ¿Qué tipo de protección virtual (anti malware, antivirus, etc) utiliza para sus equipos?
11. ¿Conoce de herramientas en línea que permitan identificar si un sitio web es sospechoso o confiable?

12. Si la respuesta anterior fue afirmativa, indique cuáles. De lo contrario puede pasar a la siguiente pregunta.

13. ¿Tiene usted la costumbre de validar la confiabilidad o seguridad de los sitios web antes de ingresar a ellos?

14. Conociendo un medio de análisis de seguridad de sitios web que advierta si el sitio es sospechoso o inseguro. ¿Lo utilizaría?

Anexo # 2

A continuación, se realiza la demostración del prototipo funcional que se desarrolló a lo largo de la investigación del proyecto. El escenario se visualiza como una guía explicativa de cómo utilizar la aplicación y las diferentes respuestas ante distintas direcciones URL.

Pantalla Inicial

La intención en el diseño fue crear una interfaz sencilla y amigable con el usuario, con la cantidad mínima de “toques” o acciones en pantalla. Es así que al abrir la aplicación nos encontramos con una visualización donde la cámara está activa y puede escanear direcciones URL, además un botón en el final para ejecutar la acción con el nombre de “Capturar URL”.

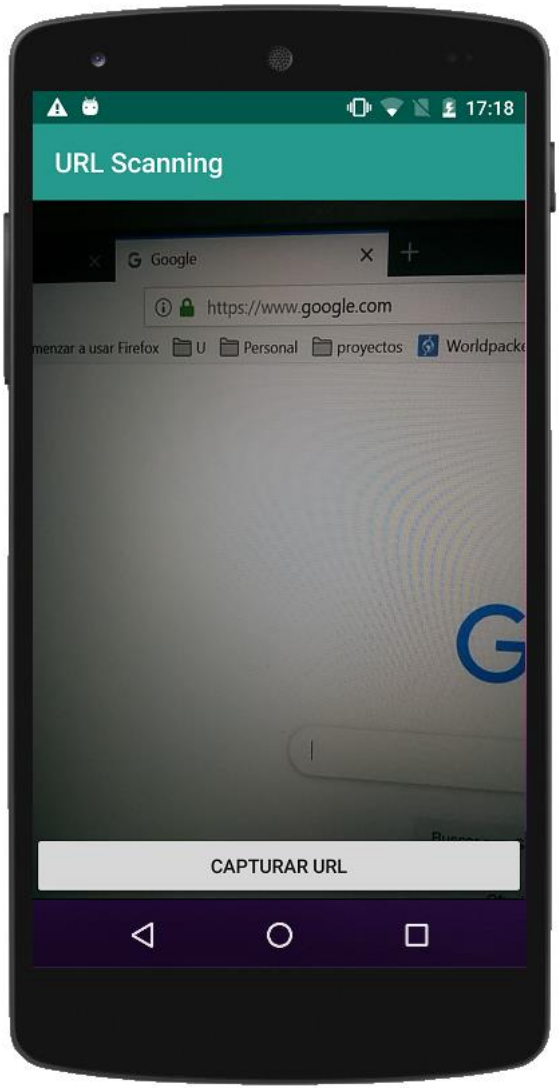


Imagen 16 - Pantalla Inicial de aplicación móvil. Fuente: Elaboración propia

Captura de direcciones URL

Una vez observamos que la aplicación posee habilitada la cámara y en funcionamiento, se procede a escanear direcciones URL, ya sea impresas o en el navegador web. Para efectos de esta demostración se procede a escanear 3 distintas direcciones URL con el fin de poder visualizar los distintos escenarios. El de un sitio sospechoso, el de un sitio pendiente de análisis y el de un sitio seguro para navegar. La siguiente imagen muestra la dirección URL encontrada luego de escanear el sitio “www.crautos.com”.

Imagen 17 - Captura de direcciones URL. Fuente: Elaboración propia

Una vez que la dirección URL es identificada, se muestra una ventana emergente con los URLs detectados. El siguiente paso es seleccionar la opción de menú que corresponde al URL por analizar.

Resultado “Sitio seguro”

Como resultado del escaneo previo y análisis al sitio “www.crautos.com”, el API de VirusTotal no encuentra indicios de amenazas. Para lo cual se le brinda una respuesta segura al usuario con una leyenda.

Imagen 18 - Respuesta sitio seguro. Fuente: Elaboración propia

Resultado “En análisis”

Al realizar el segundo análisis al sitio “https://www.independent.co.uk/life-styl”, el API de VirusTotal no encuentra una respuesta inmediata a la solicitud, por lo cual la petición queda en estado de análisis y se le indica al usuario que vuelva a intentar en unos minutos, además de comunicar que existe cierto riesgo en caso de continuar con la visita del sitio web.

Imagen 19 - Respuesta en análisis. Fuente: Elaboración propia

Resultado “Sitio sospechoso”

Finalmente, como resultado del escaneo y análisis al sitio web “www.teamclouds.com”, el API de VirusTotal encuentra indicios de riesgo y además varios motores de protección antivirus detectan el sitio como una amenaza. Para lo cual se le brinda una respuesta de advertencia al usuario de que si continúa con la visita al sitio puede ser víctima de fraude, infección o robo de datos.

Imagen 20 - Respuesta sitio sospechoso. Fuente: Elaboración propia