VICERRECTORÍA ACADÉMICA

DEPARTAMENTO CURSO MONOGRÁFICO

Trabajo Final de Grado para optar por el título de:

Ingeniería en Sistemas de Computación

Título de la monografía:

Aplicación móvil para minimizar el riesgo de exposición de información confidencial en redes sociales

Elaborado Por

Richard Sabino Medina	2011-0028	→ A00079663
Junior Bier Arroyo	2017-0117	→ A00097722
Frammy Ramos	2016-0091	→ A00094669

ASESORES:

Willis Ezequiel Polanco

Willy Alfredo Padua Ruiz

Coordinación Trabajo Final Curso Monográfico

Dra. Sención Raquel Yvelice Zorob Avila

Distrito Nacional

2021

Agradecimiento

A mi compañero, Starlyn Patrocino quien fue mi mano derecha durante todos estos 4 años, fue quien siempre estuvo ahí en aquellos exámenes difíciles y aquellas pruebas dificultosas que solo un compañero, puede imaginarse y sabe el grado de dificulta y la dedicación aplicada para que esto sea una realidad.

A Dios, una vez más le doy las gracias porque el más que nadie sabe que si su compañía no hubiese podido hacer de esto una realidad hoy en día.

A Luis Santana, un profesor que, gracias a él, y sus consejos fue quien me instruyo y gracias a eso logre plasmar mi meta y creo que realmente sin sus consejos no se si lo hubiese podido lograr.

A Patricio Bier Silverio, mi padre quien siempre estuvo ahí en los momentos que me cansaba, desenfocaba era quien me aconsejaba y me daba fuerza durante estos largos 4 años.

Junior Bier Arroyo

Primeramente, a Nuestro Padre Celestial, por haberme dado las fuerzas necesarias para poder seguir adelante. Sin Él, esto no se hubiese podio llevar a cabo, ya que toda sabiduría, todo conocimiento y fuerza provienen directamente de Él. Gracias a Él por darme las fuerzas necesarias para poder culminar con esta etapa tan importante de mi vida como profesional.

A mi esposa, porque me dio el ejemplo al obtener su título universitario y al darme los consejos que me dio, en especial el de que yo debía hacerlo si quería llegar más lejos como profesional. Gracias, porque cuando decía que pausaria la carrera, me dabas ánimo para no hacerlo. Igualmente, a mis hijos, porque parte del tiempo que pasé en la universidad, debí dedicárselo a ellos. Gracias por entender cuán importante era para mi este proyecto de vida.

A Juan Pablo Pérez Chávez, Ex Gerente General de Smurfit Kappa República Dominicana y ahora CFO of the Americas en Smurfit Kappa Group, y a Paula Andrea Gómez, Ex Financial Controller en Smurfit Kappa República Dominicana. Por gestionar el pago del 100% de mi carrera a través de Smurfit Kappa RD. Mil gracias por sus ejemplos, por sus buenos consejos, me enseñaron como ser un buen líder y gerente al hacer las cosas de la manera correcta.

Richard A. Sabino Medina

A Dios, por darme la vida, fuerzas, sabiduría y salud desde inicio a fin de mi carrera en la universidad APEC, por permitirme seguir siempre adelante en todo mi trayecto universitario sin importar los tropiezos y momentos difíciles.

A mi madre que en todo momento me ha apoyado en cada una de las decisiones importantes de mi vida, quien ha sabido darme los mejores consejos de vida para seguir creciendo espiritualmente en lo personal y académicamente.

Frammy Ramos

Dedicatoria

A Dios, por siempre darme la fuerza cuando más la necesite, y por siempre estar a mi lado en los momentos más dificultosos de la carrera, le doy las gracias porque a pesar de mis defectos permitió que esta meta pueda ser cumplida.

A Yoely Arroyo, fue alguien que indirectamente me inspiraba y me daba fuerza, porque yo como hermano mayor tenía el compromiso de terminar todos mis estudios para guiarlo por el mejor camino y se su modelo a seguir.

A Pelagia Silverio, mi abuela la cual se mantuvo brindándome apoyo, día tras día en todos los sentidos, le dedico este trabajo desde lo más profundo de mi corazón.

A Yoselin Arroyo, mi madre quien siempre me brindo su apoyo económico, y me amortiguaba cada ciclo, ayudándome siempre a tomar las mejores decisiones en los momentos más dificultoso durante estos 4 años.

Junior Bier Arroyo

A Nuestro Padre Celestial por la oportunidad de estudiar en esta universidad y por darme las fuerzas necesarias para seguir hasta el final. Sin Él, nada de lo que queremos hacer se puede lograr, todo es gracias a Él.

A mi esposa Nidia Figuereo, por apoyarme y soportar mi ausencia mientras estuve en clases presenciales.

A mis padres, Agapito Sabino e Higinia Medina por apoyarme, por darme ánimo e inspirarme para lograr este sueño que por mucho tiempo quise lograr.

A mis hijos, porque también dediqué mucho tiempo a la universidad en tiempos de clases presenciales, tiempo que debí dedicarles a ellos.

Richard Sabino Medina

A mi madre, este logro no es solo mío, de hecho, es más de ella que mío. Sí, así es, hablo de ti mami, eres sin duda mi gran ejemplo a seguir, me has llenado de valores y fuerzas para luchar por todos y cada uno de mis sueños, me has apoyado y creído en mi en todo momento y gracias a eso hoy puedo decir que no solo soy feliz, sino que además soy una persona de bien que tiene bastante claro lo que quiere en su vida. Nunca me cansaré de darte las gracias este y absolutamente todos mis logros son y serán siempre en tu honor y para ti.

Frammy Ramos

Índice General

Índice de Contenido

Índice de Figuras

Resumen

En este trabajo hemos podido identificar los riesgos de compartir información confidencial en las redes sociales y páginas webs. Identificamos algunas de las razones más relevantes por las cuales las personas comparten información confidencial en las redes sociales y páginas webs. Igualmente investigamos algunas de las técnicas más comunes que utilizan los ciber delincuentes para convencer a sus víctimas de compartir información confidencial en las redes sociales y páginas webs. Hemos analizado las técnicas más utilizadas para los ciber delincuentes lograr convencer a las personas de compartir su información confidencial. Con lo antes investigado, hemos desarrollado una aplicación que ayudará a los usuarios a no compartir información confidencial en páginas web y redes sociales, minimizando así los riesgos que estas acciones acarrean en los usuarios. Esta aplicación ayudará a bloquear e identificar si la página web, o la red social donde el usuario está compartiendo información confidencial es segura o no.

Introducción

La seguridad e integridad de la información ya sea de una persona, institución o empresa es algo fundamental. Por tal razón existen personas o individuos que intentan a diario obtener información confidencial y valiosa, para ellos tratar de obtener algún tipo de beneficio mediante la utilización de dicha información obtenida, ya sea de una empresa, persona o institución, utilizando a diario las distintas técnicas y ataques que existen, tratando de encontrar una brecha para poder penetrar la seguridad de dicha empresa y así logrando obtener las informaciones que buscan.

Mucha gente hoy en día utiliza la internet, ya sea para navegar en las redes sociales, compartiendo informaciones mediante Facebook, Instagram, Correo electrónico entre otras aplicaciones. También existen personas que se loguen en páginas web desconocidas, ya sea para hacer una compra en línea, tomar algún curso u obtener algún tipo de servicio. El problema es que muchos lo hacen sin ningún tipo de seguridad, siendo ellos lo más vulnerables al momento de navegar.

Sin embargo, hoy en día existen muchos riesgos al momento de navegar en algunas páginas web y al utilizar las redes sociales, porque en muchas ocasiones el propio usuario comparte información confidencial y valiosa para los

cibercriminales, de tal manera convirtiéndose el usuario en una víctima fácil de penetrar.

Por tal razón para reducir los riesgos de las personas y empresas al compartir información confidencial mediante la utilización de las redes sociales y distintas páginas web, así evitando de que se conviertan en futuras víctimas de los cibercriminales, en este trabajo se propone un análisis y diseño de una aplicación móvil llamada Personal Info Protector que se encarga de disminuir al máximo todos los posibles ataques y técnicas realizadas por los cibercriminales al momento de navegar en la web y redes sociales.

Personal info Protector es una aplicación que ofrece distintas funcionalidades que protege a todos los usuarios que la utilizan, mejorando su seguridad durante la navegación en páginas web y redes sociales, logrando evitar y mitigar los riesgos al momento de compartir informaciones confidenciales, Personal Info Protector le brindara a usuarios inexpertos una navegación segura y limpia ya que previene, detecta y elimina todo tipos de amenazas y posibles ataques que podrían ser proporcionado por los cibercriminales.

El desarrollo de este trabajo final de curso monográfico se ha dividido en seis capítulos:

1. Planteamiento Metodológico: En este capítulo se explica la problemática que surge al momento de compartir información confidencial a través de las redes sociales y páginas web, también se justifica el trabajo de investigación; además se plantean los objetivos, tanto general como específicos, que persigue este trabajo de investigación.

2. Marco Referencial: Este capítulo es de suma importancia, es donde se desarrolla el marco teórico, donde se identifican distintas teorías que son aplicadas durante el desarrollo de este trabajo final; después más adelante es donde se desarrolla el marco conceptual, que es ahí donde se definen los principales conceptos.

3. Riesgos y causas: En este capítulo es donde se desarrollan y se plasman algunos de los riesgos que existen al momento de compartir información confidencial, y también se muestras las causas por la cual comparten este tipo de información, además se brindan algunos ejemplos de distintos engaños y ataques que ejecutan los cibercriminales a las personas y empresas intentando sacarles información confidencial y valiosa a las víctimas.

4. Análisis y diseño del Sistema: En este capítulo es donde se muestran las diferentes interfaces del sistema de manera gráfica a través de imágenes, también es donde se desarrollan e identifican los requisitos funcionales para describir el comportamiento del sistema, así como también los requisitos no funcionales para especificar como se deben realizar las cosas.
También es donde se muestran cada una de las herramientas y funcionalidades de la aplicación, además por otra parte se muestran algunos de los distintos comportamientos que tiene la aplicación mediante diagramas.

5. Mitigación de los riesgos: en este capítulo es donde se desarrolla y se explica, como atreves de Personal Info Protector se disminuirán los riesgos agotando al máximo cada una de las herramientas y funcionalidades del sistema.
También es donde se identifican cada uno de los beneficios que obtendrán los usuarios al momento de utilizar Personal Info Protector y las desventajas y restricciones que tendrían por el uso de esta.

6. Conclusiones: En este capítulo es donde cada uno de los integrantes expresa su opinión y reflexión sobre el trabajo realizado durante todo el proceso de la realización de este.

Capítulo 1: PLANTEAMIENTO METODOLÓGICO

1.1 Identificación del Problema

En la Republica Dominicana el número de denuncias relacionadas con delitos informáticos ha ido en aumento en los últimos años. Las autoridades están haciendo lo posible para controlar y/o minimizar este tipo de ataques decretado varias leyes para castigar los delitos que se cometen especialmente cuando se utilizan dispositivos de alta tecnología. Igualmente se han creado organismos institucionales para investigar, dar seguimiento, perseguir y enviar a la justicia a aquellos ciudadanos que quebranten las leyes relacionadas con el delito de alta tecnología.

En el caso de que un cibercriminal obtenga información básica como numero de cedula, fecha de nacimiento, u otro tipo de información confidencial, este puede reproducir una cedula y hacerse pasar como el verdadero dueño de la información para tomar prestamos, vender propiedades como vehículos, tierras, casas, comprar celulares a créditos, entre otros.

Estos cibercriminales obtienen toda esa información utilizando un método llamado ingeniería social, el cual consiste en convencer a la víctima para que comparta información confidencial al hacerse pasar por una entidad bancaria de confianza, un familiar cercano, institución gubernamental, etc.

1.2.1 Justificación del Problema

En la Republica Dominicana existen leyes que controlan y castigan a los cibercriminales que violan las leyes y que cometen delitos de alta tecnología. Pero en el caso de que seamos estafados por suplantación de identidad y que un ciber delincuente obtenga beneficios a coste de nuestra identidad, todos esos beneficios que ese delincuente obtuvo no se pueden recuperar y lamentablemente, el daño causado no se puede reparar con el simple hecho de encarcelar a estos mal hechores.

Es por esta razón que proponemos una solución para diseñar una Aplicación (móvil o web) para minimizar el riesgo de exposición de información confidencial en redes sociales.

1.2.2 Justificación Teórica

La investigación propuesta busca, mediante la aplicación de la teoría y conceptos de ingeniería en sistemas, y la seguridad informática, advertir y evitar que las personas compartan información confidencial en las redes sociales, ejemplo: aplicaciones de mensajería instantánea como Facebook Messenger, WhatsApp, Telegram, etc. Igualmente evitar que estas informaciones sean enviadas vía correo electrónico, compartidas en las redes sociales como Facebook, Twitter y/o Instagram, por mencionar algunas. Igualmente buscamos

evitar que ante un ataque phishing, el usuario no caiga en la trampa de enviar datos confidenciales como nombres de usuarios, contraseñas, etc.

1.2.3 Justificación Práctica

Este sistema se basará en la necesidad que tienen las personas de no tener conocimientos necesarios para determinar si la persona que recibe esta información confidencial es confiable o no. Mediante la implementación de un código inteligente basado en Inteligencia Artificial, la aplicación podrá predecir si el destinatario es de confianza o no.

Esta solución evitara los contratiempos que tienen que pasar las personas estafadas yendo a las diferentes instituciones gubernamentales buscando resolver el problema de haber sido estafados.

1.2.4 Justificación Metodológica

Como el objetivo de la investigación es implementar una Aplicación (móvil o web) para minimizar el riesgo de exposición de información confidencial en redes sociales, aplicaremos las mejores prácticas mediante un proxy integrado el cual evitara que la información confidencial sea compartida por las personas a través de redes sociales, correos electrónicos, web, SMS, entre otros.

1.3 Objetivos

1.3.1 Objetivo General

Proponer una aplicación web y móvil que proporcione al usuario final la protección necesaria y oportuna, reduciendo así el riesgo de exposición de información confidencial en redes sociales.

1.3.2 Objetivos Específicos

- Analizar cuáles son los riesgos y las principales causas por la que los usuarios comparten información confidencial en las redes sociales y páginas web.

- Diseñar una aplicación móvil que disminuya los riesgos y exhibición de datos confidenciales en las redes sociales y páginas web.

- Evaluar como mitigaría la propuesta los riesgos al compartir información confidencial, proyectando los beneficios y desventajas al adoptar esta aplicación.

1.4 Tipo de Investigación

Este trabajo de grado posee todas las características metodológicas de una investigación aplicada, en virtud de que se utilizaron conocimientos de Ingeniería de Sistemas para aplicarlos en el proceso de la creación de una aplicación móvil y web para la gestionar y minimizar el riesgo de exposición de información confidencial en redes sociales.

Capítulo 2: MARCO REFERENCIAL

Marco Teórico

APLICACIÓN (MÓVIL O WEB) PARA MINIMIZAR EL RIESGO DE EXPOSICIÓN DE INFORMACIÓN CONFIDENCIAL EN REDES SOCIALES

La información confidencial en las redes sociales se puede visualizar en la mayoría de los perfiles, dígase Facebook, que es la más usada, Twitter, Instagram, y los ciberdelincuentes las están utilizando para delinquir, vender la información en diferentes sitios web, formar un perfil de un individuo, para luego realizar diferentes acciones ilegales desde abrir un préstamo a nombre de la víctima, adquirir productos y servicios a crédito a cargo de la víctima, entre otros. Igualmente, muchos ciberdelincuentes solicitan información confidencial a usuarios utilizando diferentes métodos de ingeniería social para hacerles creer a los usuarios que la solicitud es real y que proviene de una fuente confiable. Generalmente estos ciberdelincuentes solicitan información básica y que debe ser confidencial y que únicamente las entidades bancarias deberían manejar.

2.1 Marco Teórico

2.1.1 Información Confidencial Personal

Definición

Todo lo que se refiera a datos personales. Ninguna entidad, ni persona física puede divulgarla sin la aprobación expresa de su titular. El concepto de Información Confidencial es por tiempo indefinido, no está establecido o restringido a un vencimiento o término, en resumen, es y será confidencial y no tiene tiempo de caducidad.

Datos Personales Confidenciales

Identificación (fotografía, dirección, teléfono, numero de celular, correo electrónico, firma, Cedula, fecha de nacimiento, acta de nacimiento, edad, nacionalidad, estado civil, etc.)

Patrimoniales (información fiscal, historial crediticio, cuentas bancarias, Ingresos, egresos, etc.);

Salud (estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, etc.);

Ideológicos (creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas;

Características personales (tipo de sangre, ADN, huella digital, etc.);

Características físicas (color de piel, iris y cabellos, señales particulares, etc.); vida y hábitos sexuales, origen (étnico y racial.); entre otros.
El carácter de información confidencial es permanente y sólo pueden divulgarse si damos nuestro consentimiento expreso o por escrito.

¿Qué es confidencialidad?

La confidencialidad se refiere a cómo se manejará, administrará y difundirá la información privada de una persona o entidad. Es el derecho que tenemos de mantener nuestros datos personales privados y que solo personas con la debida autorización pueden tener acceso a ellas.

2.1.2 Aplicación Móvil

Una aplicación móvil es un programa especial que funciona únicamente en dispositivos smartphones, el cual se puede descargar para realizar diferentes funciones como reproducir música, ver videos, realizar llamadas de voz, video, etc.

2.1.3 Aplicación Web

Las aplicaciones web reciben este nombre porque se ejecutan desde cualquier navegador, sea móvil, tableta o PC/Mac. Es decir que los datos o los archivos en los que trabajas son procesados y almacenados dentro de la web. Estas aplicaciones, por lo general, no necesitan ser instaladas.

El concepto de aplicaciones web está relacionado con el almacenamiento en la nube. Toda la información se guarda de forma permanente en servidores remotos y nos envían a nuestros dispositivos o equipos los datos que requerimos en ese momento, quedando una copia temporal dentro de nuestro dispositivo.

2.1.4 Exposición Información Confidencial

Se entiende por exposición a la acción y efecto de exponer algo para que sea visto, oído y apreciado por otras personas. Ya el termino información confidencial está definido más arriba, por lo que, podríamos describir que es el hecho de exponer nuestros datos confidenciales donde otras personas puedan verlos fácilmente, ejemplo, en las redes sociales, enviarlos por correo electrónico, llenar un formulario en línea en una página sospechosa, entre otros.

Minimizar el Riesgo

Se entiende por minimizar por el hecho de reducir lo más posible el tamaño de algo o quitarle importancia. Y se entiende por riesgo a la contingencia o proximidad de un daño. En este caso, minimizar el riesgo estamos hablando de reducir el riesgo a su mínima expresión, evitando los posibles daños que la acción que estamos ejecutando pueda causar.

2.2 Marco Conceptual

La seguridad informática es una preocupación constante de todas las organizaciones. Robo de datos, hackeos, malware y muchas otras amenazas son una de las tantas preocupaciones que mantienen sin dormir a los administradores de sistemas y profesionales de TI. Este artículo hablara de los conceptos básicos y mejores prácticas que muchos profesionales de TI usan para mantener sus sistemas protegidos.

¿Cuál es la meta de la seguridad informática? La seguridad informática sigue 3 conceptos fundamentales:

- **Confidencialidad**: La información solo debe de ser vista o utilizada por las personas autorizadas para tener acceso a ella.
- **Integridad**: Prevenir e identificar cualquier cambio a la información por un usuario no autorizado y los usuarios que lo lleguen a realizar deben de ser rastreados.
- **Disponibilidad:** La información debe estar disponible cuando los usuarios autorizados la necesiten.

En base a estos conceptos fundamentales, los especialistas en seguridad informática han creado mejores prácticas para ayudar a las organizaciones a proteger y salvaguardar la información.

En la actualidad, las redes sociales se convirtieron en la principal herramienta de comunicación a nivel mundial. Las más famosas entre ellas están: Facebook, Twitter, WhatsApp, Snapchat, Instagram, Pinterest, entre otras. Estas plataformas conectan a más de dos mil quinientos millones de personas a nivel mundial, siendo estas plataformas una de las herramientas tecnológicas más utilizadas a nivel mundial.

Según este análisis deducimos que mientras más acceso se tiene, existe un riesgo mayor y cuando existe un mayor riesgo, se tiene más necesidad de supervisar y controlar dichas plataformas.

Suplantación de Identidad

La suplantación de identidad ocurre cuando alguien toma los datos de una persona real y lo utiliza para hacerse pasar por la persona dueña de la información. La razón por la cual los ciber delincuentes realizan este tipo de acciones es para estafar, extorsionar, chantajear, entre otros.

Fraude, phishing y malware

¿Cómo los ciber delincuentes realizan sus ataques en las redes sociales? Generalmente los ciber criminales utilizan mensajes o publicaciones tentadoras que contienen enlaces con contenido malicioso.

Ciberbullying o acoso cibernético

Las personas más vulnerables a este tipo de ataques son jóvenes y adolescentes entre 12 y 17 años. Las mujeres son más propensas a sufrir este tipo de ataques y muchas veces la edad es irrelevante. Ciber bullying es maltrato, agresión u ofensas utilizando mensajes de texto, mensajes de voz, fotos, videos o audios colgados en las redes sociales. Este tipo de acción está afectando a millones de personas, en especial a gente joven.

Miedo a perderse algo (FOMO, fear of missing out)

Este tipo de expresión se denomina una nueva forma de ansiedad que ha surgido por el auge de los celulares smartphones y las redes sociales, que crea una necesidad en las personas de estar todo el tiempo conectadas. Básicamente es la preocupación que sienten las personas por eventos en las redes sociales, especialmente aquellos que no requieren nuestra presencia física para poder disfrutar de él. Es básicamente sentir la necesidad de saber que están haciendo los demás y no quieren perderse nada

Problemas legales

Las personas no saben que todo lo que dicen o publican en las redes sociales puede tener consecuencias legales. Por eso, es importante tener mucho cuidado con lo que publicamos en las redes sociales. Especialmente si lo utilizamos para insultar, difamar o crear rumores falsos.

2.3 Marco Espacial

La investigación será realizada en el marco de la ciudad de Santo Domingo, República Dominicana.

2.4 Marco Temporal

Esta investigación comprenderá el período de mayo-agosto de 2021.

Capítulo 3: RIESGOS Y CAUSAS POR LA QUE LOS USUARIOS COMPARTEN INFORMACION.

3.1 Análisis de riesgos

La forma en que la tecnología nos ayuda a adquirir productos y servicios

En el mundo hoy en día, nos vemos tan involucrados con la tecnología que todo lo que hacemos necesita tecnología de alguna manera, para ver televisión, para comunicarnos con seres queridos, sea por teléfono, video llamadas, notas de voz, mensajes de textos, correo electrónico, etc.

Igualmente, cuando vamos al supermercado, compramos con dispositivos que utilizan tecnología para realizar los pagos de nuestros consumos, tarjetas de créditos para pagar en el supermercado, para comprar artículos varios para el hogar, la gasolina, entre otros.

Igualmente, cuando queremos comprar un juego de muebles, juego de comedor, nevera, estufa, lavadoras y/o algún artículo de valor medio para nuestro hogar, la mayoría de las veces no utilizamos una forma de pago para saldar el valor del artículo en ese momento, sino que utilizamos entidades financieras para luego pagar por este artículo en una cantidad de cuotas X.

Y es que el mundo ha evolucionado tanto en temas de tecnología, que ya el método antiguo que existía para pagar por nuestros consumos ha ido quedando

obsoleto y cada día son más las empresas que entran en el modo del pago digital, dígase, tarjetas de crédito y/o transferencia a cuenta bancaria. Actualmente, por el tema de la pandemia, ocasionada por el COVID-19, muchas empresas de ventas masivas no tienen una tienda abierta al público para vender sus artículos, sino que crean una tienda online en el que sus clientes ingresan a su website, ven el listado de artículos disponibles por categoría, compran lo que desean y/o necesitan para satisfacer sus diferentes necesidades, y estas luego le envían dichos artículos a su casa u oficina.

Los bancos, por ejemplo, realizan depuraciones para obtención de crédito de manera remota, ya no es necesario ir a un banco para obtener un préstamo y/o tarjeta de crédito, con solo llamar y suministrar la información que se supone solo debe saberla el usuario, el banco puede emitir un préstamo y/o tarjeta de crédito, sin tener que desplazarse a la oficina bancaria para conseguirlo.

Lo mismo para solicitar un reemplazo de tarjeta de crédito, puedes llamar al banco, suministrar información que solo el cliente debe saber y el banco la envía a la dirección deseada.

Partiendo de lo anteriormente expuesto, podríamos decir que, si una persona comparte su información personal y confidencial a través de las redes sociales y/o alguna página web pensando que es válida, un delincuente informático

podría utilizar la tecnología que hoy existe para facilitarnos la vida, pero podría hacerle la vida muy difícil a una persona si logra obtener lo que anteriormente expusimos, utilizando, obviamente, el nombre de otra persona.

3.2 ¿Cuáles son los riesgos de compartir nuestros datos en las redes sociales?

En el caso de que un ciberdelincuente logre obtener nuestro nombre completo, fecha de nacimiento, dirección, número de teléfono, que logre tener acceso a nuestro correo electrónico, numero de cedula, lugar de nacimiento, como se llaman nuestros padres y donde estos nacieron, es información suficiente para llamar a un banco, solicitar resetear la contraseña de internet banking y agregar beneficiarios y retirar dinero de nuestra cuenta bancaria.

Cuando nos demos cuenta de que el cibercriminal retiró dinero de nuestra cuenta, ya el este habrá retirado el dinero de su cuenta y el banco no podrá reembolsarnos el dinero retirado. Tendremos que ir a la policía, al departamento del DICRIM para que investiguen el caso, pero mientras tanto, el dinero que fue retirado de nuestra cuenta sigue sin poder ser recuperado. En caso de que la policía logre atrapar al malhechor, esto no garantiza que el dinero será devuelto a nuestra cuenta, en resumen, perderemos dinero robado y perderemos tiempo y dinero tratando de que la policía capture a este malhechor.

Igualmente podría duplicar nuestra cedula, agregando su foto a la misma, ir a una tienda de electrodomésticos y pedir un crédito para comprar artículos, tal como lo haríamos nosotros mismos. Lo más triste de esta situación es que las entidades bancarias, en lo que el caso se investiga, se deben pagar los préstamos que este delincuente adquirió utilizando nuestro nombre, si no lo hacemos, dañará nuestro crédito en los diferentes buros de crédito.

Otra cosa que un ciberdelincuente podría hacer es llamar a un banco y solicitar un préstamo en nuestro nombre, el préstamo podría ser desembolsado a una cuenta a nuestro nombre, pero a la que el ciberdelincuente tiene acceso, el ciberdelincuente nunca pagara las cuotas del préstamo, entonces, en tres o cuatro meses el banco estará poniéndose en contacto con nosotros mediante las vías legales que pueda, para embargar nuestros bienes debido a la falta de pago de dicho préstamo, el banco podría, amparado por la ley, embargar nuestra casa, llevarse todas las cosas de valor en nuestro hogar, para recuperar parte del dinero desembolsado al ciberdelincuente a nombre de nosotros.

Podríamos decir que es injusto, pero es la manera en que los bancos operan. Mientras demandamos y ponemos una denuncia en la policía, el banco sigue cobrando, nuestro nombre estará manchado en los diferentes buros de créditos y hasta que no paguemos, no podremos recuperar nuestro buen nombre ante la sociedad.

Algo super peligroso a la hora de compartir información personal a través de internet, redes sociales, correos, etc. Es que cuando un ciberdelincuente nos convence de que compartamos información confidencial por la vía que la pida, si llegamos a compartir nuestra información de tarjeta de crédito, este podría utilizarla para realizar compras por internet a nuestro nombre, mientras tanto, y en lo que el banco investiga, igualmente debemos pagar por dichos consumos.

Algo que también podría hacer un ciberdelincuente es solicitar nuevas tarjetas de crédito a nuestro nombre, realizar igualmente compras y no pagarlas, mientras tanto debemos pagar todas esas cuentas, si llega a darse el caso de que las autoridades logren atrapar al ciberdelincuente, debemos pagarle al banco los cargos que el ciberdelincuente consumió haciéndose pasar por nosotros y que atrapen al ciberdelincuente no garantizara que se recuperara el dinero robado.

Algo también que el ciberdelincuente puede lograr al utilizar nuestros datos personales es simplemente ir a una compañía telefónica, comprar un teléfono celular a nuestro nombre y no pagarlo, dañará nuestro crédito. Otra cosa que podría también hacer un ciberdelincuente es robar nuestra información de seguro médico e ir a una clínica y obtener servicios médicos a nuestro nombre. Podría obtener beneficios de medicinas en farmacias utilizando nuestro nombre.

Algo muy importante es que, al tener nuestra identidad de manera fraudulenta, es que podría ser apresado y utilizar nuestro nombre, en resumen, podríamos quedar manchados en la justicia, solo porque un ciberdelincuente obtenga nuestros datos personales, que logre reproducir nuestra cedula. Igualmente podría tener una licencia de conducir, tener infracciones de tránsito a nuestro nombre y en lo que se investiga el caso, debemos también pagar por ellas.

3.3 Causas por las que los usuarios comparten información confidencial en las redes sociales, páginas webs y correo electrónico.

Las causas por las cuales las personas comparten información confidencial en las redes sociales, páginas web y correo electrónico varía dependiendo del tipo de persona. Muchas personas lo hacen por ignorancia, otros lo hacen porque no creen que alguien sería capaz de hacerles daño, algunos confían en la tecnología y creen que esta es lo suficientemente segura como para evitar que caiga en manos equivocadas, pero no es así.

Una de las razones por las cuales las personas comparten su información personal o que se pueden ver compelidos y/o convencidos a hacerlo es al recibir un correo electrónico de una persona haciéndose pasar por una organización de renombre, convencen a la víctima para que comparta su información personal a cambio de ofrecer más información concerniente al caso que expone, lo hacen para hacerle creer a la víctima que necesitan confirmar que él es la persona con la cual ellos desean expresar la magnífica noticia que le tienen.

Lo hacen haciéndose pasar por entidades bancarias, organizaciones sin fines de lucro ofreciéndole dinero para que abra una entidad sin fines de lucro, también se hacen pasar por bancos ofreciéndoles dinero prestado o una suma de dinero que necesitan transferir a la cuenta de la víctima pero que necesitan sus datos para poder proceder con dicha transferencia.

También, existen organizaciones malintencionadas que atacan grandes empresas que contienen bancos de datos con información confidencial de muchos usuarios, por ejemplo, podrían atacar a una tienda de ventas al detalle, la cual tiene una base de datos con millones de usuarios en la cual obtienen información básica como sus nombres completos, dirección, número de teléfono, fecha de nacimiento, entre otros, y que podría ayudarles a ellos a formar un perfil de las personas que desean atacar.

La causa más común por lo que las personas comparten su información personal es al recibir un correo electrónico informándoles que se han ganado una suma muy alta de dinero y que necesitan sus datos personales para poder transferir dicha suma a sus cuentas bancarias. La persona que ignora la frase muy popular que dice, si es muy bueno para ser verdad, entonces no es verdad, el usuario entonces procede a creer en lo que dice el correo y enviar todos sus datos personales como su nombre completo, dirección, teléfono, fecha de nacimiento, numero de cedula, lugar de nacimiento, etc. Que es más que

suficiente para que un ciberdelincuente logre obtener múltiples beneficios a nombre de su víctima.

Mas abajo podemos ver un ejemplo de correo electrónico en el cual el ciber atacante solicita información confidencial al usuario:


Bank Name: SunTrust Bank
Contact Person: Mary Alken
General Auditor
E-mail: maryaiken.frs04@accountant.com

Provide the following information below to the bank for processing and remittance of your payment.
Full name:.....
Age : .....
Occupation: .....
Address:.....
Mobile number:.....
Home Phone#: .....

Figura 1: Ejemplo 1 de cibercriminales.

En el correo más arriba, podemos ver que el ciberdelincuente se está haciendo pasar por una entidad bancaria de renombre y le está pidiendo al usuario todos sus datos personales más importantes para luego utilizarlos confines maliciosos como obtener préstamos bancarios, comprar teléfonos celulares en línea, realizar solicitudes de tarjetas de crédito, entre otros.

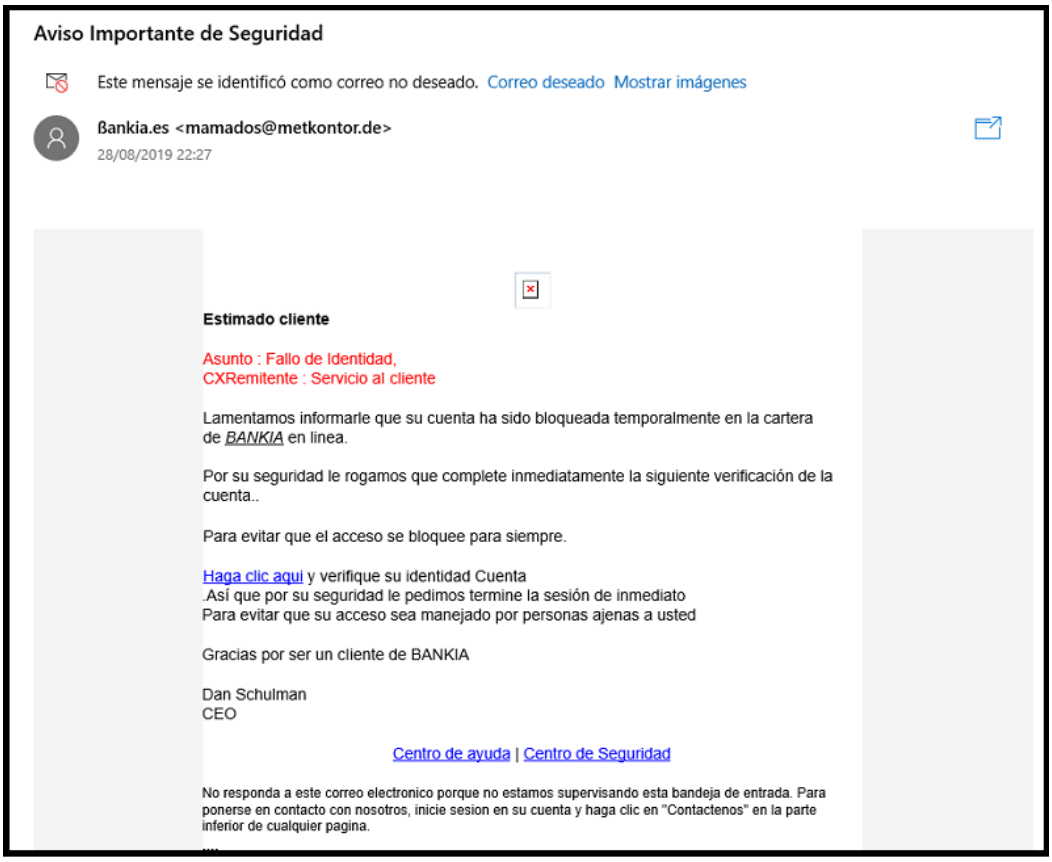
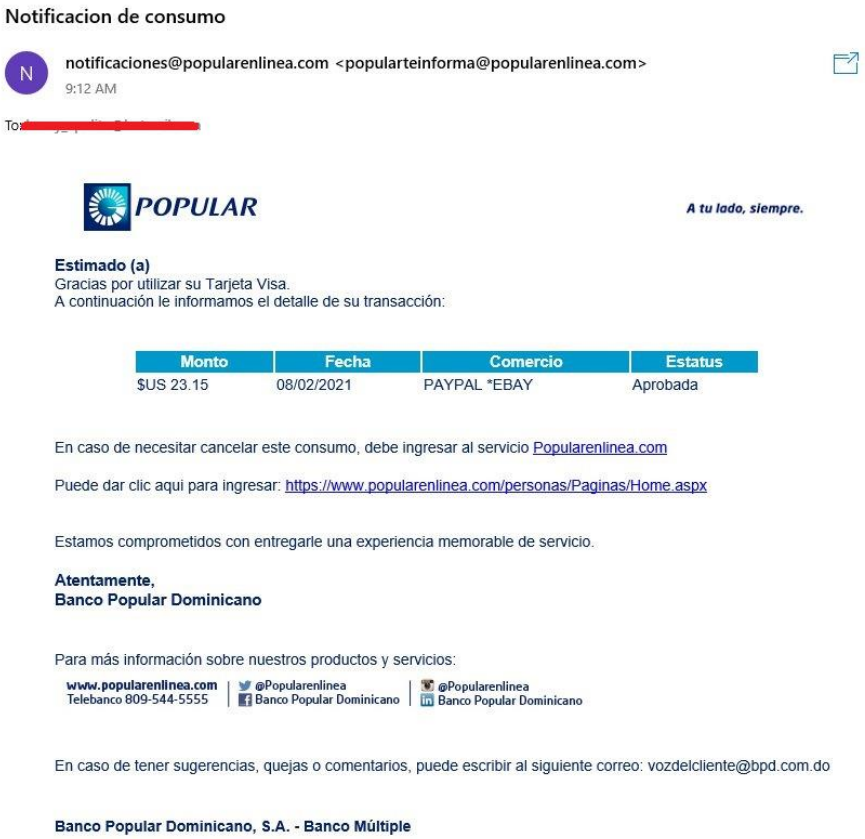


Figura 2: Ejemplo 2 de cibercriminales.

Otra forma muy común de los ciberdelincuentes obtener nuestra información personal es la de convencernos de hacer clic de páginas webs fraudulentas para luego solicitar que nosotros llenemos un formulario web con nuestros datos personales. En el correo de ejemplo más arriba, se puede ver como este correo se hace pasar por una entidad bancaria y nos quiere convencer de que hagamos clic en un enlace para validar nuestra información personal.

Una de las formas muy populares que los ciberdelincuentes están utilizando hoy en día es el envío de correo fraudulento con fines de robar información personal, especialmente los accesos a banca por internet. Podemos ver más abajo un correo

fraudulento haciéndose pasar por el Banco Popular Dominicano, en el cual le indican a su víctima que su tarjeta de crédito fue utilizada recientemente y le dicen a su víctima que para poder cancelar esa transacción deben hacer clic en un enlace fraudulento que ellos proporcionan. En la segunda imagen podemos ver que abre una página fraudulenta del Banco Popular pidiendo su usuario y contraseña.



Notificacion de consumo

N notificaciones@popularenlinea.com <popularteinforma@popularenlinea.com>
9:12 AM

To: [redacted]

POPULAR A tu lado, siempre.

Estimado (a)
Gracias por utilizar su Tarjeta Visa.
A continuación le informamos el detalle de su transacción:

Monto	Fecha	Comercio	Estatus
$US 23.15	08/02/2021	PAYPAL *EBAY	Aprobada

En caso de necesitar cancelar este consumo, debe ingresar al servicio Popularenlinea.com

Puede dar clic aqui para ingresar: https://www.popularenlinea.com/personas/Paginas/Home.aspx

Estamos comprometidos con entregarle una experiencia memorable de servicio.

Atentamente,
Banco Popular Dominicano

Para más información sobre nuestros productos y servicios:
www.popularenlinea.com | @Popularenlinea | @Popularenlinea
Telebanco 809-544-5555 | Banco Popular Dominicano | Banco Popular Dominicano

En caso de tener sugerencias, quejas o comentarios, puede escribir al siguiente correo: vozdelcliente@bpd.com.do

Banco Popular Dominicano, S.A. - Banco Múltiple

Figura 3: Clonación de página web.

Figura 4: Clonación de página web.

Luego de que la persona ingresa su usuario y contraseña, el ciberdelincuente solicita que el usuario valide el tipo de dispositivo de segundo factor de seguridad.

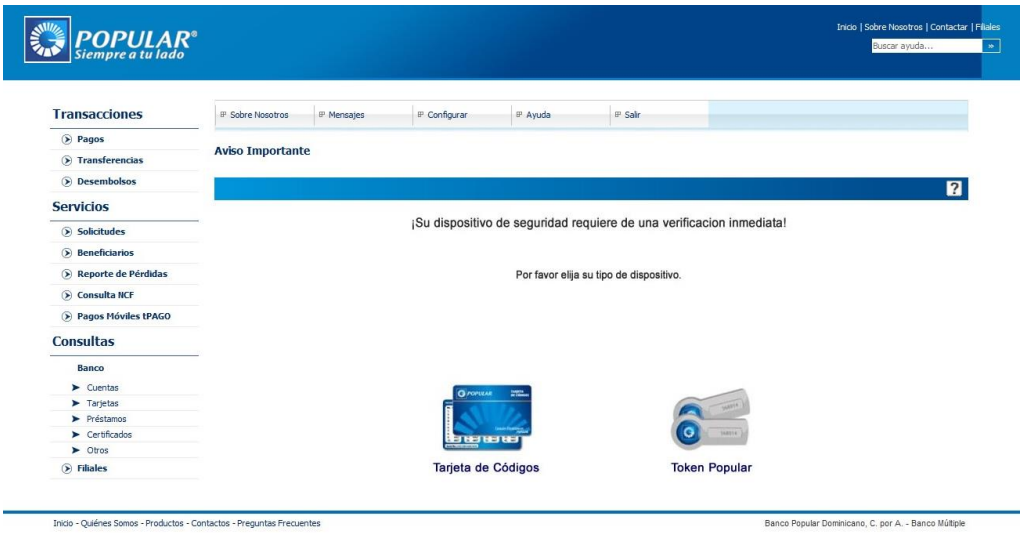


Figura 5: Clonación de página web.

Aquí luego podemos ver como el ciber delincuente pide el ingreso de todos los códigos de la tarjeta de códigos, y le solicita luego que digite toda la información para luego utilizarla a su favor, retirar fondos, solicitar préstamos, desembolsarlos y transferirlos a la cuenta del ciberdelincuente, solicitar tarjetas de créditos y luego utilizarlas para realizar compras fraudulentas.

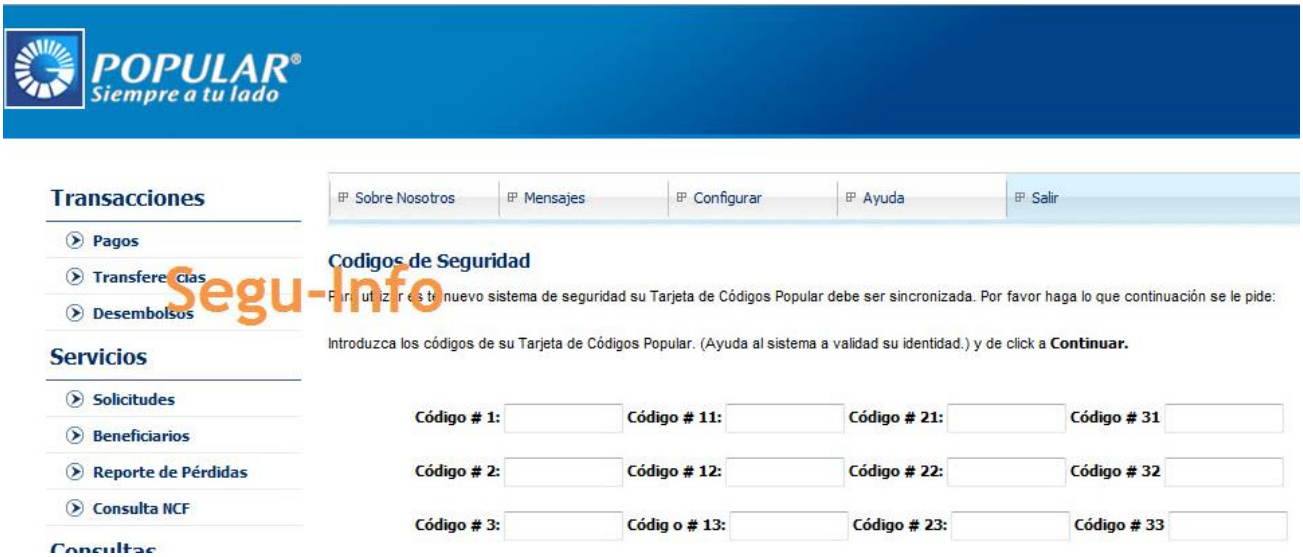


Figura 6: Clonación de página web.

Capítulo 4: ANÁLISIS Y DISEÑO DEL SISTEMA

4.1 Análisis y Diseño del Sistema.

4.2 Definición de los objetivos del sistema.

Para realizar un correcto análisis del sistema, primero se deben especificar los objetivos que se persiguen con la implementación de este, para luego desglosar dichos objetivos en términos de análisis y diseño de software. En este caso, los objetivos que se buscan conseguir con la implementación de este sistema son los siguientes:

- Protege las acciones de los usuarios sin importar el tipo de dispositivos que estos estén utilizando, reduciendo con esto la posibilidad de sufrir un ataque cibernético.
- Detectar y bloquear de manera instantánea las amenazas que afectan directamente a los usuarios
- Permitir la navegación de los usuarios de manera eficiente y protegida
- Reducir los riesgos de enviar información personal al proteger las actividades de los usuarios.
- Dotar a los usuarios de una protección avanzada, ofreciendo conexiones seguras para el correo electrónico y las redes sociales. Logrando así ofrecer un escudo protector, que sea muy difícil de penetrar para los ciberdelincuentes.

Flujograma de Filtrado de Información

Los requisitos funcionales son aquellos que describen el comportamiento del sistema, mencionando cómo debe reaccionar el mismo ante ciertas entradas, así como también las salidas que debe producir. En ese sentido, para la definición de requisitos funcionales del sistema, se representó un flujo de información para proyectar las acciones que tomaría la herramienta al momento de identificar el siguiente tipo de información:

- Datos Buenos Conocidos
- Datos Malos Conocidos
- Cancelación de ruido
- Publicidad no deseada

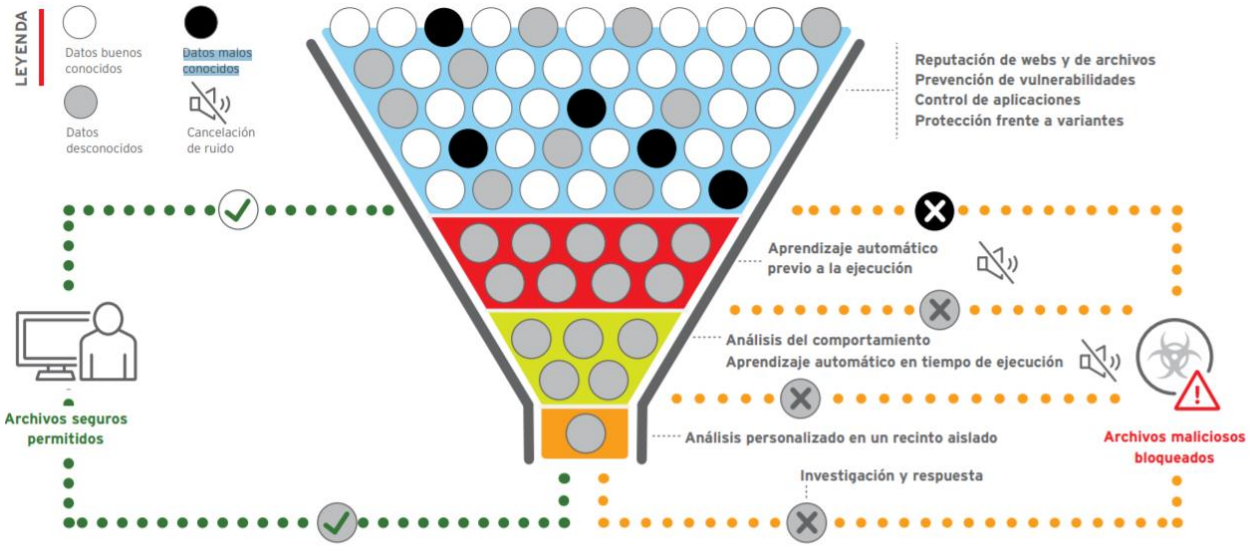


Figura 7: Flujo grama de filtrado de la información.

- **Máxima Seguridad.** La seguridad que ofreceremos estará dotada de un sistema con inteligencia artificial y técnicas de defensas ante todo tipo de amenazas, ofreciendo así una máxima protección para los usuarios. Contará igualmente, con tecnología de Machine Learning, el cual se encargará de analizar análisis en tiempo real, antes, durante y luego de la ejecución, esto nos llevará a tener una detección más precisa.

- **Protección 360 contra todo tipo de amenazas**. Incluye una protección Incluye una amplia gama de protección integrada en pasarelas, puntos de conexión, dispositivos móviles y las aplicaciones de redes sociales. Conseguirá múltiples capas de funciones contra amenazas en toda su red para protegerla incluso frente a las amenazas más recientes.

- **Seguridad interconectada**. Te protege automáticamente contra amenazas locales y bloquear igualmente ataques emergentes.

- **Protección de la información confidencial.** Evita la perdida de información confidencial, protegiendo la información cifrándola a la hora de almacenarla e igualmente al transmitirla. Logrando con esto que solo las personas autorizadas puedan ver la información confidencial. Igualmente cuenta con un bloqueo para evitar que la información sea enviada a destinatarios de procedencia dudosa.

- **Administración de la seguridad del usuario.** Capacidad para administrar los niveles de seguridad desde una consola administrativas, en la que se pueden analizar los datos y las amenazas de una forma eficiente.

4.3 LISTADO DE FILTROS

Con las listas de filtro puedes elegir qué elementos bloquear y que elementos permitir. Puedes también elegir listas de filtros previamente configuradas y también puedes crear tus propias listas. Igualmente puedes customizar las listas preexistentes, puedes cambiar, agregar y quitar.

La mayoría de la publicidad que aparece en internet contienen material no deseado y en la mayoría de los casos contienen malware que sustraen información personal y confidencial de los usuarios. Muchas páginas webs igualmente están infectadas sin que los dueños de dichas paginas lo sepan. Esto aumenta el riesgo de pérdida de información. Con el listado de filtros este tipo de amenazas igualmente quedan bloqueados dentro de los filtros predeterminados.

4.3.1 Listas de filtros predeterminadas

Al momento de instalar la aplicación las siguientes listas de filtros se activan de manera automática:

4.3.2 Anuncios en lista negra

Una lista de filtros que bloquea anuncios (por ejemplo, Lista Fácil) lista que proporcionamos de manera automática una vez se instala la herramienta, dicha lista se actualiza de manera recurrente adicionando lista de direcciones de internet categorizadas como sospechosas.

4.3.3 Anuncios aceptables

Esta lista permite que el usuario pueda ver anuncios que no comprometan sus datos personales confidenciales. En caso de que desees bloquear todos los anuncios, solo debes hacer click en la configuración necesaria para lograrlo. Igualmente puedes modificar esta lista de manera automática al permitir y bloquear los anuncios antes de que se muestren.

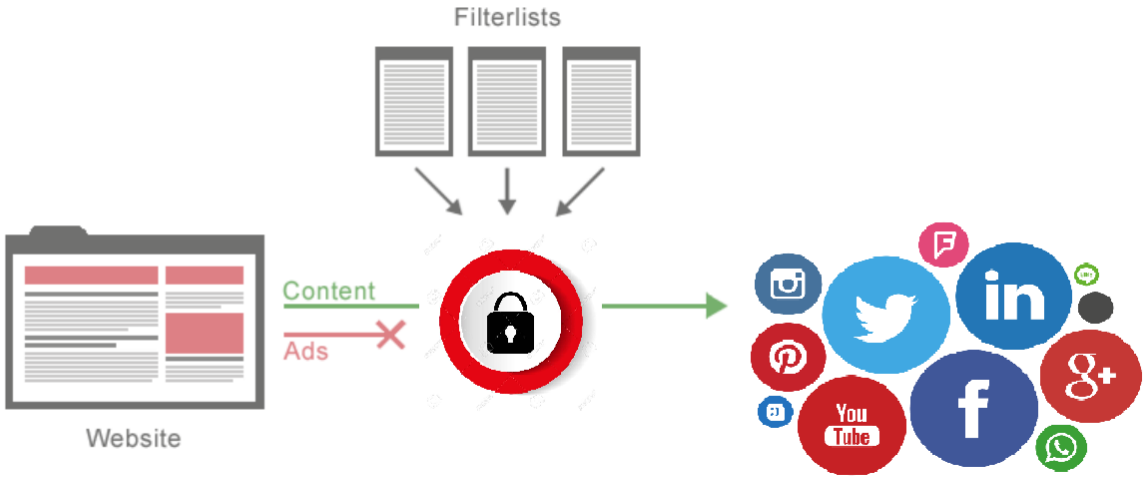


Figura 8: Anuncios aceptables.

UNA SEGURIDAD MÁS RÁPIDA E INTELIGENTE CON DEFENSA FRENTE A AMENAZAS CONECTADA

La herramienta cuenta con una solución multicapa integrada con “VirusTotal” el cual es un sitio web que proporciona de forma gratuita el análisis de archivos y páginas web y aplicaciones a través de antivirus, esto permite detectar vulnerabilidades, puntos de conexión, igualmente ofrece protección contra amenazas utilizando diferentes técnicas de protección.

A continuación, un mapa de la función de detección de amenazas conectadas en tiempo real:

Figura 9: Mapa de la función de detección de amenazas conectadas en tiempo real.

4.4 ¿QUÉ OFRECE LA HERRAMIENTA?

La herramienta ofrecerá varias funcionalidades las cuales estarán disponibles una vez sea instalada en cualquier dispositivo.

4.4.1 Protección Avanzada

La aplicación utiliza un sistema de aprendizaje automático para detectar nuevas amenazas y bloquearlas de manera automática. Detectando a su vez actividades maliciosas en las redes sociales, páginas webs, etc. Los sitios webs sospechosos son bloqueados automáticamente, igualmente las aplicaciones maliciosas que se encargan de capturar información personal confidencial son

bloqueadas por igual. Una novedosa funcionalidad es que se puede activar una contraseña especial para modificar las listas de filtro. Ofreciendo así un mayor control en cuanto a la privacidad de los datos confidenciales del usuario.

4.4.2 Antivirus

Protege los dispositivos de los usuarios para evitar y neutralizar software malicioso.

- **Antivirus en tiempo real.** Analiza permanentemente tus dispositivos para encontrar virus, gusanos, troyanos, “criptolockers”, “rootkits” y “spyware”: te protege tanto de amenazas en línea determinadas como nuevas.

- **Prevención automática de exploits.** Verifica las vulnerabilidades de red confusas en el dispositivo. Esto incluye la detección de las vulnerabilidades “EternalBlue” y “SMBloris”, las cuales pueden bloquear sistemas.

- **Removedor de troyanos.** Detecta y remueve virus troyanos y gusanos de Internet que hacen que tus dispositivos sean lentos sus dispositivos. Esto se realiza automáticamente, por lo que no es necesario editar manualmente los archivos del sistema.

- **Detección al instante de amenazas.** Provee un análisis ininterrumpido de archivos, aplicaciones y páginas web en tiempo real en tus dispositivos móviles y PC. Logrando con esto proteger tus datos al detectar las amenazas de manera rápida y efectiva.

4.4.3 “Antispyware”

El motor antispyware te informa sobre spyware encontrado en el dispositivo mientras navegas en la web o mientras visualizas las redes sociales. Con esto logramos detener las aplicaciones y páginas webs maliciosas que tratan de capturar tu información confidencial.

4.4.4 Sistema anti-hackeo

Bloquea el acceso no autorizado a tu información personal confidencial al evitar igualmente el secuestro de tus dispositivos

- **Corta fuegos bidireccionales.** Evita que personas no autorizadas ingresen a tu equipo y/o red de manera remota sin tu previa autorización. Al igual que reporta las conexiones salientes y entrantes en tus dispositivos. Bloqueando las que no deseas y permitiendo las que si deseas tener, garantizando así que solo conexiones que desees sean las que se mantengan.

- **Protección de pagos.** En vista que sobre las redes sociales hay mucho “marketing” que te desvía hacia un navegador, la herramienta ofrecerá protección encriptando la información de tráfico de información de nivel bancario cuando realizas una transacción en línea evitando que los hackers puedan interceptar tus datos de tarjeta de crédito y financieros.

- **Anti ransomware.** Inspecciona tu dispositivo en tiempo real para identificar actividad que coincida con los patrones y el comportamiento confirmados del “ransomware”. Esto permite bloquear al instante la actividad sospechosa y evitar que los ataques de ransomware te impidan acceder a tus equipos.

- **Bloqueo de aplicaciones.** Te ayuda a proteger las aplicaciones en todos tus dispositivos y bloquea los ataques maliciosos. Tan pronto una aplicación es bloqueada, la única forma de desbloquear dicha aplicación es mediante un PIN privado, con un patrón de desbloqueo o utilizando autenticación biométrica.

4.4.5 Protección de alta tecnología

Análisis avanzado para detectar “malware” sin archivos y amenazas de día cero.

- **Detector de vínculos maliciosos**. Bloquea las páginas webs maliciosas al momento de abrirlas, antes de estas páginas abrir, se hace un escaneo y se determina si la página es segura o no.

- **Defensor “ antimalware”**. Protección contra una gama de “malware” peligrosos y sofisticados, como el “malware” “sin archivos” que se escribe directamente en la RAM del dispositivo en lugar de estar en la memoria de almacenamiento.

- **Control de aplicaciones**. Bloquea las aplicaciones de poca confianza a los datos personales confidenciales de los usuarios. Protegiendo de esta manera la información confidencial de los usuarios.

4.4.6 Protección de privacidad

Encripta los datos personales, los datos de navegación y evita que los cibercriminales espíen tus actividades online.

- **VPN rápida e inteligente.** Encripta la información enviada e igualmente la información es recibida con cifrado AES de 256bits. Esto impide que los ciberdelincuentes vean tu información personal. Igualmente oculta la IP original y no pueden de esta forma rastrear tu ubicación.

- **Protección contra phishing.** Evita que ingreses a páginas web falsa, que fueron creadas con la única intención de capturar información de los usuarios, robando así información confidencial importante. Igualmente recibirá alertas en el momento que la página web visitada no sea de confianza.

- **Navegación privada.** Evita que las páginas web y las redes sociales hagan un seguimiento de tus actividades y recopilen información personal confidencial.
- **Protección de cámara web.** Bloquea el acceso no autorizado a la cámara web de tus dispositivos. Con esto logramos mayor privacidad del lado del usuario. En caso de que una aplicación, programa, o página web desee acceder a tu cámara, recibirás un aviso para permitir o denegar dicho acceso.

4.4.7 Herramienta antirrobo

Si pierdes tu dispositivo tableta, computadora, teléfono, las funciones antirrobo se pueden activar de forma remota, con esto podrás activar una alarma y obtener una foto de identificación del usuario que lo está usando actualmente. Las funciones antirrobo también bloquean el dispositivo, te permite conocer su ubicación actual y realizar un restablecimiento completo para garantizar que los datos confidenciales se borren del dispositivo eliminando así el riesgo de robo de información por dispositivo perdido.

4.4.8 Protección extendida.

Funciones de protección para tus dispositivos conectados a una red Wi-Fi y periféricos.

- **Administrador de contraseñas.** Protege las contraseñas, tarjetas bancarias y documentos confidenciales en una carpeta cifrada que solo puede desbloquearse con una contraseña. Adicionalmente, genera contraseñas seguras protegiendo con esto, la privacidad de los usuarios.

- **Defensor contra ataques de red.** Analiza la actividad del tráfico entrante para detectar indicios de ataques de red en tus dispositivos. Tras detectar un ataque, bloquea la actividad de red del equipo atacante durante una hora y le envía una alerta con la opción de bloquearla por más tiempo.

- **Bloqueador de anuncios.** Bloquea los molestos banners de sitios web y otros tipos de publicidad que puedan ser maliciosa aparezcan en tu dispositivo. En caso de que desees recibir publicidad de sitios específicos, puedes ponerlos en una lista de páginas webs admitidas para seguir viendo la publicidad cuando los visites.

- **Protección contra keyloggers.** Bloquea de manera automática los keyloggers y evita que registren pulsaciones del teclado de tu dispositivo,

protegiendo así tus contraseñas, datos bancarios y cualquier tipo de información confidencial personal que escribas con el teclado de tu dispositivo.

4.5 MODELO DE IMPLEMENTACIÓN DE LA HERRAMIENTA Y DIAGRAMAS DE ARQUITECTURA

4.5.1 Descripción general de la configuración del entorno

Como parte de la configuración del entorno para la implementación de la herramienta, puede determinar la URL del entorno y el inicio de sesión. Credenciales, generar certificados para administrar ciertas plataformas, configurar telecomunicaciones, configuraciones de privacidad, personalizar la consola de administración de los usuarios entre otras cosas.

4.5.2 Certificados APN para el servicio de notificación

Para administrar los dispositivos con el agente de la herramienta, primero deben obtener un certificado del Servicio de notificaciones “push de notifications” (APN). Un certificado APN que le permitirá a la herramienta comunicarse de manera segura con los dispositivos móviles para así tener una comunicación bidireccional.

Dichos certificados APN serán válido por un año para luego ser renovad, en ese sentido la consola de administración enviará un recordatorio a través de notificaciones a medida que se acerca la fecha de vencimiento para el usuario solo acepte la notificación de actualización.

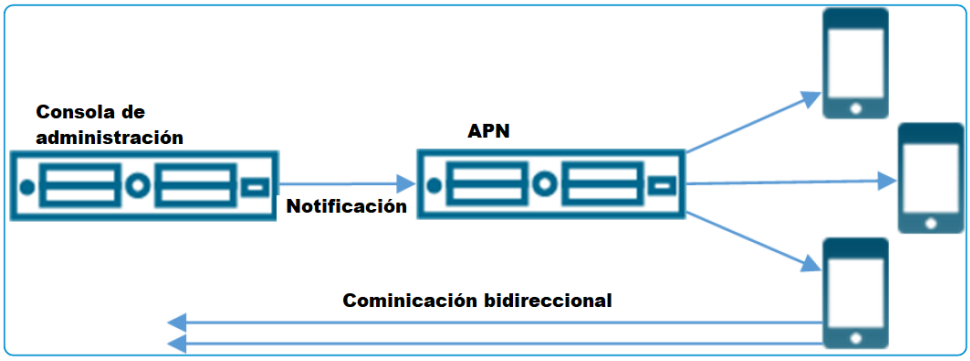


Figura 10: APN.

4.6 DESCRIPCIÓN GENERAL DE CUENTAS DE USUARIO Y ADMINISTRACIÓN DE LA HERRAMIENTA

La herramienta permitirá establecer una infraestructura de administración y usuarios completa proporcionando las opciones de configuración, autenticación, uso para el público en general, integración empresarial y mantenimiento continuo de todo el ambiente de gestión de la herramienta.

4.6.1 Autenticación de los usuarios en la herramienta

Antes de que se pueda inscribir cualquier dispositivo, cada usuario del dispositivo debe tener una cuenta de usuario auténtica que sea reconocida por la herramienta. El tipo de autenticación de usuario que elija depende de las necesidades que el mismo tenga al momento de instalar la aplicación en su dispositivo.

4.6.2 Autenticación de usuario

La herramienta identificará los usuarios en la arquitectura de la herramienta iniciando sesión mediante el uso de la interfaz de programación de aplicaciones "API" de su cuenta de correo de iCloud, Microsoft Exchange, G-mail y Outlook donde automáticamente quedará autenticado.

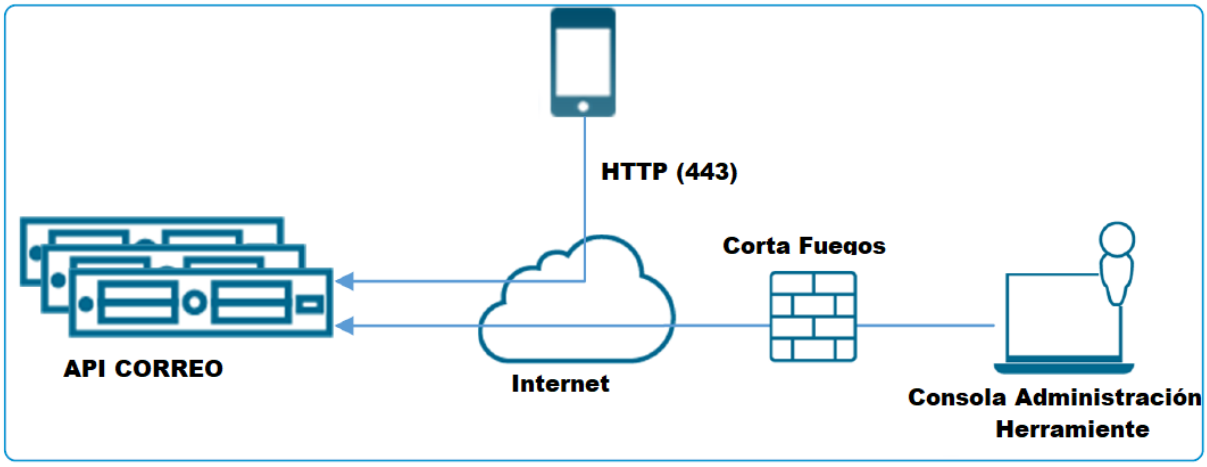


Figura 11: Autentificación de usuario.

4.6.3 Cortafuegos y zona desmilitarizada “DMZ”

Para minimizar los riesgos derivados de un servidor con acceso desde Internet que pudiera comprometer la seguridad de la infraestructura, se utilizará dos cortafuegos y una red local denominada **zona desmilitarizada o DMZ** (por su traducción del inglés, *Demilitarized Zone*).

Implementaremos un cortafuegos para filtrar el tráfico de información entre la **zona desmilitarizada o DMZ** y la red interna y otro cortafuegos para filtrar la información entre la red pública y la DMZ.

4.6.4 Servidor de administración de la consola

Emplearemos un servidor principal para instalar la herramienta.

4.6.5 Servidor WSUS de Virus Total

Utilizaremos un servidor WSUS para gestionar las actualizaciones de patrones de virus, amenazas y vulnerabilidades proporcionadas por el sitio web gratuito **VirusTotal**, manteniendo así los agentes de la herramienta instaladas en los dispositivos actualizadas en línea y en tiempo real.

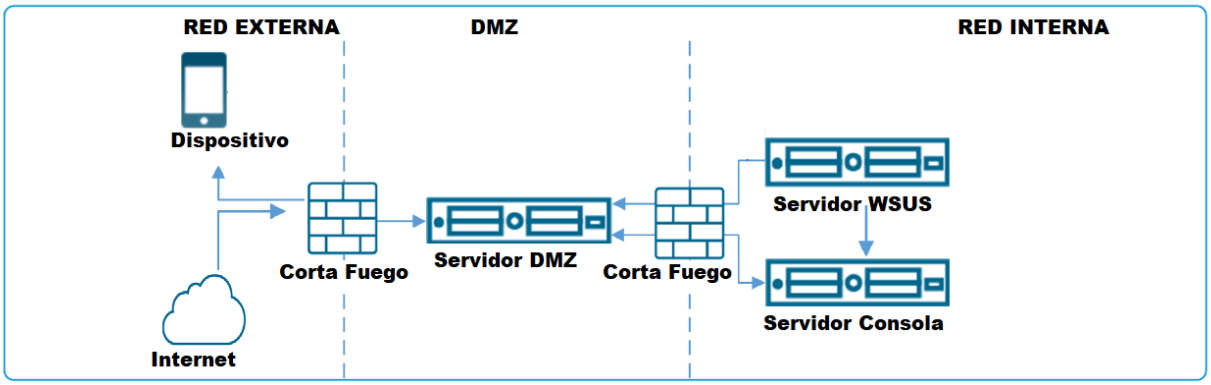


Figura 12: Servidor WSUS de Virus Total

4.7 REQUERIMIENTO DE ESPECIFICACIONES DEL SOFTWARE

4.7.1 Requisitos Funcionales

- Debe iniciar sesión con una cuenta de correo de iCloud, Microsoft Exchange, G-mail y Outlook donde automáticamente quedará autenticado
- Utilizará el GPS del dispositivo para ubicación en tiempo real
- Escaneo en tiempo real
- Alerta de nuevas amenazas detectadas
- Alerta de nuevas amenazas eliminadas
- Permitirá el registro de varios dispositivos con una misma cuenta de usuario
- Portal web de administración personalizada para el usuario
- Reporte recurrente de las estadísticas de las actividades de gestión de amenazas durante la navegación en las redes sociales.

4.7.2 Requisitos de Recursos de Software

A partir de los objetivos del sistema especificados, se deben definir los requisitos de software del dispositivo para que la herramienta funciones de manera eficiente.

- Sistema operativo IOS y Android
- Memoria RAM del dispositivo mínima 512 MB
- Pantalla táctil (mínimo 480x800px)

- Procesador: 500+ MHz ARM7 y posteriores
- Conexión a Internet

4.7.3 Requisitos de Interfaz gráfica

Interfaces de usuario

La interfaz gráfica de la aplicación tendrá disponible varias opciones que se ajustarán a la necesidad de los usuarios.

- **Catálogo de Filtros:** Las listas de filtros son conjuntos de reglas que le dicen a tu aplicación qué elementos bloquear. Puedes bloquear tan poco o tanto como quieras y sea necesario. Elige entre listas de filtros ya preparadas, mantenidas externamente o crea las tuyas. Casi todas las listas de filtros ya preparadas son creadas, publicadas y mantenidas por los usuarios para los usuarios que hacen uso de las principales redes sociales

- **Protección de Documentos:** Opción que escanea y categoriza el tipo de documento que esté alojado en dispositivo para proporcionar protección. Si se trata de extraer algún documento sin autorización del usuario el mismo se volverá corrupto por el tipo de encriptado que proporciona la herramienta

- **Dispositivo Protegido:** El dispositivo se mantendrá protegido durante la navegación del usuario por las redes sociales

- **Opciones de Seguridad:** Las opciones de seguridad le permitirán al usuario modificar las acciones que se llevarán a cabo ante la detección de alguna actividad sospechosa

- **Centro de Notificaciones:** El usuario verá todas las alertas disponibles, acciones a tomar, amenazas detectadas, bloqueadas y borradas

- **Soporte Usuarios:** Centro de soporte disponible para el usuario donde podrá encontrar todo lo referente a aplicación

- **Catálogo de Redes Sociales:** Cuenta con varias opciones:

    - **Aplicaciones:** Listado de todas las redes sociales de las cuáles la herramienta ofrece protección, el usuario solo tendrá que entrar al catálogo y seleccionar la red social que está usando en su dispositivo y descargar el paquete de protección
    - **Aplicaciones Instaladas:** Donde se visualizarán las aplicaciones instaladas

- **Actualizaciones:** Centro de actualización de las aplicaciones instaladas
- **Buscador:** Para buscar las aplicaciones de redes sociales disponibles en la herramienta

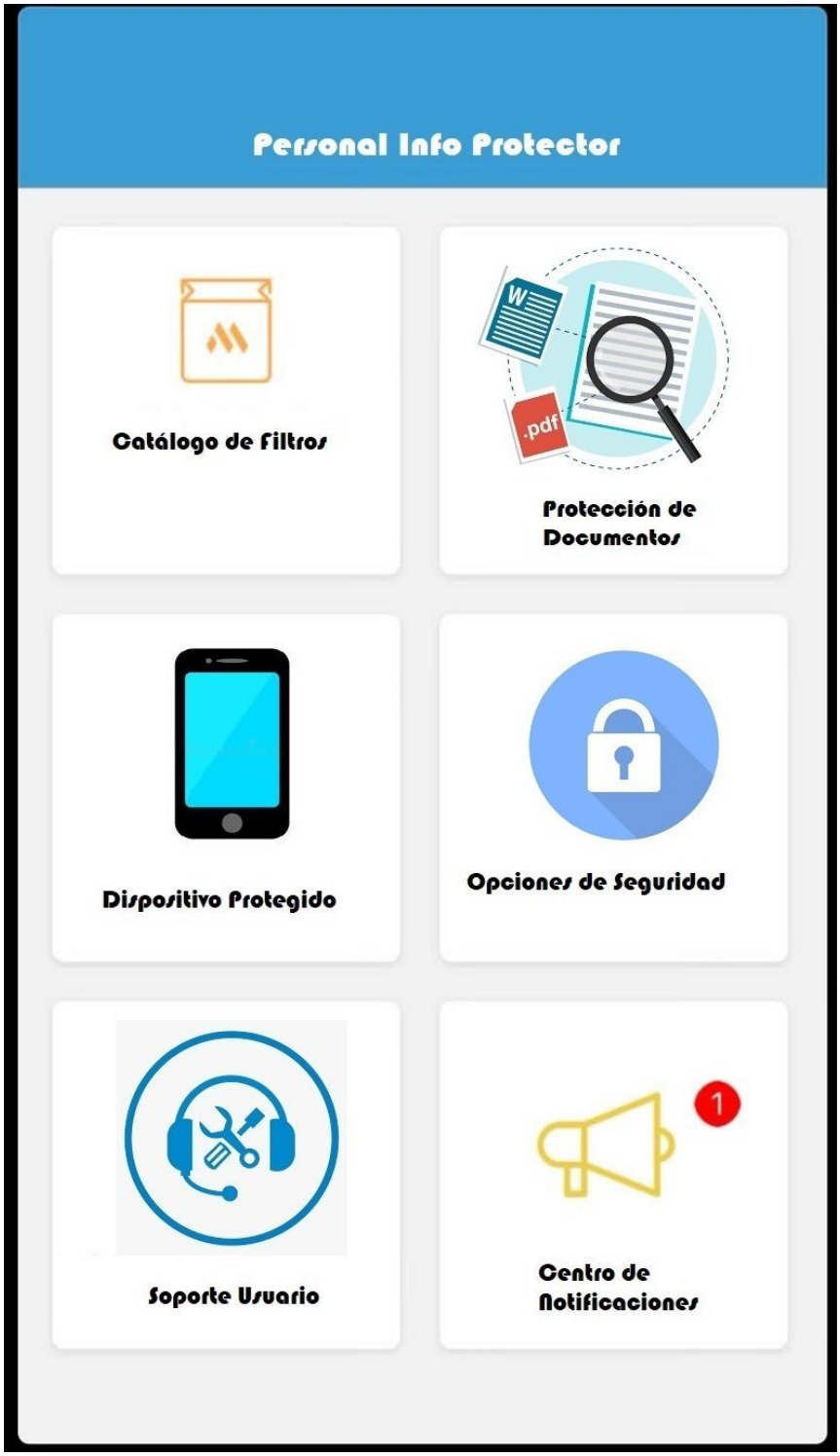


Figura 13: Interfaces de Usuarios

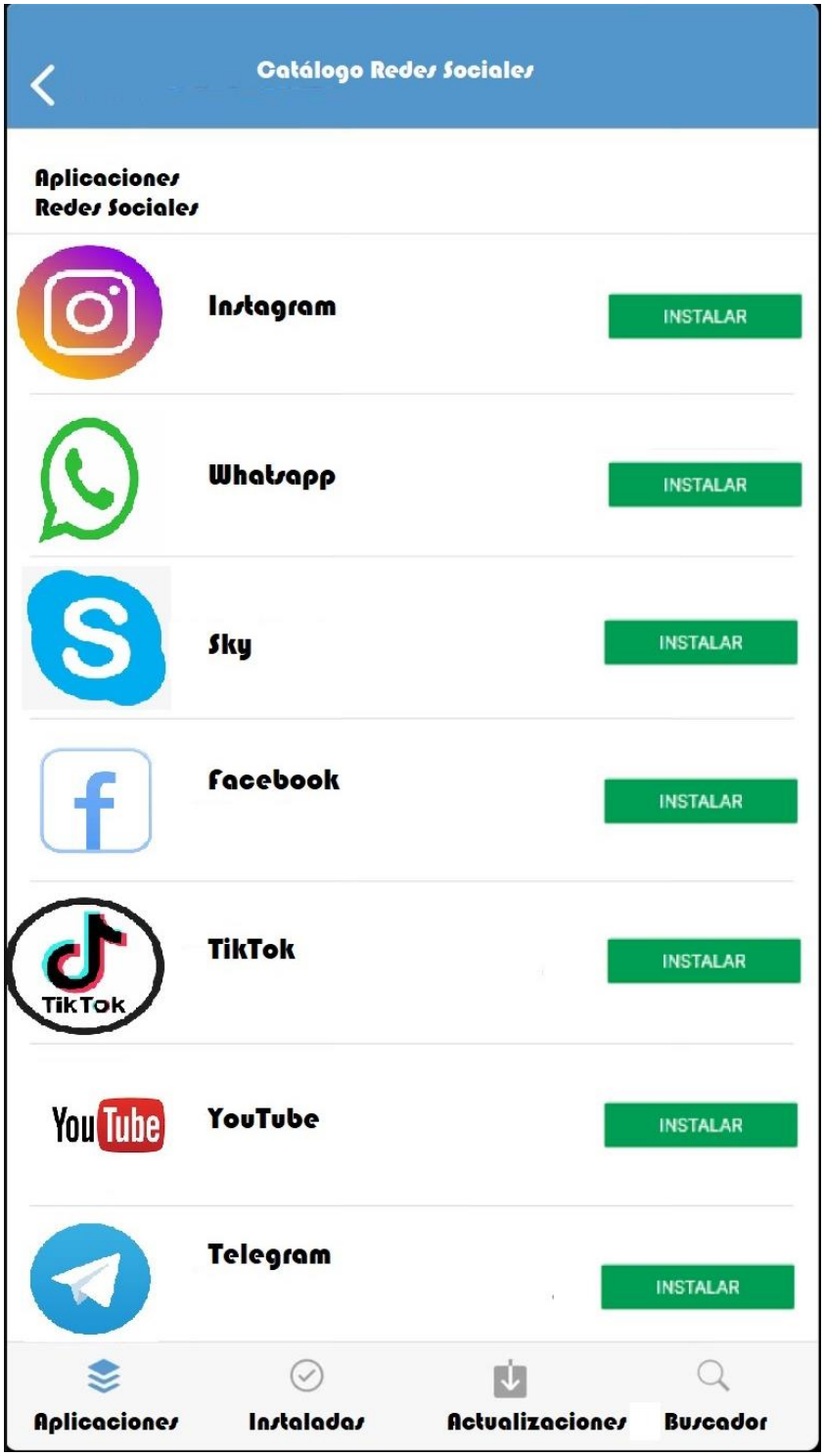


Figura 14: Interfaces de Usuarios

Capítulo 5: MITIGACION DE LOS RIESGOS

5.1 INFORMACION

5.1.1 Concepto.

La información en la actualidad es como si fuera un grupo o conjunto de datos organizados importantes para una o más personas que extraen de ahí algún tipo de conocimiento, es decir la información es la guía fundamental que a través del conocimiento que nos brinda nos permite resolver problemas y nos ayuda a tomar decisiones en momentos difíciles, ya que su aprovechamiento racional es la base del conocimiento.

5.1.2 Tipo de información

Actualmente la información se puede clasificar en forma distintas, de acuerdo a numerosos criterios que existen, por tal razón estaremos brindándole una breve clasificación de ellos como tal.

Información confidencial o clasificada: este tipo de información es al cual le haremos más énfasis en este proyecto, la información confidencial como su nombre lo dice es aquella información la cual solo puede tener acceso un pequeño número de personas, dada la naturaleza que este tipo de información siempre es peligrosa, secreta, y muy delicada.

Información pública: esta información es todo lo contrario a la confidencial debido a que en esta si tienen acceso un gran número de

personas, tal como su nombre lo dice publica quiere decir que sin requerir ningún tipo de permisos cualquier persona puede acceder a ella.

Información personal: este tipo de información es muy delicada, porque las informaciones personales hay que tener en cuenta y ser precavido al momento de la persona compartir su propia información porque si eligen la persona incorrecta podrían darle un mal uso a esa información personal ya comentada.

Información externa: esta se origina de algún tipo de institución, empresa u organismo la cual los destinatarios son personas externas a la misma.

Información interna: este tipo de información es la que surge dentro de un organismos o empresa, con la finalidad de ser consumida de manera interna en otras palabras este tipo de información solo es consumida por las personas que pertenecen a ese organismo o empresa, sin salir al exterior.

5.1.3 Uso de la información

La información tiene muchos usos, pero todo depende del uso que el receptor quiera o pueda darle en algún momento en específico, porque quizás ese receptor tenga una información valiosa pero tal vez en el momento no sepa cómo aplicar esa información en algo útil.

Por tales razones todo lo que tiene que ver con información es un tema muy delicado, porque si dicha información cae en el receptor no indicado esto puede traer consecuencias debido a que una vez el receptor obtenga un a información x estará en sus manos el tipo de utilización que el atacante decida darle si mala, buena o ninguna.

Pero por otra parte existen otros tipos de usos la cual pueden ser un poco más estratégicos, facilitándole al receptor llevar a cabo una mejor toma de decisiones, ayudándole a realizar mejores procesos y distintas o mejores reglas de evaluación según la información adquirida será el grado de conocimiento.

5.2 Robo de información

A través del tiempo han surgido nuevas tecnologías como los Smartphone o una Tablet. Son muy atractivos para los cibercriminales ya que gracias a estos dispositivos tienen más posibilidades de robar a los usuarios datos confidenciales, debido a que el usuario al momento de estar navegando está más expuesto a posibles ataques o trampas ejecutadas por el atacante o cibercriminal.

Según unos estudios en Estados Unidos, la gran mayoría de los sitios de entidades bancarias identifican un fraude cuando el cliente lo denuncia con más de un 70%.

5.3 Riesgos al compartir información confidencial en redes o páginas web.

Todas las personas hoy en día corren un gran riesgo a diario, con el simple hecho de navegar en la web y en las redes sociales, pero la mayoría de los usuarios no saben en realidad que tanto se están exponiendo al compartir informaciones confidenciales en las redes sociales o en distintas páginas web.

5.3.1 Malware

A pesar de tener instalados antivirus, en ocasiones los malware pueden penetrar y cruzar. Los cibercriminales constantemente intentan hacer robo de identidades con algunas herramientas como bots, virus y rootkits. Todas estas técnicas son utilizadas mayormente para tratar de robar datos personales de los archivos de su ordenador personal. Los bots toman el control de su computador para ingresar más malware desde su ordenador. Los rootkits tiene una técnica especial la cual es ocultar el malware en archivos camuflajeados que parecen seguros para el software antivirus, pero realmente esconden un virus dentro de ellos.

5.3.2 Spyware

Este se puede identificar como un tipo de malware este está diseñado para una misión, la cual es espiar a la víctima del ataque y a todos sus datos, en esta función va incluidos rastreos de adware y cookies, en marketing este tipo de técnica de espionaje es muy utilizado para los proveedores observar que tipo de productos y servicios estas buscando en línea.

5.3.3 Ransomware

Así como su nombre lo indica este se encarga de secuestrar los datos para luego pedir una especie de rescate a sus víctimas para devolverle dichos datos. Según Norton, una empresa de software antivirus, en promedio los ladrones pidieron un rescate de 522 dólares en 2017.

5.3.4 Phishing

Los cibercriminales que utilizan esta técnica o método harán hasta lo imposible para lograr que la víctima tenga algún tipo de contacto con ellos, de ser necesario posiblemente te envíen correos electrónicos o te hagan llamadas, con el objetivo de tratar de engañarlo para que piensen que son una agencia o persona. Cuando el phishing se vuelve aún más personal es cuando el atacante utiliza tu propia información personales que encontró disponible en línea o en redes sociales para que sus correos parezcan más reales al momento de ellos tratar de contactarte.

5.3.5 Robo de correo electrónico empresarial

Este robo tiene una combinación de spoofing y phishing para ejecutar varios grandes ciberataques a las empresas que ellos tomen como víctimas. Los cibercriminales implementan procesos de ataques que suelen tardar hasta varios meses.

El FBI suele dividir este tipo de procesos en 4 pasos:

- Identificación de un objetivo.
- Preparación
- Intercambio de información
- Transferencias bancarias.

5.3.6 Fraudes con tarjetas de crédito y debito

Este tipo de robo soy muy terribles y comunes en nuestro país, mayormente cometemos el error de compartir información bancaria a través de nuestras redes sociales ya sea WhatsApp, Instagram, Correo electrónico o Facebook por lo tanto es un grave error porque cuando somos afectado por un ciberataque entonces nos volvemos más vulnerable y dicho atacante logra obtener nuestras informaciones bancarias de una manera más fácil.

5.3.7 Robo de identidad en las redes sociales

Mientras menos informaciones personales publiquemos en nuestras redes sociales es mucho mejor, porque pueden ser utilizadas para averiguar aún más sobre nosotros, con la información más insignificante los cibercriminales pueden llegar muy lejos, incluso con el simple hecho de obtener nuestro nombre completo y fecha de nacimiento pueden ser más que suficiente, además dichos estafadores o atacantes suelen crear cuentas falsas de tal manera que nos roban nuestra propia identidad.

5.4 Ataques

5.5 TIPOS DE ATAQUE

Las entidades, instituciones y empresas reciben ataques a diario de distintos atacantes, por lo tanto, debemos tener en cuenta algunas de las distintas metodología y tipos de ataque que existen y que buscan intentar robar información confidencial de algún usuario ya sea para atacar a la entidad a la que pertenece o para utilizar la información personal de dicho usuario fraudulentamente para adquirir productos o servicios:

5.5.1 Ataques de phishing basados en suplantación

En estos casos la técnica consiste en sustituir o suplantar la verdadera dirección de una página web por una falsa, a continuación, le estaremos mostrando algunas de las técnicas de phishing por suplantación más utilizadas:

5.5.2 Nombre de dominios erróneos

Este se identifica con la peculiaridad de registrar dominios parecidos a lo de entidades bancarias.

5.5.3 Ofuscación de URL

Esta técnica es la cual en donde se crea un sitio web falso y se oculta de alguna manera su URL de tal forma evitando que el usuario lea la dirección a la que va a ingresar en realidad.

Figura 15: Ofuscación de URL

5.5.4 Clonación de páginas web

Este método consiste en alojar en la internet una página web falsa, muy parecida a la página de la entidad o institución que decidirá atacar, en un servidor controlado por el atacante. Hoy en día este es uno de los métodos o técnicas más utilizadas y más común para realizar ataques de phishing, a

continuación, le presentare un ejemplo en la cual se está atacando una entidad bancaria.

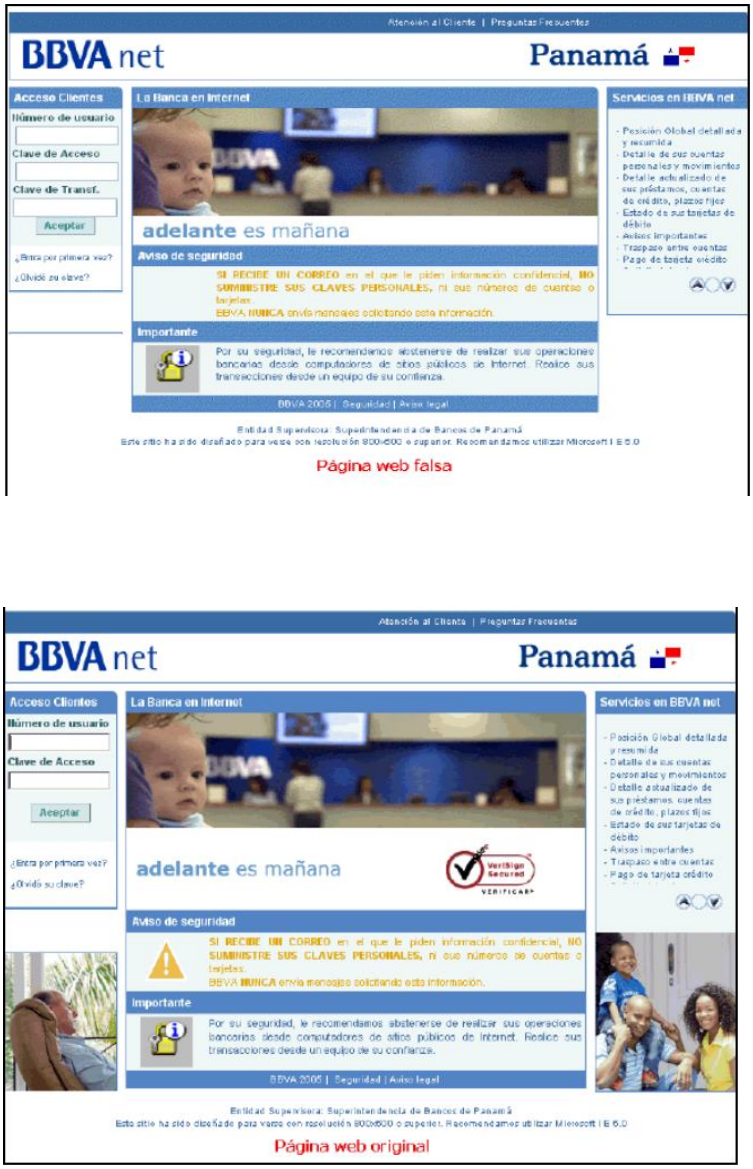


Figura 16: Clonación de página web.

5.5.5 Utilización de troyanos Bancarios

En distinción con los keyloggers, los troyanos bancarios están creados para identificar patrones de cadenas, ejemplo contraseñas, cada vez que el usuario o la victima entra a la zona de registro de la institución o entidad que será atacada, se activa de manera inmediata la recolección o captura de información específica, de tal manera logrando obtener la información de registro del usuario.

Luego más adelante para disminuir estos ataques comenzaron a implementar algunas medidas como por ejemplo los teclados virtuales, esta medida es eficiente ya que te permite ingresar información simplemente utilizando el mouse y a través de un teclado que se despliega en la pantalla, de tal manera permitiéndole al usuario que ingrese sus datos sin presionar ninguna tecla.

Figura 17: Keyloggers

5.5.6 Redireccionamiento Web

Este es uno más de los métodos y técnicas favoritas de los atacantes es la denominada DNS poisoning, envenenamiento de DNS, esta técnica consiste en modificar el DNS para redireccionar el real dominio hacían una dirección IP que fue creada anteriormente por el atacante.

5.6 Propuesta que mitigaría el riesgo

Tal y como nuestro tema lo indica la propuesta consiste en proponer una aplicación móvil llamada Personal Info Protector, que le brinde la seguridad, la protección necesaria y oportuna a los usuarios que utilicen esta app, reduciendo con algunas técnicas y prevenciones de lugar la exposición de información confidenciales en las redes sociales y en las páginas web inseguras.

5.7 ¿Como nuestra aplicación mitigara los riesgos?

Nuestra app Personal Info Protector al momento de ser instalada, en cualquier móvil se activarán un sin número de herramientas y funcionalidades que vienen integradas en la app por default, a continuación, se la estaremos comentando:

Personal Info Protector viene con un sistema de **protección avanzada,** la cual le permite un aprendizaje automático para lograr darle una respuesta inmediata a las nuevas amenazas, así bloqueando e identificando de manera rápida posibles ataques durante la navegación del usuario en las redes sociales y páginas web.

Por otro lado, con los **antivirus,** Personal Info Protector trae un conjunto de antivirus de varios niveles, para así poder lograr y neutralizar todos los **malware.**

- Antivirus en tiempo real.
- Prevención automática de exploits.
- Removedor de troyanos.
- Detección instantánea de amenazas.

También trae integrado **Antispyware,** esta tecnología es muy importante debido a que nos permite saber y encontrar algún spyware que podría estar dándole seguimiento a las llamadas, mensajes y actividades que realice el usuario.

En esta rama para así lograr una navegación más segura y mitigar los riesgos durante el usuario utiliza las redes sociales, Personal Info Protector también trae funcionalidades como:

5.7.1 Protección de pagos

Te brinda una mayor seguridad encriptando la información a nivel bancario así protegiendo al usuario cuando valla a realizar actividades como transacciones en línea.

5.7.2 Bloqueo de aplicaciones

Esta sección de Personal Info Protector le permite al usuario tener sus aplicaciones fuera de peligro y a la vez impide al usuario que descargue futuras aplicaciones infecciosas.

5.7.3 Protección de privacidad

Con esta funcionalidad activa en Personal Info Protector, le permite al usuario tener una mayor protección ya que cifra los datos personales al momento de la navegación, de tal manera evitando que los cibercriminales obtengan información valiosa.

5.7.4 Protección contra phishing

Esta es otra de la gran funcionalidad de Personal Info Protector, que es de suma importancia debido a que con esta funcionalidad protegemos al usuario, de que no entre a sitios web falsos y que bloquee los correos electrónicos creado por ciber criminales avisándole al usuario con una notificación de que han intentado atacarlo.

5.7.5 Protección de cámara web

Muchos cibercriminales obtienen acceso a tu cámara y logran manipularla espiando al usuario y en ocasiones capturando y tomando fotos de momentos íntimos de la víctima, para luego mostrársela de manera anónima y chantajear a la víctima, pero utilizando Personal Info Protector esto no podrá lograrse ya que inmediatamente Personal Info Protector detecta algún proceso mal manipulado infeccioso y no autorizado la cámara se bloquea de manera automática.

5.7.6 Protección antirrobo

Inmediatamente cualquier usuario que instale Personal Info Protector en su dispositivo, obtendrá esta funcionalidad, y en cualquier momento que su dispositivo sea robado o se le pierda, esta funcionalidad será activada de manera remota, por lo que se podría tener acceso a la alarma, cámara, ubicación del dispositivo y también logrando realizar una eliminación total de todos los datos e información confidenciales para evitar que el criminal las obtenga.

5.7.7 Protección contra keyloggers

Se les impide de inmediato que los keyloggers registren pulsaciones del teclado al dispositivo, lo que le permite al usuario mitigar los riesgos, protegiendo así robo de contraseña, informaciones bancarias entre otras.

En fin, este grupo de funcionalidades que Personal Info Protector, nos permite mitigar la gran mayoría de los riesgos que se toman al navegar en sitios web y en redes sociales son un sin número de técnicas que evitan que el usuario sea victima por cibercriminales y que sea afectado por futuras estafas a través del robo de información confidenciales ya sea personales o institucionales.

5.8 BENEFICIOS

- Protege al usuario de diferentes amenazas.
- Asistencia remota al usuario.
- Menos falsos positivos.
- Prevención de posibles ataques.
- Mayor seguridad al navegar.
- Detención de amenazas de una forma más rápida y eficiente.
- Mayor defensa de la información confidencial personal.
- Protección de phishing.
- Protección de spyware.
- Bloqueo de anuncios y spam.

5.9 DESVENTAJAS

- Restricciones al navegar en la web.
- Inconvenientes al realizar algunas asignaciones.

Capítulo 6: Conclusiones

CONCLUCIONES

A pesar de los esfuerzos en mejorar la seguridad informática y protección de la información personal de los usuarios que hacen uso recurrente de las redes sociales, la tasa de éxito siguen siendo muy bajas y la incidencia alta, por lo que, la implementación de una aplicación que proteja los datos personales de los usuario es de suma importancia, así como también al implementación de una campaña de educación y concientización de los usuarios para que hagan un uso responsable y adecuado de los recursos tecnológicos que tenemos hoy en día.

Debemos comprender que la tecnología, el uso de las redes sociales ha llegado para desempeñar un papel importante en nuestra cultura, diario vivir y hasta nuestra forma de trabajar y es por eso que se ha convertido en el vector principal de ataque para obtener sensitiva y personal de las personas, llevar a cabo la implementación de un sistema de gestión de riesgo de fuga de información, gestión de información y protección de data es de vital importancia para los usuarios que usan las redes sociales a diario.

Durante el análisis FODA pudimos observar que es extremadamente necesaria una aplicación móvil que facilite al usuario proteger su información de terceros de manera eficiente, nuestro proyecto representa una buena oportunidad para mitigar el riesgo de fuga de información ya que cuenta con las tecnologías y

mejoras necesaria para facilitar al usuario dicha protección conforme a la necesidad de los usuarios.

Por lo tanto, cada una de las funcionalidades que contiene la aplicación propuesta tiene como objetivo mitigar el riesgo de fuga de información de acuerdo a los objetivos antes planteando en este trabajo, lo cual resolvería la problemática identificada en el capítulo uno del mismo:

- Protección avanzada esta es la que permite tener un aprendizaje automático a la aplicación para que así la aplicación se mantenga constante mente actualizada y pueda detectar nuevas amenazas nunca antes vistas realizada por los cibercriminales, esta funcionalidad es bastante importante ya que los cibercriminales viven innovando día tras día, y creando nuevas estrategias y técnicas de ataque, por lo tanto con esta funcionalidad de protección avanzada esta aplicación también se mantendrá innovando constantemente, debido a su aprendizaje automático así convirtiéndose en un aplicación más robusta al pasar de los tiempos.

- En la funcionalidad nombrada antivirus, esta funcionalidad no es un antivirus común y corriente debido a que dentro de esta funcionalidad viene integrado antivirus en tiempo real, una prevención automática de exploits, removedor de troyanos, detección instantánea de amenazas, esta funcionalidad es clave debido a las características que vienen integrada dentro de ellas, la cual son de gran utilidad al momento de mitigar los riesgos de posibles ataques.

- Protección de privacidad, esta funcionalidad es otra de la más importante de la aplicación, debido a que cifra los datos personales y los datos de navegación, así a su vez evitando el espionaje de los cibercriminales, esta funcionalidad es muy útil, porque una de las principales técnicas de los cibercriminales es mediante la utilización de spyware, logrando así un espionaje constante de su víctima captando toda las informaciones confidenciales y valiosas para luego sacarle beneficios a esos datos espiados, pero gracias a la funcionalidad de protección de privacidad con la aplicación propuesta, para los cibercriminales esto no podría ser posible.

Finalmente, la idea de esta propuesta es garantizar la integridad, disponibilidad y seguridad de la información personal que los usuarios exponen durante el uso de las redes sociales. Además, el sistema será realizado enfocado en dar solución a los problemas actuales sobre fuga de información que tanto afecta de manera recurrente a los usuarios hoy en día en la República Dominicana.

BIBLIOGRAFIA

Referencias Bibliográficas

Consejos para proteger tu información en RR.SS
https://www.allianz-assistance.es/blog/legal/peligros-redes-sociales-privacidad.html

Protección de la privacidad en las redes sociales
https://lam.norton.com/internetsecurity-privacy-protecting-privacy-social-media.html

Redes sociales, ¡cuidado con lo que compartes
https://www.iberdrola.com/innovacion/redes-sociales-privacidad-seguridad

Cómo proteger la privacidad en las redes sociales
https://www.das.es/blog/como-proteger-la-privacidad-en-las-redes-sociales/
https://www.welivesecurity.com/wp-content/uploads/2013/11/guia-redes-sociales-eset.pdf

10 consejos para proteger tus redes sociales
https://amalialopezacera.com/10-consejos-proteger-redes-sociales/

Seguridad en las redes sociales
https://www.ceupe.com/blog/seguridad-en-las-redes-sociales.html

5 consejos de seguridad en redes sociales
https://www.reclamador.es/blog/seguridad-en-redes-sociales/

Internet y redes sociales
https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales

Significado de Riesgo
https://dle.rae.es/riesgo

Significado de Minimizar
https://dle.rae.es/minimizar

Significado de Exposición
https://www.significados.com/exposicion/

Gestión de datos de investigación
https://biblioguias.cepal.org/c.php?g=495473&p=4398114

¿Cuáles son los Datos Personales Confidenciales?
https://www.uv.mx/transparencia/preguntas/datos-confidenciales/

¿Qué es la Información Confidencial?
https://www.uv.mx/transparencia/preguntas/informacion-confidencial/

Evitar el robo de identidad
https://www.consumidor.gov/articulos/s1015-evitar-el-robo-de-identidad#!qu%C3%A9-es

Robo de identidad
https://es.wikipedia.org/wiki/Robo_de_identidad

Suplantación de identidad y secuestro de cuentas: ¿cómo actuar?
https://www.osi.es/es/actualidad/blog/2021/02/05/suplantacion-de-identidad-y-secuestro-de-cuentas-como-actuar

6 tipos de suplantación de identidad y cómo evitarlas
https://www.conletragrande.cl/mi-empresa/6-tipos-de-suplantaci%C3%B3n-de-identidad-y-c%C3%B3mo-evitarlas

9 consejos para proteger tu identidad digital
https://www.viafirma.do/consejos-proteger-identidad-digital/

Suplantación de la identidad
https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/riesgos-asociados-al-uso-de-las-tecnologias/suplantacion-identidad/

¿Quiénes Pueden Ser Embargados?
https://fc-abogados.com/es/quienes-pueden-ser-embargados/

Suplantación de identidades, un delito frecuente en el país
https://listindiario.com/la-republica/2009/01/25/88897/suplantacion-de-identidades-un-delito-frecuente-en-el-pais

Nuevos requerimientos de Información de la Superintendencia de bancos *https://www.sb.gob.do/pdf/Descripcion-General-Nuevos-Requerimientos-de-Informacion-Octubre-2011.pdf*

Ley No. 288-05 que regula las Sociedades de Intermediación Crediticia y de Protección al Titular de la Información *http://www.oas.org/es/sla/ddi/docs/RD4%20Ley%20N%20288-05%20de%202005.pdf*

Anexo detalle del nivel de Plagio de nuestro documento.