DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN, PREVIO LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA: MÉTODO ALTERNATIVO DE INGRESO DE CREDENCIALES BASADO EN EL USO DE DISPOSITIVOS MÓVILES ANDROID Y UNA EXTENSIÓN DE MOZILLA FIREFOX

AUTORES: MARTÍNEZ ALBÁN, ANDRÉS EDUARDO
ERAZO CARVAJAL, BRYAN STEVEN

DIRECTOR: Ph.D. YOO, SANG GUNN

SANGOLQUÍ

2019

CERTIFICADO DEL DIRECTOR

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERIA EN SISTEMAS

CERTIFICACIÓN

Certifico que el trabajo de titulación, *"MÉTODO ALTERNATIVO DE INGRESO DE CREDENCIALES BASADO EN EL USO DE DISPOSITIVOS MÓVILES ANDROID Y UNA EXTENSIÓN DE MOZILLA FIREFOX"* fue realizado por los señores: ***Andrés Eduardo Martínez Albán y Bryan Steven Erazo Carvajal***, el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto, cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 25 de enero del 2019

YOO, SANG GUUN
C.C.: 1306853720

AUTORÍA DE RESPONSABILIDAD

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERIA EN SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

Nosotros, ***Andrés Eduardo Martínez Albán y Bryan Steven Erazo Carvajal***, declaramos que el contenido, ideas y criterios del trabajo de titulación: ***"MÉTODO ALTERNATIVO DE INGRESO DE CREDENCIALES BASADO EN EL USO DE DISPOSITIVOS MÓVILES ANDROID Y UNA EXTENSIÓN DE MOZILLA FIREFOX"*** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz

Sangolquí, 28 de Enero de 2019

Andrés Eduardo Martínez Albán
C.C.: 1724472186

Bryan Steven Erazo Carvajal
C.C.: 1723437164

AUTORIZACIÓN

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERIA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Nosotros, ***Andrés Eduardo Martínez Albán y Bryan Steven Erazo Carvajal,*** *autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación:* ***"MÉTODO ALTERNATIVO DE INGRESO DE CREDENCIALES BASADO EN EL USO DE DISPOSITIVOS MÓVILES ANDROID Y UNA EXTENSIÓN DE MOZILLA FIREFOX"*** *en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.*

Sangolquí, 28 de Enero de 2019

Andrés Eduardo Martínez Albán
C.C.: 1724472186

Bryan Steven Erazo Carvajal
C.C.: 1723437164

DEDICATORIA

A mi madre, la mejor mujer del mundo, quien me ha regalado todo lo bueno y me ha inculcado los valores necesarios e indispensables para alcanzar este objetivo, quien jamás se ha rendido y siempre me ha llenado de su amor incondicional, a quien admiraré eternamente por su gran ejemplo, dedicación, paciencia y fortaleza, por quien vivo y a quien ha sido y será dedicado todo mi esfuerzo y mis logros.

A mis hermanas, Verónica y Paulina, cómplices de mi vida quienes me han brindado siempre su apoyo y me han compartido su ternura y sencillez.

Andrés Martínez.

A mi abuelita la gran madre que me enseñó a ser una persona de bien junto con el conocimiento y valores que utilizo cada día, toda esta enseñanza me sirve para cumplir los objetivos que se presentan y superar cada escalón de la vida, por lo cual dedico esta etapa que es parte de un gran camino por delante.

A mi padre, mi madre y hermano por ofrecerme todo el apoyo y afecto emocional los cuales me vieron en los buenos y malos momentos durante este ciclo de mi vida, dedico el esfuerzo y mis logros hacia ellos.

A mi tía abuela también por estar pendiente siempre cada día de esta etapa que la he superado con buenos recuerdos, experiencias y conocimiento.

Bryan Erazo

AGRADECIMIENTO

A todos quienes se permitieron compartir junto a mí el camino que finaliza con este documento, e hicieron de mi instancia académica la experiencia más enriquecedora de mi vida.

A mi carrera, por la cual descubrí mi vocación y la más emocionante de mis pasiones. Finalmente, agradezco a mi universidad por todo el conocimiento adquirido, el mismo que me permitirá cumplir mis sueños y colaborar con el desarrollo para un mejor porvenir de nuestro país, gracias ESPE.

Andrés Martínez.

A las todas personas que estuvieron involucradas en mi desarrollo como persona y académicamente el cual me ha permitido agrandar mis conocimientos de mi gran carrera, siempre tuve en mente desde los inicios además es una experiencia inolvidable y me llevo grandes recuerdos de mi querida alma mater mi universidad, querida ESPE.

Bryan Erazo

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

INTRODUCCIÓN

1.1 Antecedentes

A medida que la tecnología avanza, los medios de vulneración se van perfeccionando, esta situación ha provocado que la seguridad informática se convierta en una temática importante para todos los usuarios de sistemas de información en general, porque permite salvaguardar la información que, actualmente, es el activo más importante y valioso de las organizaciones (Mieres, 2009).

De acuerdo con Martelo (2018), pese al continuo esfuerzo de las empresas en el fortalecimiento de la seguridad de sus sistemas de información, ninguno puede ser considerado como seguro en su totalidad, debido a que diariamente aparecen nuevos y sofisticados métodos de ataques informáticos que aprovechan las vulnerabilidades de los sistemas y logran tener acceso a la información.

Existen diversos métodos para precautelar la seguridad de los sistemas informáticos, entre ellos, el más usado es el de credenciales de acceso, denominado como “tradicional”. Para el uso de este método, el usuario debe proporcionar al sistema un par de cadenas de texto: el nombre de usuario, de conocimiento público, permite verificar la existencia del mismo en el sistema y la contraseña que teóricamente solo el usuario en cuestión debe conocer, posibilita la comprobación de su identidad (Oracle, 2012).

Al ser este método de autenticación el más utilizado, es evidente la existencia de herramientas que intentan obtener o capturar las credenciales de acceso de los usuarios a los distintos sistemas de información, entre las más conocidas existe una clase denominada “keyloggers”.

Estas herramientas pueden ser de dos tipos; basados en hardware (pequeños dispositivos externos) o basados en software. Ambos tienen un objetivo en común, que es el de capturar las pulsaciones de teclado realizadas por el usuario. La información capturada es posteriormente almacenada en registros a los cuales el atacante tiene acceso.

Existen keyloggers más sofisticados que permiten el envío de los datos capturados en tiempo real a través de internet, facilitando el proceso de obtención de información y acelerando el uso que el delincuente pretenda darle a la misma según su conveniencia (López J. , 2015).

Solairaj (2016) menciona en sus estudios, algunas técnicas para evitar el robo de información por malware, las cuales utilizan herramientas especializadas en la detección de spyware y accesos seguros a cuentas protegidas con contraseñas. La debilidad de estas técnicas radica principalmente en la detección de keyloggers, debido a que este tipo específico de software malicioso tiene la capacidad de ocultarse y pasar desapercibido en cualquier clase de equipo computacional.

Junto con esta condición y según Sukhram (2017), es importante considerar que los paquetes de antivirus convencionales no están enfocados en la detección de ataques realizados por medio de keyloggers, debido a que se encargan principalmente de controlar otros aspectos importantes, dando lugar así a posibles vulnerabilidades de seguridad.

1.2 Problemática

La mayoría de usuarios que utilizan el internet para realizar diferentes tipos de transacciones, no tienen conocimiento de las distintas amenazas a las que se enfrentan (Cullina, 2013).

Los delincuentes informáticos se encuentran constantemente en búsqueda de vulnerabilidades que les permitan adueñarse de información personal de los usuarios y conseguir sus credenciales de acceso a sistemas. Con la obtención de esta información y

mediante suplantación de identidad, tratan de realizar diferentes procedimientos o transacciones con el fin de obtener algún beneficio personal, generalmente económico (Connell, 2017).

Según cifras publicadas en el comunicado de prensa de Symantec (2018), se estima que los delincuentes informáticos consiguieron robar aproximadamente 172 mil millones de dólares a 978 millones de usuarios ubicados en 20 diferentes países alrededor del mundo en 2017. La principal causa de la facilidad con la que se cometen este tipo de delitos, es el exceso de confianza de los usuarios, al no aplicar los principios básicos de ciberseguridad. El informe detalla que, uno de los problemas más frecuentes es el uso de la misma contraseña para ingresar a distintos sistemas, error que cometió el 25% de las víctimas de robo de información en Estados Unidos.

Según datos recolectados por diario el Telégrafo, en Ecuador se registraron 635 denuncias por delitos informáticos en 2016, la mayoría relacionada con temas de apropiación fraudulenta por medios electrónicos. Es importante mencionar que el porcentaje de denuncias realizadas, es mínimo en comparación a la cantidad de delitos cometidos (Diario el Telégrafo, 2016).

Las aplicaciones web de los bancos son objetivos frecuentes de ataques informáticos, estos se realizan principalmente con el fin de obtener las credenciales de acceso de los usuarios. Para evitar el delito de suplantación de identidad posibilitado por los ataques mencionados, estas aplicaciones comúnmente utilizan teclados en pantalla (OSK – On Screen Keyboards) como medio de entrada para contraseñas. Sin embargo, los spyware enfocados en el robo de información de usuario, se adaptaron a este modelo de ingreso de datos y permiten capturar imágenes de la pantalla, incluyendo información de las coordenadas en las que el usuario realiza pulsaciones con el mouse, invalidando así la eficiencia de esta solución (Information Security , 2016).

1.3 Justificación

Symantec, organización que ha conformado un repositorio de 95.800 vulnerabilidades y ha dado seguimiento a las actividades maliciosas de la red en 175 millones de puntos que se encuentran en 157 países durante 20 años, evidencia en su reporte anual de amenazas a la seguridad de internet (ISTR), el crecimiento constante de prácticas ilícitas realizadas con malware a nivel mundial (Symantec, 2018).

Un estudio realizado por Thomas (2017), señala que las cifras de credenciales de acceso robadas por software malicioso entre phishing y keyloggers, superan los mil millones. Detalla también que la media de victimas de captura de información personal por keyloggers es de 15.000 usuarios por semana. Adicional a esto, el estudio presenta a Gmail, el sistema de correo electrónico de Google, como la plataforma con mayor índice de cuentas apoderadas, específicamente el 29.8%, seguido de Yahoo con el 11.5%. En cuanto a los países con mayor cantidad de casos registrados por ataques de keyloggers se menciona a Brasil con 18.3%, India con 9.8% y Estados Unidos con 8.0%.

Los datos y estadísticas presentes en este documento, evidencian el problema ocasionado por la captura de información mediante el uso de keyloggers, problemática que se potencializa cuando los usuarios acceden a los distintos sistemas de información por medio de equipos pertenecientes a sitios públicos como: bibliotecas, cibercafés, etc. Debido a que, en estos casos, se pierde el control de la seguridad al usar un terminal en el cual, algún atacante pude haber instalado malware o colocado algún dispositivo externo que le permita adueñarse de la información procesada (Mieres, 2009).

Por lo anterior mencionado, se plantea establecer un método alternativo de ingreso de credenciales que evite la captura de información por spyware keyloggers, el cual se presenta

como una contribución en el campo de la seguridad informática para los usuarios de sistemas de información que utilizan el método de acceso tradicional.

1.4 Objetivos

1.4.1 Objetivo General

Desarrollar un método alternativo de ingreso de credenciales basado en el uso de dispositivos móviles para disminuir el robo de estas por medio de herramientas de spyware conocidas como keyloggers.

1.4.2 Objetivos Específicos

i. Realizar una revisión de literatura que permita analizar las diferentes propuestas que han sido presentadas como métodos alternativos de ingreso de credenciales.
ii. Diseñar el método alternativo de ingreso de credenciales, de modo que permita un óptimo acoplamiento de todos sus componentes y principalmente, garantice la seguridad de la información procesada.
iii. Aplicar el método alternativo de ingreso de credenciales al portal web académico Mi ESPE.

1.5 Alcance

El alcance del presente proyecto comprende el desarrollo de un método alternativo para el ingreso de credenciales, basado en el uso de dispositivos móviles con sistema operativo Android y en una extensión del web browser “Mozilla Firefox”.

Con el fin de verificar la funcionalidad del método desarrollado, este será aplicado al ingreso del portal web académico Mi ESPE, plataforma educativa perteneciente a la Universidad de las Fuerzas Armadas ESPE que permite gestionar todos los procesos académicos.

Cabe mencionar que no existen registros de la operatividad del sitio web en los diferentes navegadores, por lo cual, la verificación de la eficiencia del método desarrollado, estará sujeta únicamente a las funcionalidades que operen en el navegador Mozilla Firefox.

CAPÍTULO II

REVISIÓN DE LITERATURA

En esta sección se analizan diferentes propuestas presentadas como métodos alternativos de ingreso de credenciales, obtenidas tras haber realizado un mapeo sistemático de literatura o también conocido como estudio de antecedentes (Wohlin & Runeson, 2013), es decir, un análisis de estudios primarios en un área temática específica, que tiene como objetivo identificar evidencias actuales y disponibles sobre el tema (Kitchenham & Charters, 2007).

El proceso de estudio de antecedentes realizado contempla las siguientes fases: (1) planteamiento del estudio sistemático de literatura, (2) obtención del grupo de control y palabras clave para la investigación, (3) creación y afinación de la cadena de búsqueda, (4) selección de estudios primarios y, (5) elaboración del estado del arte. Cada actividad de este proceso se describe a continuación.

2.1 Planteamiento del estudio sistemático de literatura

Como fase inicial del proceso de estudio de antecedentes, se realizó la descripción del problema en el que está enfocada la investigación, a fin de definir el marco de búsqueda de los estudios científicos, seguido del planteamiento de las preguntas de investigación y finalmente el establecimiento de los criterios de inclusión y exclusión.

2.2 Obtención del grupo de control y palabras clave para la investigación

De acuerdo a Levac (2010), esta fase implica identificar los estudios relevantes y desarrollar un plan de decisión que permita definir los términos que se van a buscar y las fuentes en las que se deben consultar, incluyendo bases de datos electrónicas, listas de referencia, búsquedas manuales de revistas clave, organizaciones y conferencias.

Tras el análisis de varios artículos científicos propuestos por los investigadores, se obtuvo el grupo de control (GC) que está conformado por 4 artículos científicos que se

consideraron relevantes e influyentes en la investigación. Esta información se encuentra detallada en la Tabla 1.

Tabla 1
Estudios de Control

Código	Título	Cita	Palabras clave
EC1	**Random Multiple Layouts Keylogger Prevention Technique**	(Tasabeeh, Omer, & Abeer, 2016)	keylogger user-space keylogger, kernel- space keylogger, keyboard input model, password, credentials
EC2	**A Novel Method for Authentication Protocol using Barcode Generator**	(Ranganadham & Ravi, 2016)	key logging, authentication protocols, spyware, visual authentication, security
EC3	**Defend a System against Keyloggers with a Privilege-limited Account**	(Chien-Wei, Fu-Hau, & Shih-Jen, 2013)	authentication, computer security, keylogger, privacy, attack
EC4	**Improved keylogging and shoulder-surfing resistant visual two-factor authentication protocol**	(Kheder, 2018)	authentication, Web, keylogger, shoulder-surfing, smartphone

Con la selección de los artículos pertenecientes al GC, se pudo determinar las palabras clave que se encuentren alineadas al objetivo de la investigación, las cuales fueron: key logging, keylogger, key-logger, spyware, attack, authentication, password, credentials, Web, security.

2.3 Creación y afinación de la cadena de búsqueda

Una vez que las palabras clave fueron identificadas, se crearon las diferentes cadenas de búsqueda que se aplicaron en la base digital SCOPUS. La primera cadena de búsqueda creada fue la siguiente:

ALL*({key logging}* ***OR*** *{keylogger})* ***AND ALL****({spyware})* ***AND ALL****({keyboard input model}* ***OR*** *{authentication method})* ***AND ALL****({security})*

Esta cadena obtuvo muy pocos artículos científicos como resultado de búsqueda, por lo que se tuvo que seguir con la afinación de la misma y tras varias cadenas generadas con la combinación de las palabras clave definidas y los conectores de la base digital, se determinó la cadena de búsqueda final:

ALL*({key logging}* ***OR*** *{keylogger}* ***OR*** *{key-logger})* ***AND ALL****({spyware}* ***OR*** *{attack})* ***AND ALL****({authentication}* ***OR*** *{password}* ***OR*** *{credentials})* ***AND ALL****({Web})* ***AND ALL****({security})*

2.4 Selección de estudios primarios

La cadena de búsqueda final, arrojó 39 artículos científicos como resultado, entre los cuales se encontraban la mayoría de artículos pertenecientes al GC, por lo que se decidió tomar esta como definitiva.

A fin de detallar con mayor precisión el tipo de artículo científico que se consideraría como válido para la realización del estudio de antecedentes, se determinó aplicar dos filtros de búsqueda adicionales:

1. **Año:** Los artículos candidatos deberían haber sido publicados a partir del año 2012. Se decidió aplicar este filtro con el objetivo de que las soluciones propuestas a la problemática investigada, se encuentren lo más apegadas a la realidad actual de los avances tecnológicos.
2. **Tipo de documento:** Se consideraron únicamente documentos de tipo: Conference Paper y Article, debido a que estos son reflejo de una investigación que genera alto impacto en la comunidad científica.

Con la adición de estos dos criterios de exclusión, se presenta a continuación la cadena de búsqueda generada por la base digital SCOPUS:

ALL *({key logging}* ***OR*** *{keylogger}* ***OR*** *{key-logger})* ***AND ALL*** *({spyware}* ***OR*** *{attack})* ***AND ALL*** *({authentication}* ***OR*** *{password}* ***OR*** *{credentials})* ***AND ALL*** *({Web})* ***AND ALL*** *({security})* ***AND*** *(* ***LIMIT-TO*** *(PUBYEAR , 2018)* ***OR LIMIT-TO*** *(PUBYEAR , 2017)* ***OR LIMIT-TO*** *(PUBYEAR , 2016)* ***OR LIMIT-TO*** *(PUBYEAR , 2015)* ***OR LIMIT-TO*** *(PUBYEAR , 2014)* ***OR LIMIT-TO*** *(PUBYEAR , 2013)* ***OR LIMIT-TO*** *(PUBYEAR , 2012))*

Esta cadena presentó un menor número de artículos científicos candidatos, de los cuales a criterio de los investigadores, fueron seleccionados 20 como estudios primarios y son detallados en la Tabla 2.

Tabla 2
Estudios Primarios

Código	Título	Cita
EP1	Random Multiple Layouts Keylogger Prevention Technique	(Tasabeeh, Omer, & Abeer, 2016)
EP2	A Novel Method for Authentication Protocol using Barcode Generator	(Ranganadham & Ravi, 2016)
EP3	EAM: Architecting Efficient Authentication Model for Internet Security using Image-Based One Time Password Technique	(Jesudoss & Subramaniam, 2016)
EP4	Graphical One-Time Password (GOTPass): A usability evaluation	(Alsaiari, Papadaki, & Dowland, 2016)
EP5	Improved keylogging and shoulder-surfing resistant visual two-factor authentication protocol	(Kheder, 2018)
EP6	Keylogging-resistant visual authentication protocols	(Nyang, Mohaisen, & Kang, 2014)
EP7	Securing cloud-based healthcare information systems using enhanced password-based authentication scheme	(Jesudoss & Subramaniam, 2016)
EP8	Designing leakage-resilient password entry on touchscreen mobile devices	(Yan, Han, Li, Zhou, & Deng, 2013)
EP9	SAFE Shoulder-surfing attack filibustered with ease	(Gowraj, Avireddy, Ravi, Subramanian, & Prabhu, 2013)

CONTINÚA

EP10	A QTE-based Solution to Keylogger Attacks	(Hung, et al., A QTE-based Solution to Keylogger Attacks, 2012)
EP11	GAS A novel grid based authentication system	(Gowraj, Avireddy, & Prabhu, 2013)
EP12	Defend a System against Keyloggers with a Privilege limited Account	(Hung, et al., 2013)
EP13	Understanding DMA Malware	(Stewin & Bystrov, 2013)
EP14	On screen randomized blank keyboard	(Neenu, 2015)
EP15	Image steganography for increasing security of OTP authentication	(Wilfred & Skarbek, 2018)
EP16	Data Breaches, phishing, or malware understanding the risks of stolen credentials	(Thomas, et al., 2017)
EP17	Secure login protocols An analysis on modern attacks and solutions	(Waheed, Shah, & Khan, 2016)
EP18	Web based testing application security system using semantic comparison method	(Iskandar, et al., 2018)
EP19	KeyStroke logs Are strong passwords enough	(Sukhram, 2017)
EP20	SoK Keylogging Side Channels	(Monaco, 2018)

2.5 Elaboración del estado del arte

Con el fin de detallar claramente las características de los estudios que conforman el estado del arte, se procedió a clasificar los estudios primarios de acuerdo al tipo de contribución presentada. Para tal efecto se han agrupado los estudios en 4 categorías: Modelos, Métodos, Técnicas y Lineamientos.

Modelos propuestos: EP3, EP7

La propuesta de (Jesudoss & Subramaniam, 2016) trata acerca de la adición de una serie de imágenes en el proceso de renderización de las páginas de ingreso a sitios web. El usuario debe enviar su ID, contraseña y seleccionar cinco imágenes que validen cada sesión, de esta manera no se permiten transacciones con sesiones duplicadas o robadas.

El limitante de esta propuesta es que no está enfocada a prevenir ataques de keylogger y no presenta evidencia de su efectividad ante estos.

Por otro lado, (Jesudoss & Subramaniam, 2016) presenta, en otro estudio, un modelo de autenticación único que protege el Sistema de información de atención médica basado en la nube de varios ataques de seguridad, como ataques de repetición, ataques de adivinación de contraseñas y ataques de keylogger.

El modelo denominado EPBAS se implementó utilizando Java 7.0 y Tomcat 7.0.40. El cifrado AES (Advanced Encryption Standard) de 256 bits se realizó con la ayuda de JCE (Java Cryptography Extension). Además, se implementó la función hash criptográfica SHA25 (Secure Hash Algorithm), mientras que la clave secreta se genera en función de la contraseña del cliente utilizando el algoritmo PBKDF2WithHmacSHA1 (Password-Based key Derivation Function 2 with Hash-based Message Authentication Code Secure Hash Algorithm 1).

La novedad de este modelo es que reduce el costo involucrado en el proceso de autenticación y también evita la dependencia de dispositivos externos para el mismo, como la OTP móvil, sensores de autenticación biométrica, entre otros.

Métodos propuestos: EP2, EP4, EP5, EP6, EP8, EP9, EP10, EP11, EP12, EP14, EP15, EP18

(Gowraj, Avireddy, Ravi, Subramanian, & Prabhu, 2013) , (Gowraj, Avireddy, & Prabhu, 2013), (Wilfred & Skarbek, 2018) y (Alsaiari, Papadaki, & Dowland, 2016), proponen métodos basados en autenticación gráfica.

En el primer caso, (Gowraj, Avireddy, Ravi, Subramanian, & Prabhu, 2013) propone un sistema llamado SAFE: ShoulderSurfing Attacks Filibustered with Ease que utiliza el algoritmo RALUT-G (Tablero de búsqueda aleatoria) que propone un esquema novedoso para generar una tabla de búsqueda aleatoria que contiene la contraseña de los usuarios junto con los

caracteres de señuelo aleatorios. Sin embargo, los resultados experimentales y el análisis de complejidad demostraron que aún existe gran margen de mejora en cuanto a temas de usabilidad y el tiempo requerido para el inicio de sesión en comparación a otros métodos.

Por otro lado, (Gowraj, Avireddy, & Prabhu, 2013) propone un sistema de autenticación basado en contraseña gráfica denominado GAS (Grid based Authentication System). La metodología implica elegir un patrón llamado Auth Pattern, que se forma al colocar imágenes en una cuadrícula determinada. Esto debido a que la autenticación de contraseña gráfica ha demostrado ser más potente y útil en comparación con la autenticación de contraseña de texto tradicional.

Más allá de esto, (Wilfred & Skarbek, 2018) proporciona un método que utiliza tanto una imagen con información oculta del cliente del banco como la One Time Password (OTP) que se envía por medio del servicio de mensajes cortos (SMS) al dispositivo móvil del usuario. El número de identificación personal (PIN) proporcionado por el banco en el momento del registro se utiliza para activar el proceso de esteganografía de imagen y el envío de OTP al usuario, donde la OTP debe ingresarse en un teclado virtual con teclas aleatorias para evitar el registro de teclas, que se utiliza para descifrar la información oculta en la imagen. Esta información oculta debe coincidir con la información en la base de datos, proporcionando así la sesión para el cliente. Sin embargo, el problema de este método es su limitación y enfoque a sistemas de acceso a bancos.

Adicionalmente, (Alsaiari, Papadaki, & Dowland, 2016) propone un método híbrido de autenticación de usuario que consiste en agregar dos fases más de seguridad al proceso de inicio de sesión. A más del ingreso tradicional con la ID de usuario y contraseña, este método requiere en primera instancia la definición de una figura en un patrón de desbloqueo 4x4. Posteriormente se cuenta con el desplazamiento de una serie de imágenes escogidas por el usuario hasta una

posición definida, permitiendo al sistema tomar las coordenadas de dichas imágenes para procesarlas en dos distintos niveles.

La evaluación de usabilidad de este método demostró que, a pesar del aumento en los niveles de seguridad, los usuarios consideran que son demasiados pasos a seguir para ingresar a un sistema, por tal razón los índices de satisfacción al utilízalo fueron desalentadores.

(Ranganadham & Ravi, 2016), (Kheder, 2018), (Nyang, Mohaisen, & Kang, 2014) y (Neenu, 2015) proponen métodos basados en autenticación visual.

La propuesta de (Ranganadham & Ravi, 2016) comprende una solución visual de ingreso de contraseñas que hace uso de la realidad aumentada a través de una aplicación móvil. El servidor de la aplicación web a la cual se desea acceder envía un teclado invisible junto con un código de barras, que, al ser escaneado por la aplicación, hará visible el teclado en la pantalla del dispositivo móvil, así los usuarios sabrán en qué lugar deben hacer sus pulsaciones con el ratón.

Esta solución evita el robo de información por keyloggers e incluso por software que almacena información de pulsaciones de ratón.

Por otro lado, la propuesta de (Kheder, 2018), consiste en la generación de una OTP como un código Quick Response (QR), este deberá ser solicitado por el usuario desde su dispositivo móvil de confianza. El código deberá ser escaneado por la cámara web del equipo en donde se desea iniciar sesión y con la información descifrada, se completará automáticamente el campo de la contraseña.

El principal inconveniente encontrado en esta solución tiene relación con la falta de cámaras web en todos los equipos computacionales.

Además, (Nyang, Mohaisen, & Kang, 2014) propone dos métodos de autenticación visual: uno es un método de contraseña de un solo uso OTP y el otro es un protocolo de

autenticación basado en contraseña. A través de un análisis riguroso, se verificó que ambos métodos son inmunes a varios tipos de keyloggers. Más allá de esto, pudieron lograr un alto nivel de usabilidad al tiempo que cumplen con estrictos requisitos de seguridad.

Mientras, (Neenu, 2015) propone un método de autenticación visual basado en contraseña que utiliza un teclado en blanco aleatorio con algunos símbolos especiales asociados con cada carácter. Usando este nuevo teclado, los usuarios pueden ingresar sus credenciales. Este método probó ser efectivo contra los ataques de keyloggers y los ataques de shoulder surfing al aumentar la cantidad de memoria a corto plazo requerida. Incluso puede ser implementado en cajeros automáticos al ingresar sus claves.

(Yan, Han, Li, Zhou, & Deng, 2013), (Hung, et al., 2012), (Chien-Wei, Fu-Hau, & Shih-Jen, 2013) y (Iskandar, et al., 2018) proponen métodos que hacen uso de la pantalla táctil de un dispositivo móvil, un área especial dentro de la página web, un segundo dispositivo para el ingreso de credenciales y comparación semántica, respetivamente.

El método de (Yan, Han, Li, Zhou, & Deng, 2013), denominado CoverPad, permite la entrada de contraseña en dispositivos móviles con pantalla táctil. CoverPad mejora la resistencia a las fugas al enviar mensajes ocultos de forma segura, lo que rompe la correlación entre la contraseña subyacente y la información de interacción observable para un adversario. La principal desventaja de este método se refleja en los resultados de la evaluación de usabilidad, en donde se comprobó que es complicado de utilizar por nuevos usuarios.

En cambio, el método Quick Time Events (QTE) de (Hung, et al., 2012) utiliza un área específica para indicar a los usuarios en dónde su entrada será registrada o ignorada por el complemento QTE, brindando la oportunidad de ofuscar a los keyloggers insertando letras sin sentido entre las pulsaciones de teclas de sus contraseñas. Además, puede aplicarse a todos los sitios web sin ninguna modificación de ellos.

El método propuesto considera parámetros muy importantes, como la memoria del usuario y la longitud de la contraseña. Sin embargo, resulta aún más complicado de usar que otros sistemas y aunque provee de protección contra key loggers, ésta es mínima.

Más allá de esto, el método Broker propuesto por (Chien-Wei, Fu-Hau, & Shih-Jen, 2013) es efectivo ante la mayoría de los keyloggers de kernel, hipervisor, hardware y segundo canal en el espacio del usuario, incluso con una cuenta con privilegios limitados. El método Broker usa un segundo dispositivo para comunicarse de manera segura con una computadora pública no confiable. Lo más llamativo de esta propuesta es que fue probada con siete diferentes keyloggers y ninguno de ellos pudo obtener las contraseñas reales.

Finalmente, (Iskandar, et al., 2018) diseñó e implementó un método de prueba de seguridad web mediante el uso del método de comparación semántica para evitar ataques de inyección SQL. Después del diseño y la aplicación del método, se pudo determinar que mediante el uso del método de comparación semántica se puede evitar la aparición de ataques de inyección de SQL y se puede proteger la cuenta de los usuarios de pruebas web mediante el uso de MD5.

Técnicas propuestas: EP1

(Tasabeeh, Omer, & Abeer, 2016) propone una nueva técnica de prevención del robo de información de usuario por keyloggers. La idea consiste en la creación y uso de un teclado que utilice múltiples diseños (layouts). Con cada pulsación de las teclas, uno de los diseños se elegirá al azar y se configurará como válido, haciendo que el diseño del teclado sea inconstante de modo que los keylogger interceptarán las pulsaciones después de que estas hayan sido traducidas por el diseño activo del teclado y, por tal razón, la información capturada será ilegible, al haber sido traducida por un diseño de teclado elegido al azar.

El inconveniente inicial de esta solución es que el usuario tampoco podrá ver en pantalla la tecla real que seleccionó, para lo cual, los autores del artículo indican que esto será solventado con la utilización de un mapa de conversión específico para el layout válido y el idioma deseado.

La limitante de esta propuesta es que, al realizar los cambios aleatorios de presentaciones de teclado, se está ocupando tiempo de procesamiento, por lo que la eficiencia de esta idea es cuestionable.

Lineamientos propuestos: EP13, EP16, EP17, EP19, EP20

(Stewin & Bystrov, 2013) introduce a DAGGER, un keylogger que ataca las plataformas Linux y Windows, el cual puede atacar de manera eficiente las estructuras del kernel, incluso si la asignación aleatoria de direcciones de memoria está en su lugar. Más allá de esto, se evaluaron y presentaron posibles contramedidas tales como configuraciones especiales para la I/OMMU (unidad de gestión de memoria de entrada y salida).

(Thomas, 2017) presenta el primer estudio de medición longitudinal del ecosistema subterráneo que alimenta el robo de credenciales y evalúa el riesgo que representa para millones de usuarios. Además, se muestra el endurecimiento de los mecanismos de autenticación para incluir señales de riesgo adicionales, como las geolocalizaciones históricas del usuario y los perfiles de dispositivos, ayudan a mitigar el riesgo de robo de credenciales.

En cambio, (Waheed, Shah, & Khan, 2016) agrupó los enfoques existentes y se evaluaron críticamente los ataques modernos en términos de severidad de ataques de modo que los resultados puedan ayudar a los expertos en seguridad, analistas y diseñadores de políticas de seguridad para seleccionar la arquitectura de autenticación apropiada según sus necesidades.

(Sukhram, 2017) discute las características de los keyloggers además de proporcionar un resumen de los métodos de protección. Se probaron tres keyloggers contra dos programas anti-keylogging para identificar qué información se captura y qué método de protección es más

fuerte. También se incluyó una discusión sobre la evaluación del riesgo con respecto a los keyloggers y las técnicas de remediación que deben ser consideradas para evitar ser víctima de este tipo de ataques.

Por último, (Monaco, 2018) revisa el estado actual de los ataques de keylogger y se discuten algunas de las técnicas de mitigación que se pueden aplicar.

En general, muchos de los lineamientos propuestos se enfocan en evitar otros tipos de ataques más allá de los keyloggers ya que estos son sólo una parte del amplio espectro existente en cuanto a métodos de robo de credenciales se refiere.

2.6 Evaluación del estado del arte

Existen varias investigaciones realizadas con el objetivo de minimizar o reducir el impacto del robo de información con herramientas de spyware conocidas como keyloggers, estas soluciones varían en su nivel de complejidad, usabilidad y sobretodo en el apartado de la adaptabilidad.

Las falencias de cada uno de los modelos alternativos de ingreso de credenciales presentados en la descripción de los estudios primarios, pueden ser solventadas con un método que permita agrupar todas las consideraciones extraídas de esta investigación y que sea adaptable a sitios que ya se encuentran en producción.

CAPÍTULO III

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA

Con el avance y crecimiento de las nuevas tecnologías de la información y comunicación (NTIC), se hace evidente la necesidad de realizar un estudio de la seguridad informática, donde se pueda ejecutar un análisis de los métodos que permitan mitigar, prevenir y reducir los riesgos asociados a los principios de la seguridad de la información CID, Confidencialidad, Integridad y Disponibilidad (Abril, 2013). En esta sección se detallará los fundamentos teóricos de la seguridad informática y los riegos informáticos con especial énfasis en los keyloggers como medio para robo de credenciales, así como los métodos de prevención y respuesta ante estas amenazas.

3.1 Seguridad Informática

La expansión fenomenal del ciberespacio ha traído crecimiento económico, oportunidades y prosperidad sin precedentes. Más allá de esto, también presenta a los malos actores amenazas y oportunidades de crimen completamente nuevas (Kriz, 2011).

Por un lado, de acuerdo con (Addae, Radenkovic, Sun, & Towey, 2016), la seguridad informática se refiere a la protección contra el acceso y el uso no autorizados de dispositivos, aplicaciones y datos conectados a Internet.

Por otro lado, para (Jang-Jaccard & Nepal, 2014), la seguridad informática se relaciona con la comprensión de los problemas circundantes de diversos ataques cibernéticos y el diseño de estrategias de defensa, es decir, contramedidas que preservan la confidencialidad, integridad y disponibilidad de cualquier tecnología digital y de información.

Sin embargo, (Parekh, et al., 2018) consideran que la seguridad informática comprende un área vital de creciente importancia para la competitividad de las empresas, en donde existe una falta de claridad conceptual y consenso sobre qué es y cómo se debe aplicar.

3.1.1 Principios

A medida que la industria y los gobiernos trabajan juntos para desarrollar el marco de políticas adecuado para mejorar la seguridad informática, hay seis principios rectores a seguir (Kriz, 2011). Para ser efectivos, los esfuerzos para mejorar la seguridad informática deben:

- Aprovechar las asociaciones público-privadas, las iniciativas existentes y los compromisos de recursos;
- Reflejar la naturaleza sin fronteras, interconectada y global del entorno cibernético actual;
- Ser capaz de adaptarse rápidamente a las amenazas, tecnologías y modelos de negocio emergentes;
- Basarse en la gestión eficaz de riesgos;
- Enfocarse en la sensibilización pública; y
- Centrarse directamente en los malos actores y sus amenazas.

3.1.2 Fases

(Fojón & Sanz, 2010) mencionan que en la actualidad, muchas actividades fundamentales de la sociedad se basan en el uso de las TIC, por lo que se hace necesario contar con procesos bien definidos sobre ciberseguridad de modo que se puedan mitigar los riegos. Por tal motivo, el proceso se puede dividir en tres fases: prevención, detección y reacción.

1. **Prevención:** Se deben conocer todos los riesgos y vulnerabilidades de los sistemas de modo que se puedan crear acciones y planes de gestión de la ciberseguridad con

el fin de proteger todos los activos de la organización, principalmente la información (Mylrea, Gupta, & Nicholls, 2017).

2. **Detección:** Se deben monitorear constantemente todos los procesos que hacen uso de tecnologías de información dentro de la organización con el fin de detectar cualquier actividad anormal dentro de la red o cualquier otro evento de ciberseguridad (Mylrea, Gupta, & Nicholls, 2017).
3. **Reacción:** Al momento de detectar un evento de ciberseguridad se deben poner en marcha los procesos adecuados para responder al ataque con prontitud y efectividad y en el peor de los casos se deben poner el marcha acciones que permitan minimizar el impacto del ataque (Mylrea, Gupta, & Nicholls, 2017).

3.2 Riesgos Informáticos

"Riesgo" como término general se refiere a la probabilidad de que ocurra una eventualidad no deseada. Las empresas en la actualidad de alguna manera están asociadas a sistemas informáticos donde se gestiona todo tipo de información y sufrir algún tipo de ataque podría tener resultados catastróficos. Para analizar los riesgos es necesario hacer un estudio acerca de las vulnerabilidades existentes y medir el daño que estas pueden causar, de modo que se pueda determinar si las mismas se pueden constituir en una amenaza (Baca, 2016).

3.2.1 Vulnerabilidad

Una vulnerabilidad es un punto débil donde puede o no ocurrir una amenaza. En seguridad informática, cuando una vulnerabilidad existe se puede considerar un defecto de diseño, error al implementar el sistema, mal uso de los protocolos de seguridad o personal mal intencionado ya sea interno o externo de las organizaciones.

3.2.2 Amenaza

Las amenazas son las vulnerabilidades que se convierten en causas que afectan a los sistemas de información ocasionando pérdidas significativas, estos daños pueden ser desde una simple modificación de un dato hasta la eliminación de una base de datos. De acuerdo con (François, 2016), existen varios tipos de amenazas como:

Errores y omisiones: Por lo general son errores humanos que pueden ser entradas de datos, errores de programación etc.

Fraude y robo: Este tipo de amenaza ocurre cuando una persona roba información interna o externamente. El autor menciona que internamente existe la mayor probabilidad de amenaza por la cercanía de los usuarios a la información.

Sabotaje de los empleados: Existe la posibilidad de las personas que tienen acceso a los sistemas privilegiados utilicen los accesos para cometer fechorías.

Programas maliciosos: El malware es un software malicioso que puede afectar a los equipos o redes de una empresa que pueden provocar daños a la infraestructura de las aplicaciones o datos.

Hackers: Son personas que acceden a los sistemas informáticos sin autorización ya sea desde el interior o exterior de las organizaciones, utilizando procedimientos difíciles de detectar.

Ingeniería social: Es un método muy utilizado por los delincuentes y que se centra en la recuperación de la información confidencial de las empresas, utilizando la manipulación psicológica de los usuarios o empleados.

3.3 Autenticación

La autenticación en la actualidad representa un reto para la criptografía moderna, debido a los distintos ataques informáticos que buscan interceptar la información (Morán, 2003). La utilización de servicios de certificación permite verificar la identidad de las entidades participantes a través de firmas digitales, contraseñas o por la biometría (Rodriguez & Ochoa, 2016).

Los métodos de autenticación son los procesos de verificación de la identidad de un usuario por o para un sistema donde el objetivo principal es acceder a ciertas funcionalidades o recursos que le son asignados (Morales, Fierrez, Vera, & Ortega, 2015). El proceso general de autenticación consiste en dos pasos:

1. Identificación: Se presenta la identificación de un usuario.
2. Verificación: Se comprueba la identificación del usuario.

3.3.1 Factores

Existen diversos factores que se utilizan en la autenticación (Morales, Fierrez, Vera, & Ortega, 2015), a continuación se detallan y ejemplifican cada uno de estos.

1. Algo que el usuario conoce (Ejemplo. Id y contraseña o PIN).
2. Algo que el usuario posee (Ejemplo. Tarjetas electrónicas, Smart Card).
3. Algo que la persona es (Ejemplo. Huella digital, reconocimiento facial, iris).
4. Algo que el usuario hace (Ejemplo. Reconocimiento de voz, escribir, caminar).

3.4 Riesgos en procesos de autenticación

(Misbahuddin, Bindhumadhava, & Dheeptha, 2017) establece que varios sistemas y aplicaciones en la red son blancos de ciberataques debido a que la gran mayoría aún confía en métodos simples de autenticación para proteger los datos de sus usuarios. Sin embargo, los riesgos son muchos y pueden deberse a diversos factores que las organizaciones deben tomar en cuenta para poder garantizar a sus clientes la privacidad de sus datos.

3.4.1 Credenciales poco robustas

La gran mayoría de sistemas usan autenticación tradicional con el par usuario/contraseña, el cual es el método de autenticación más susceptible a ataques por parte de hackers en la red (Misbahuddin, Bindhumadhava, & Dheeptha, 2017). La creación de una contraseña con un mayor nivel de complejidad y extensión puede lograr un alto nivel de seguridad al autenticar al usuario a través de Internet (Venkatesh, Gopal, Meduri, & Sindhu, 2017).

3.4.2 Ataques de fuerza bruta

De acuerdo con (Zapata, 2012) este método consiste en formar palabras combinando caracteres de uno en uno y probando hasta que se consiga la clave correcta, y en caso de que el sistema no cuente con un límite de intentos de ingreso, entonces la tarea de los atacantes será mucho más sencilla.

(Waheed, Shah, & Khan, 2016) menciona dos tipos de ataques:

1. Ataque dirigido: Este tipo de ataque es utilizado para adivinar la contraseña correcta por muchos intentos. En esto, el atacante está adivinando algunas palabras del diccionario. Puede haber muchos intentos de inicio de sesión para adivinar la contraseña exacta.

2. Ataque de arrastre: En el arrastre, el atacante toma una contraseña y trata de encontrar el nombre de usuario relacionado con esa contraseña. Es totalmente inverso al ataque dirigido.

3.4.3 Robo de credenciales

El robo de credenciales es un problema muy común debido a que conociendo las credenciales de un usuario, es posible acceder no solo a su información personal sino también a información vital para la organización además de otros activos (Wilcox & Bhattacharya, 2016).

En el robo de credenciales, (Plaza, 2014) establece que es posible hacerse con las credenciales de clientes o usuarios de sistema por medio diversas herramientas y métodos como los spywares y keyloggers.

3.4.4 Falta de mecanismos de protección en la comunicación

Se debe tomar en cuenta mecanismos para asegurar la transmisión segura de la información de un equipo a otro haciendo uso de diversos protocolos criptográficos que protejan la información que es ingresada por los usuarios y enviada a los diversos servidores donde funcionan los sistemas de los cuales hacen uso (Kumar & Khurshid, 2014).

3.5 Keylogger

Es un tipo de spyware cuyo principal objetivo es guardar cada pulsación del teclado de un dispositivo (Smartphone, computadora), sin el consentimiento de la víctima. Algunas empresas lo utilizan con fines de seguridad, pero también pueden ser utilizados con fines delictivos (Kaspersky, 2018).

3.5.1 Características

(Wazid, et al., 2013) menciona que dentro de las múltiples características que posee este tipo de malware, las más comunes hacen referencia a la capacidad de éstos programas para registrar las teclas que son pulsadas en el teclado del equipo infectado, su presencia en un equipo no puede detectarse con facilidad ya que no aparecen en la lista de programas instalados, son prácticamente invisibles ante los antivirus y permiten apoderarse de información sensible para los usuarios como credenciales de ingreso a bancos, entre otros.

3.5.2 Funcionamiento

De forma simple, un keylogger es instalado en un equipo y comienza a registrar todo lo que se digita en el teclado para luego almacenarlo y enviarlo a través de la red hacia otro equipo o servidor (ver *Figura 1*), donde el atacante puede acceder y recuperar la información para luego disponer de ella a su gusto (Moses, Mercado, Larson, & Rowe, 2015).

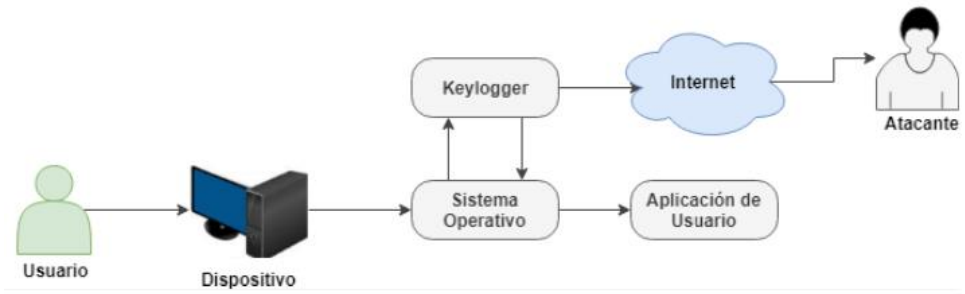

Figura 1. Funcionamiento del keylogger

Fuente: (Rahim, et al., 2018)

3.5.3 Tipos de keylogger

A pesar de los importantes esfuerzos comerciales y de investigación, los keyloggers aún representan una importante amenaza de robo de información personal y financiera debido a que

pueden implementarse como pequeños dispositivos de hardware, o de forma más conveniente, en el software (Ladakis, Koromilas, Vasiliadis, Polychronakis, & Ioannidis, 2013).

- **Keyloggers de hardware:** se encuentran instalados en la computadora y el teclado como un dispositivo físico, el cual registra la actividad de este en una memoria interna. El hardware del keylogger está disponible para trabajar con cualquier tipo de teclados (Plaza, 2014).
- **Keyloggers de software:** registran y monitorean las pulsaciones y datos dentro del sistema operativo de destino, almacenan esta información en el disco duro o en ubicaciones remotas, y la envían al atacante (Pathak, Pawar, & Patil, 2015). Se puede encontrar en cualquier tipo de programas que están en la red, al igual que también pueden ser una ayuda para los administradores de redes, ya que pueden saber que están realizando los usuarios en sus horas laborales (Plaza, 2014).

3.5.4 Formas de contagio

De acuerdo con (Pathak, Pawar, & Patil, 2015), los keyloggers se propagan de la misma manera que se propagan otros algoritmos maliciosos, dejando de lado el caso en el que el keylogger es comprado con fines positivos y/o de seguridad. Las principales formas de contagio son:

- Un keylogger puede posiblemente ser instalado después de abrir un archivo adjunto al correo electrónico.
- Cuando se inicia un archivo desde un directorio de acceso abierto en una red Peer-To-Peer (P2P), se puede instalar un keylogger.
- Un keylogger se puede instalar a través de un sitio infectado.

- Un programa malicioso puede ser instalado por otro programa malicioso presente en la máquina de la víctima.

3.6 Métodos de prevención

3.6.1 Firewall

Es una barrera que protege a todo sistema de cualquier código maliciosos o paquete sospechoso que provenga de la red y que infecte los puertos de comunicación. El firewall decide qué paquetes deben pasar y cuáles deben ser bloqueados (Plaza, 2014).

Muchos tipos de firewalls son capaces de filtrar el tráfico de datos que intenta salir de la red al exterior, evitando así que los diferentes tipos de código malicioso, virus y gusanos, entre otros, sean efectivos.

3.6.2 Antispyware

(Kwak, McAlister, & Jung, 2011) considera al antispyware como un programa capaz de identificar o detectar spyware malicioso en el equipo y neutralizarlo completamente, protegiendo la privacidad de los usuarios.

3.6.3 Antikeylogger

Para (Arora, Sharma, & Chauhan, 2016), un antikeylogger es un tipo de software diseñado específicamente para la detección de keyloggers; a menudo, dicho software también incorporará la capacidad de eliminar o al menos inmovilizar el malware keylogger.

En comparación con la mayoría de los programas antivirus o anti-spyware, la principal diferencia es que un anti-keylogger no hace una distinción entre un programa legítimo de keylogger y un programa ilegítimo (como malware); todos los keyloggers serán marcados y eliminados (opcionalmente).

3.6.4 Monitores de red

(Mollo, 2013) menciona que, en general, los monitores de red (llamados también cortafuegos inversos) se pueden utilizar para alertar al usuario cuando el keylogger use una conexión de red. Esto da al usuario la posibilidad de evitar que el keylogger envié la información obtenida a terceros.

3.6.5 Otros métodos

La mayoría de los keyloggers pueden ser engañados sin usar un software especializado en su combate (Mollo, 2013). A continuación se mencionan algunos de éstos métodos que son efectivos especialmente para evitar el robo de credenciales de acuerdo a lo expuesto por (Waheed, Shah, & Khan, 2016):

- **Criptografía de clave pública:** Se generan dos claves relacionadas matemáticamente. Esas claves son clave pública y clave privada. El mensaje enviado a través de la red se puede cifrar mediante el uso de una clave pública o una clave privada. La desventaja puede ser el mayor uso de energía y el costo para el cálculo. También el costo de una comunicación significativa puede ser la otra desventaja (Jaballah, Meddeb, & Youssef, 2010).
- **Patrón de clics:** En este método, la contraseña ingresada es el patrón de clics del mouse realizados por el usuario y se puede disfrazar colocando varias imágenes a las cuales el usuario debe hacer clic. Además, el ritmo de clics del usuario también sirve para verificar la autenticación del mismo. La ventaja es que no se requiere de hardware adicional (Raza, Iqbal, Sharif, & Haider , 2012).
- **Basado en teléfono móvil:** Un teléfono móvil se utiliza como token mediante la criptografía pública y la autenticación Secure Socket Layer (SSL). Es útil

principalmente en sistemas bancarios. En esta técnica, el teléfono móvil se utiliza para visitar algunos sitios web deseados y se establece una conexión entre el teléfono del cliente y el sitio web del banco para la autenticación. De esta manera, a un cliente no le preocupa la memorización de las contraseñas largas (Bonneau, Herley, Van Oorschot, & Stajano, 2012).

- **OTP vía SMS:** El usuario solicita la autenticación mediante el ingreso de algún ID y recibe una contraseña a través del SMS. Esa contraseña llamada OTP solo se puede usar una vez. Cuando se aplica ese código o contraseña específica, se inicia el proceso que se muestra en la *Figura 2* (Blauw & Von Solms, 2014), en la cual podemos observar a un usuario que envía una transacción al servidor, el mismo que genera una OTP y la entrega al dispositivo móvil del usuario, este envía la OTP de vuelta al servidor para su verificación y, de ser exitosa ejecuta la transacción.

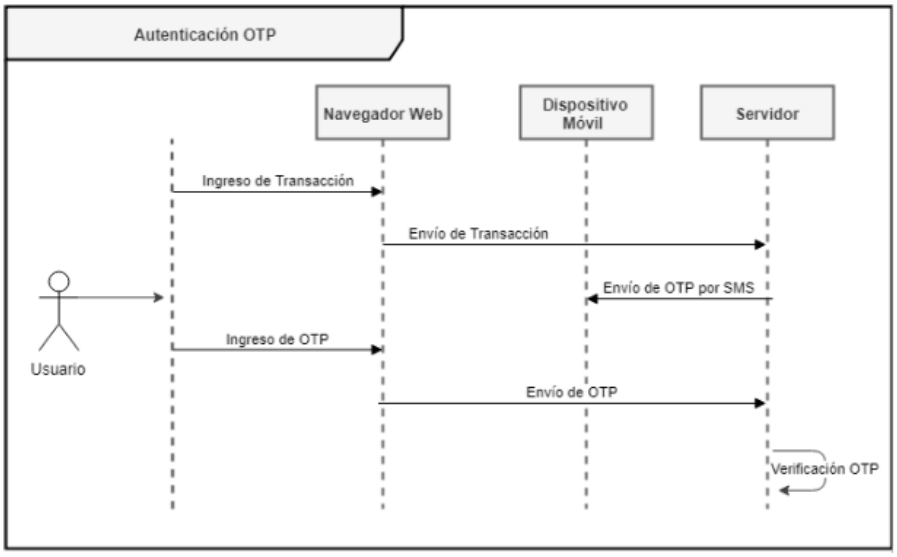

Figura 2. Autenticación OTP

Fuente: (Waheed, Shah, & Khan, 2016)

CAPÍTULO IV

METODOLOGÍA

En esta sección se detallan las metodologías empleadas en el desarrollo del método propuesto para el ingreso alternativo de credenciales.

4.1 Metodología basada en prototipos

La metodología basada en prototipos funciona como cualquier otra metodología de desarrollo de software, es decir, se cumplen las mismas actividades de análisis, diseño, implementación y evaluación que en las metodologías tradicionales pero con la diferencia de que es un ciclo repetitivo, en el cual se va modificando el prototipo hasta que este cumple con las expectativas y necesidades del usuario. Para esto se requiere de gran habilidad en comunicación, organización y control, con el fin de poder construir prototipos útiles en cada iteración y así no desperdiciar recursos (Mayhew & Worsley, 1992).

4.1.1 Características

Este modelo en particular presenta las siguientes características de acuerdo con (Wu, Chen, Liu, & Liu, 2010):

- El prototipo permite visualizar el sistema de forma rápida, de modo que el cliente puede comprender qué es lo que se está desarrollando desde el inicio del proceso, reduciendo así la incertidumbre.

- Se desarrolla en función de las necesidades y requisitos del cliente.

- Se requiere de una buena comunicación entre el cliente y los desarrolladores, de modo que con cada prototipo se pueda ir mejorando la calidad del sistema, encontrando

malentendidos o cambiando requisitos a través de la evaluación y retroalimentación oportuna.

- Reduce los costos de mantenimiento en el largo plazo.
- Se centra más en el desarrollo que en la documentación, aunque igual se realiza.

4.1.2 Ventajas frente a otras metodologías

La metodología basada en prototipos fue seleccionada ya que presenta las siguientes ventajas en comparación a otras metodologías:

- Sirve para que el cliente comprenda el trabajo que se está realizando en poco tiempo y al mismo tiempo permite a los desarrolladores construir algo de inmediato (Méndez, 2006).
- Permite evaluar de forma más adecuada la eficacia de algún algoritmo, el diseño de las interfaces de usuario o el funcionamiento del sistema en determinados entornos (Pressman, 2010).
- Recomendada para sistemas pequeños y/o medianos con equipos de desarrollo reducidos (Gutiérrez, 2011).
- El prototipo es evaluado por el cliente en cada iteración y con la retroalimentación se hacen los cambios o ajustes necesarios hasta cumplir con los requisitos establecidos por el cliente (López, Vargas, Reyes, & Vidal, 2011).
- Es más probable que el producto final satisfaga el deseo del usuario de apariencia, sensación y rendimiento (Ganpatrao & Dani, 2012).

4.1.3 Fases de la metodología basada en prototipos

El proceso inicia con la comunicación, en donde las partes interesadas se reúnen para definir los objetivos generales del software así como los requisitos que se espera cumpla el sistema en primera instancia (Méndez, 2006).

Una iteración de prototipos se planifica rápidamente, y se realiza el modelado (en forma de un "diseño rápido"). De acuerdo con (Pressman, 2010), un diseño rápido se centra en una representación de aquellos aspectos del software que serán visibles para los usuarios finales (por ejemplo, el diseño de la interfaz humana o los formatos de visualización de salida). El diseño rápido conduce a la construcción de un prototipo.

Posteriormente el prototipo será desplegado y evaluado por las partes interesadas, quienes proporcionarán comentarios que se utilizarán para refinar los requisitos (Méndez, 2006).

La iteración se produce a medida que el prototipo se ajusta para satisfacer las necesidades de varias partes interesadas, mientras que al mismo tiempo permite comprender mejor lo que se necesita hacer. En la *Figura 3* se muestran las fases que componen esta metodología:

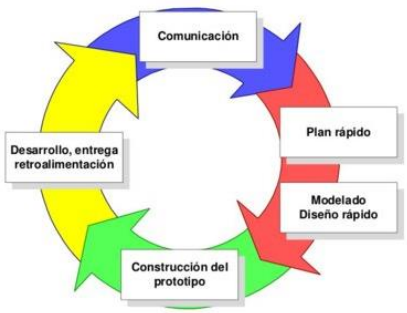

Figura 3. Metodología basada en prototipos

Fuente: (Pressman, 2010)

4.2 Investigación Acción

Para el desarrollo del proyecto se aplicará la metodología denominada "Investigación-Acción", propuesta por (Susman, 1978) y (Baskerville, 1999), el método tiene 5 fases que se comportan de forma cíclica, las etapas son: diagnosticar, planificar, actuar, observar y reflexionar, como se muestra en la *Figura 4*. Las fases de ejecución del método permiten generar nuevos conocimientos por cada iteración que se realice, de esta manera, cada vez se consigue un mejor acercamiento a la solución. Los ciclos son ejecutados iterativamente hasta tener la solución final del problema.

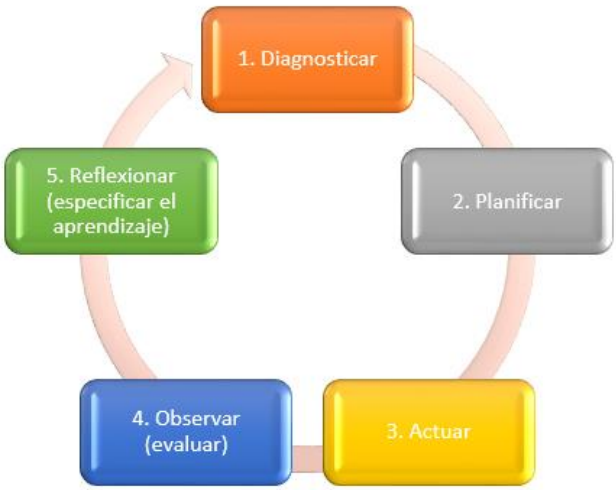

Figura 4. Ciclo de la Metodología Investigación Acción

Fuente: (Baskerville, 1999)

4.2.1 Características

Rodriguez (Rodríguez et al., 2011), menciona las características más significativas de la metodología:

- **Cíclica, recursiva:** Etapas se repiten en una secuencia similar.
- **Participativa:** Los involucrados se implican como participantes activos, en el proceso de investigación.

- **Cualitativa:** Es de carácter cualitativa, usa más lenguaje que los números.
- **Reflexiva:** Reflexión crítica sobre el proceso y los resultados por cada iteración.

Se ha optado por utilizar la metodología Investigación-Acción, porque por su naturaleza iterativa, se adapta al desarrollo del método alternativo de ingreso de contraseñas, permitiendo conseguir mejoras en cada versión y así llegar a una final definitiva.

CAPÍTULO V

DESARROLLO DE LA PROPUESTA

5.1 Análisis

Dando cumplimiento a las fases de la metodología basada en prototipos seleccionada para el desarrollo del método propuesto para el ingreso alternativo de credenciales, a continuación se presenta los requisitos identificados a modo de historias de usuario. Adicional se presenta el diagrama de casos de uso que será considerado para el desarrollo de la aplicación.

5.1.1 Requisitos identificados

Una historia de usuario es la descripción de una funcionalidad que debe ser incorporada a un sistema de software, y cuya implementación aporta valor al cliente (Tenstep, 2014). Las historias de usuario descritas en las tablas [3 - 6], detallan todas las funcionalidades que conforman el método alternativo de ingreso de credenciales propuesto por los investigadores.

Tabla 3
Historia de usuario HU01

Id	HU01
Nombre	Escanear código QR de identificación de acceso alternativo.
Descripción	El usuario podrá escanear el código QR que aparecerá en el formulario de acceso al sistema.
Entradas	Código de identificación de acceso alternativo.
Salidas	Representación gráfica de espera a recepción de credenciales en la extensión.
Proceso	1. Acceder al formulario de inicio de sesión del sistema. 2. Escanear el código QR de identificación de acceso alternativo.
Precondiciones	El acceso al formulario de inicio de sesión del sistema debe realizarse por medio del web browser Mozilla Firefox que cuente con la extensión del metodo alternativo de ingreso de credenciales instalado. El escaneo del código QR debe hacerse con la aplicación movil del método alternativo de ingreso de credenciales.

CONTINÚA

Post condiciones	Se habrá enlazado el formulario de acceso al sistema con la aplicación del dispositivo móvil del usuario.
Prioridad	Alta
Rol que lo ejecuta	Usuario

Tabla 4
Historia de usuario HU02

Id	HU02
Nombre	Enviar credenciales de acceso al sistema.
Descripción	El usuario podrá enviar sus credenciales de acceso al sistema desde su dispositivo móvil.
Entradas	Credenciales de usuario de ingreso al sistema.
Salidas	Representación gráfica de recepción exitosa de credenciales en la extensión.
Proceso	1. Ingresar credenciales de acceso al sistema en la aplicación móvil. 2. Enviar credenciales ingresadas.
Precondiciones	El codigo QR de identificación de acceso alternativo debe haber sido escaneado.
Post condiciones	El usuario habrá enviado sus credenciales de acceso al sistema desde su dispositivo móvil.
Prioridad	Alta
Rol que lo ejecuta	Usuario

Tabla 5
Historia de usuario HU03

Id	HU03
Nombre	Recibir PIN temporal de ingreso al sistema.
Descripción	El usuario recibirá un PIN temporal que le permitirá ingresar al sistema.
Entradas	-
Salidas	PIN temporal de ingreso al sistema.
Proceso	1. Esperar respuesta con el PIN temporal de ingreso al sistema.
Precondiciones	El usuario debe haber enviado sus credenciales de acceso al sistema por medio de la aplicación móvil.

CONTINÚA

Post condiciones	El usuario recibirá el PIN temporal de ingreso al sistema.
Prioridad	Alta
Rol que lo ejecuta	Usuario

Tabla 6
Historia de usuario HU04

Id	HU04
Nombre	Enviar PIN temporal de ingreso al sistema.
Descripción	El usuario podrá enviar su PIN temporal de ingreso al sistema desde la extensión.
Entradas	PIN temporal de ingreso al sistema.
Salidas	-
Proceso	1. Igresar PIN temporal de acceso al sistema en la extensión. 2. Enviar PIN ingresado.
Precondiciones	El usuario debe haber recibido en la aplicación de su dispositivo móvil un PIN temporal de ingreso al sistema.
Post condiciones	El usuario habrá iniciado sesión en el sistema.
Prioridad	Alta
Rol que lo ejecuta	Usuario

Requerimientos de Seguridad

- El sistema mantendrá la confidencialidad de la información procesada.
- El sistema no almacenará ningún tipo de información recibida.

5.1.2 Diagrama de casos de uso

Un caso de uso describe el comportamiento sobre cómo interactúa el usuario con el sistema en situaciones específicas (Pressman, 2010).

La propuesta del método alternativo de ingreso de credenciales señala al usuario como único actor, este puede escanear el código QR de identificación de acceso alternativo, enviar

sus credenciales de acceso al sistema, recibir el PIN temporal de ingreso y finalmente enviar el PIN desde la extensión instalada en el web browser para completar el proceso de inicio de sesión.

Es importante mencionar que las acciones definidas para el usuario son secuenciales, como los indica la Figura 5 y se realizan en uno de los componentes que conforman el método propuesto, sea esta la extensión del web browser o la aplicación móvil.

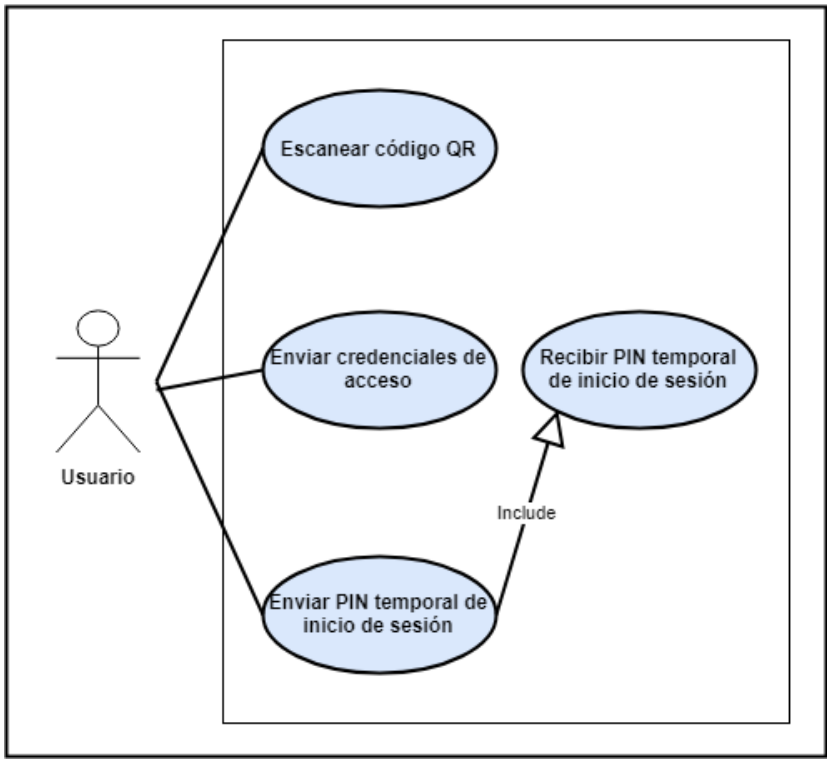

Figura 5. Casos de uso - Usuario

5.2 Diseño

Una vez que los requisitos funcionales fueron identificados y se definió el diagrama de casos de uso, se presentan los diagramas de arquitectura y secuencia con los cuales se muestra la operatividad del método alternativo de ingreso de credenciales propuesto.

5.2.1 Diagrama de Arquitectura

Un diagrama de arquitectura ayuda a plantear una vista completa del sistema que se va a construir, mostrando la estructura y organización de los componentes de software (Pressman, 2010).

La Figura 6 muestra la arquitectura con la que fue diseñado el método alternativo de ingreso de credenciales propuesto. Se puede observar la interacción que tiene el usuario con los componentes del método en las diferentes fases del proceso de inicio de sesión, el cual empieza con el acceso a la página de ingreso al sistema académico Mi ESPE, acción detectada por la extensión instalada en el web browser Mozilla Firefox que por medio de una petición a la API Rest implementada, obtiene un identificador de acceso alternativo, que es presentado al usuario como un código QR.

El proceso continúa con el escaneo del código QR por medio de la aplicación móvil Android instalada en el dispositivo personal del usuario, la cual interpreta el código QR y habilita el ingreso de las credenciales de acceso al sistema. Toda esta información ingresada a la aplicación móvil, es enviada por medio de una petición a la API Rest al servidor, que se encargará de relacionar estas credenciales con el identificador de acceso alternativo generado anteriormente, proceso que tendrá como respuesta a la aplicación móvil un PIN que actúa como una OTP.

Finalmente, el usuario deberá ingresar el PIN mostrado en su dispositivo a la interfaz del elemento agregado por la extensión de navegador a la página de ingreso al sistema Mi ESPE, nuevamente se hará una petición al servidor que recibirá el PIN y responderá con las credenciales de acceso al sistema, mismas que serán procesadas por la extensión y se tendrá como resultado el inicio de sesión al sistema.

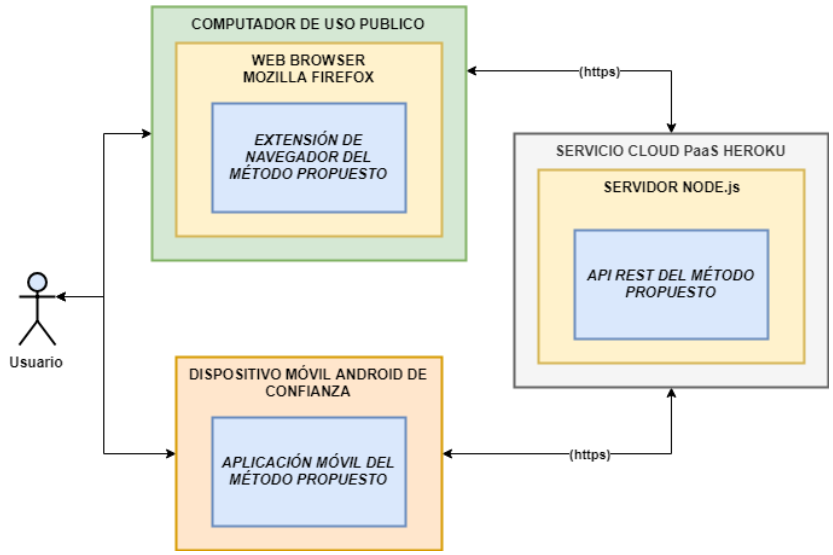

Figura 6. Diagrama de Arquitectura

5.2.2 Diagramas de secuencia

Un diagrama de secuencia se utiliza para mostrar las interacciones entre los objetos que conforman un sistema en el orden secuencial en que ocurren durante un escenario específico (Booch, 1999).

Quien utilice el método propuesto de ingreso alternativo de credenciales, deberá interactuar con dos interfaces independientes. En la Figura 7 y la Figura 8 se pueden observar las secuencias correspondientes a la interacción con la extensión del web browser y la aplicación móvil respectivamente.

El usuario ingresa a la página de inicio de sesión del sistema, evento reconocido por el complemento instalado que solicita al servidor la generación de un identificador de acceso alternativo presentado al usuario como un código QR. Este código deberá ser escaneado por medio de la aplicación móvil, acción que permitirá el envío de credenciales desde el dispositivo móvil del usuario y solicitará al servidor la generación de un PIN como una OTP que relacione el contenido del código QR presentado en el elemento agregado por la extensión a la página de

acceso al sistema, con las credenciales enviadas desde la aplicación móvil. Este PIN será devuelto al dispositivo móvil del usuario y deberá ser ingresado en el elemento agregado por la extensión del web browser para conseguir un inicio de sesión exitoso, habiendo ingresado las credenciales desde un dispositivo de confianza y no por medio del teclado del equipo de uso público que podría tener instalado un spyware keylogger.

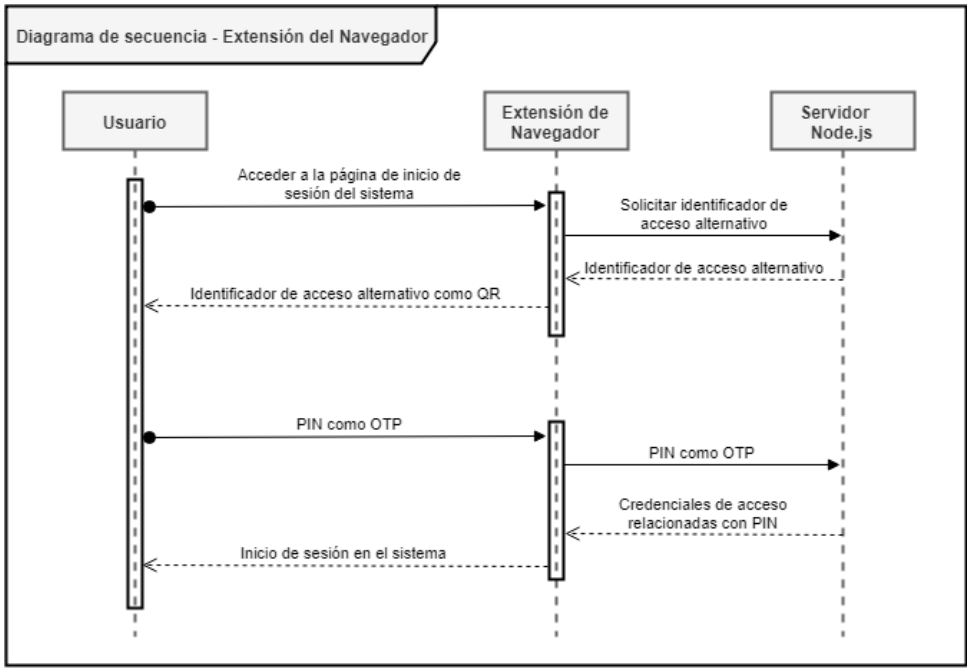

Figura 7. Diagrama de secuencia – Extensión del Navegador

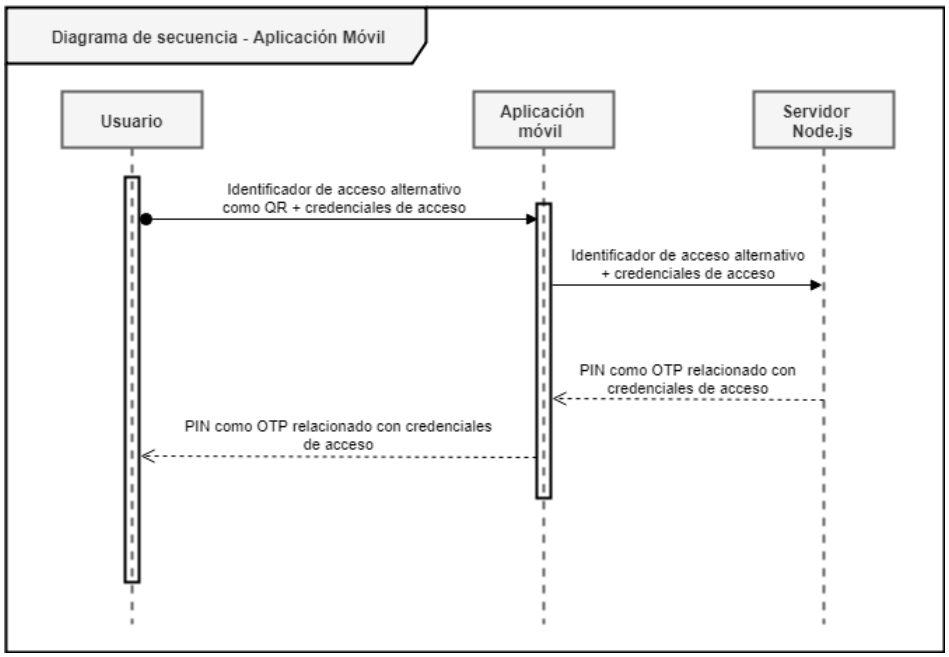

Figura 8. Diagrama de secuencia – Aplicación Móvil

5.3 Implementación

Después de haber definido los requisitos funcionales con las historias de usuario y diagrama de casos de uso, además de los no funcionales con los diagramas de secuencia y arquitectura, en esta sección se detalla la implementación del método alternativo de ingreso de credenciales propuesto.

5.3.1 Selección de herramientas

A continuación se describen las herramientas seleccionadas para el desarrollo e implementación del método propuesto:

- **NodeJS**

Es un entorno que permite la ejecución del lenguaje JavaScript de lado del servidor, lo que posibilita el manejo de eventos asíncronos orientados al diseño de aplicaciones en redes escalables (Node.js, 2018). Esta herramienta fue seleccionada para servir de intermediario en

la comunicación de la aplicación móvil con el complemento del navegador Mozilla Firefox. Se decidió escogerla como servidor de la API Rest del método propuesto debido a la gran cantidad de complementos y módulos estables que ofrece frente a otras herramientas similares aún prematuras.

- **Heroku**

Es una plataforma como servicio de computación en la nube (PaaS) que permite desplegar aplicaciones desarrolladas en distintos lenguajes de programación (Heroku, 2018). Se seleccionó este servicio cloud para realizar el despliegue del API Rest implementada en NodeJS porque a diferencia de otras plataformas en la nube, ofrece un servicio gratuito sin límite de tiempo en su versión de test y adicionalmente permite contar el protocolo de comunicación HTTPS por defecto, el mismo que es indispensable al tratarse del envío y recepción de credenciales de acceso.

- **Android Studio**

Es un entorno de desarrollo integrado (IDE) y editor de código fuente para el desarrollo de aplicaciones móviles Android, permite el desarrollo con un entorno unificado para todos los dispositivos (Google, 2018). Se utilizó esta herramienta para desarrollar la aplicación Android que permitirá el ingreso de contraseñas de manera remota al portal web académico Mi ESPE debido a que, al ser el IDE propio de Android nos permite tener acceso directo a las funciones del sistema operativo necesarias para hacer uso del hardware, en este caso la cámara, con la cual se escaneará el código QR mostrado en la extensión del navegador.

5.3.2 Implementación de la extensión del navegador

Una extensión añade funcionalidades extras a los navegadores. Se desarrollan en base a tecnologías Web: CSS, HTML y lenguaje JavaScript, este nos permite aprovechar la gran

cantidad de APIs y librerías existentes, además de brindarnos la posibilidad de crear nuestros propios componentes o módulos (MDN Web Docs, 2018).

El propósito de la extensión de navegador dentro del método alternativo de ingreso de credenciales propuesto, es el de agregar un elemento HTML adicional a la página de inicio del portal web académico Mi ESPE. Este elemento permitirá la interacción con el usuario del método alternativo de ingreso de credenciales y la comunicación con el servidor del mismo.

La Figura 9 muestra la página de inicio del portal web académico Mi ESPE sin contar con la extensión de navegador instalada, mientras que la

Figura ***10*** muestra la misma página con el elemento añadido por la extensión al haber sido agregada al navegador.

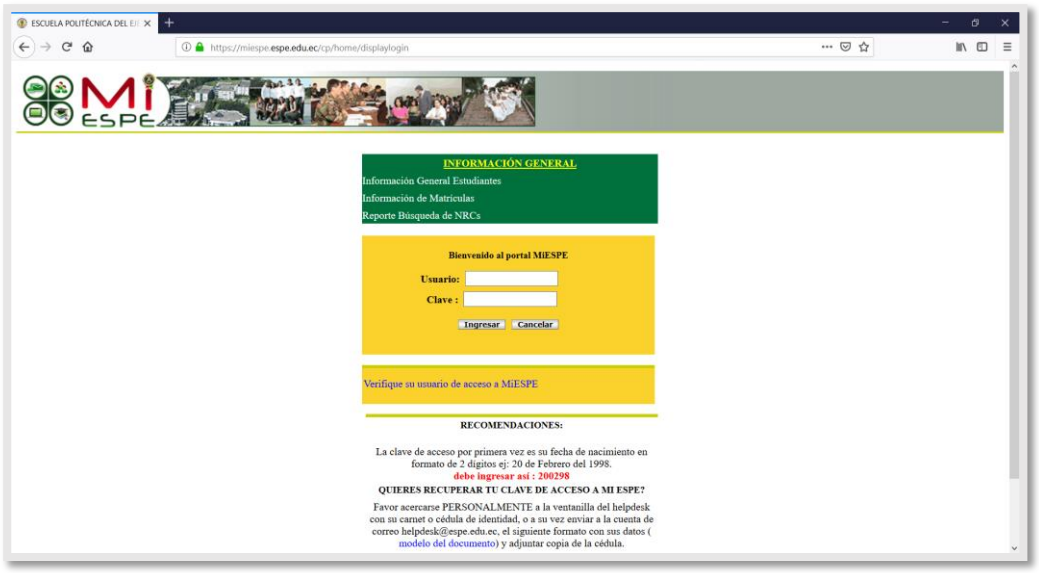

Figura 9. Extensión no instalada.

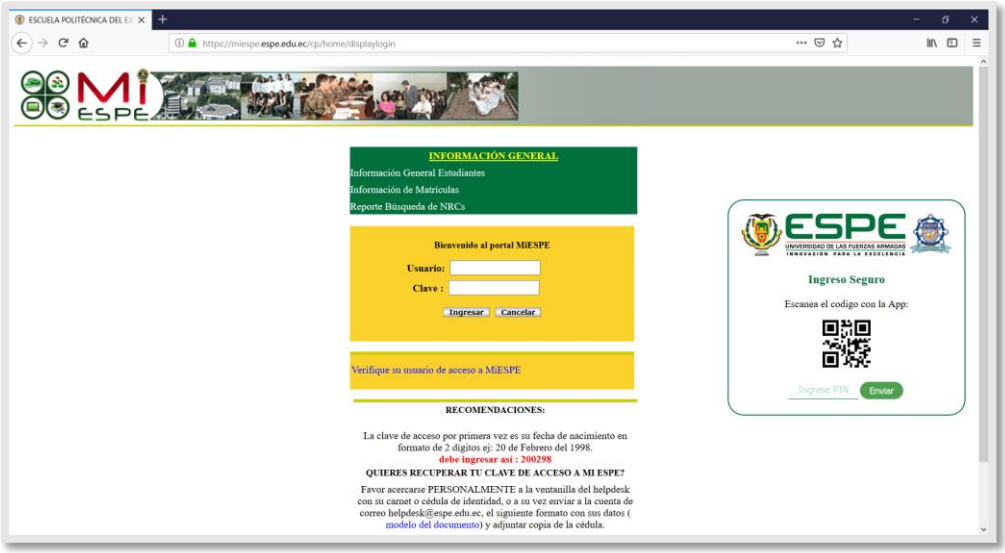

Figura 10. Extensión instalada.

5.3.3 Implementación de la Api Rest

Con el fin de facilitar la comunicación entre los componentes del método alternativo de ingreso de credenciales propuesto y debido a la sensibilidad de la información que se transmite entre ellos, se implementó una API Rest en JavaScript sobre un servidor NodeJS, el cual se encuentra alojado en la plataforma como servicio cloud (PaaS) conocida como Heroku. Esta plataforma brinda la posibilidad de contar con un certificado SSL, lo que permite garantizar la confidencialidad de la información mediante comunicaciones con el protocolo HTTPS.

En las tablas [7 - 9] a continuación, se describen los métodos pertenecientes a la API Rest mencionada.

Tabla 7
Generar identificador de acceso alternativo

Campo	Descripción	Tipo		Ejemplo
clientIDclient	Número único de identificación de usuario que accedió a la pagina de inicio del portal web academico Mi ESPE contando	Number	Obligatorio	3475

CONTINÚA

	con la extensión del método instalada en su navegador.			

Ejemplo JSON de Respuesta


```
{
   "clientIDserver": "2795"
}
```


Tabla 8

Recibir credenciales de usuario y generar PIN como OTP

Campo	Descripción		Tipo	Ejemplo
CliQrNonceScan	Identificador de acceso alternativo generado previamente.	String	Obligatorio	2795
Ruser	Nombre de usuario del sistema académico Mi ESPE.	String	Obligatorio	dnperez5
Rclave	Contraseña de ingreso al sistema académico Mi ESPE.	String	Obligatorio	******

Ejemplo JSON de Respuesta


```
{
   "clientOtpApp": "5759"
}
```


Tabla 9

Recibir PIN como OTP y enviar credenciales de usuario asociadas

Campo	Descripción		Tipo	Ejemplo
clientOtpNav	PIN ingresado por el usuario en el elemento agregado por la extensión del navegador.	String	Obligatorio	5759

Ejemplo JSON de Respuesta


```
{
   "usuario": "dnperez5",
   "clave": "*****"
}
```

5.3.4 Implementación de la aplicación móvil

Para el desarrollo de la aplicación móvil se utilizó el IDE Android Studio ya que la herramienta permite realizar tres capas (Frontend, Middleware y Backend), componentes permiten la implementación y comunicación entre capas adyacentes.

El frontend está escrito en el lenguaje XML basado en los esquemas de diseño en Android mientras que la capa del middleware está codificado en el lenguaje java y el Backend está desarrollado en el motor de base de datos SQLite.

Características de operativas de la aplicación móvil

Versión SDK:

- Compilación: versión 25
- Mínima: versión 23
- Target: versión 25

La aplicación se puede ejecutar desde la versión de Android Marshmallow 6.0 hasta la versión de Oreo 8.1.0.

Se diseñaron las siguientes pantallas que son detalladas a continuación con su descripción de implementación y funcionamiento.

La pantalla principal se muestra en la Figura 11. Se utiliza para el escaneo del código QR, está implementada con la librería zxing versión 1.9 la cual permite capturar un evento al leer un código QR. La funcionalidad de esta pantalla requiere de acceso a internet y el recurso físico de la cámara del dispositivo móvil.

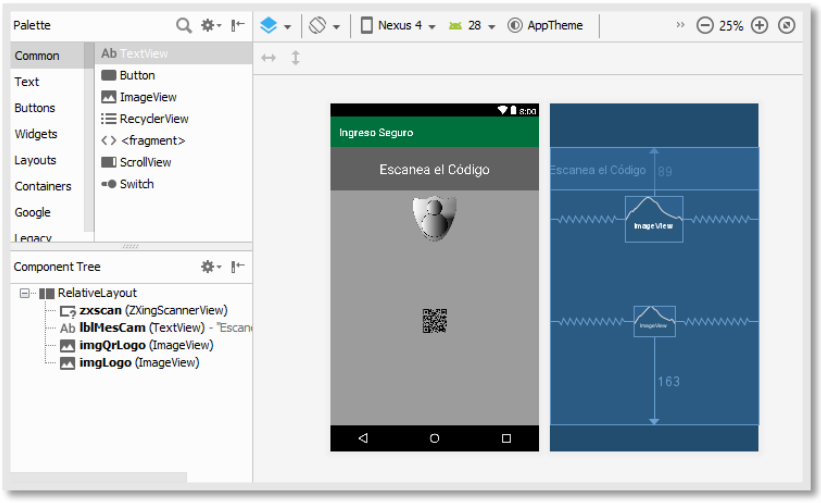

Figura 11. Pantalla inicial escaneo del código QR

En la Figura 12 se muestra el diseño del formulario de login que se utiliza para realizar a la autenticación en el sitio web Mi ESPE. La pantalla tiene la funcionalidad de implementar la comunicación con el servidor, para la conexión se utiliza la librería volley que permite realizar peticiones de tipo POST enviando un objeto JSON en el request, simultáneamente recibiendo una respuesta con un objeto del mismo tipo.

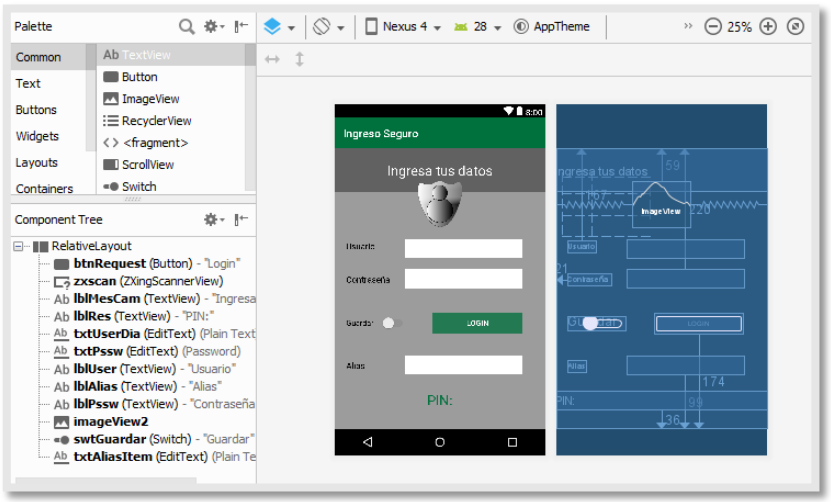

Figura 12. Pantalla formulario login

Adicionalmente para el formulario login se diseñaron dos botones flotantes como se muestra en la Figura ***13***. La función de estos elementos es regresar a la pantalla principal (en el caso del botón QR) mientras que el otro botón permite guardar la sesión que se esté utilizando en ese instante.

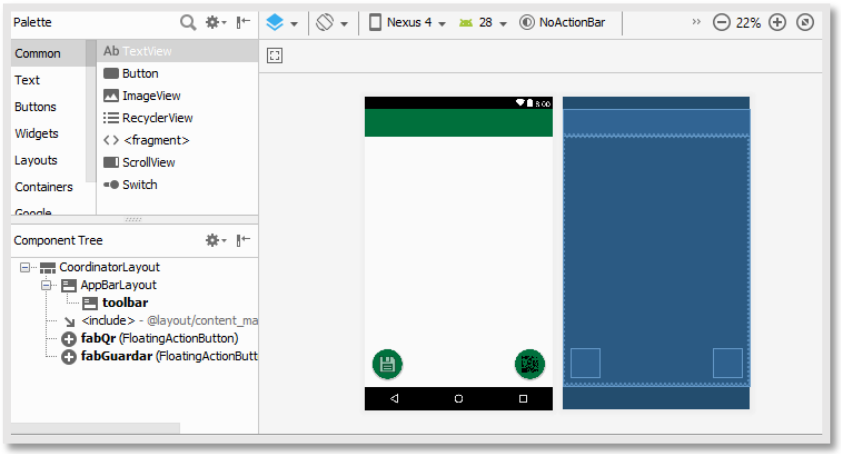

Figura 13. Diseño de botones flotantes parte del formulario login

El diseño del menú lateral izquierdo se muestra en la Figura 14, el menú tiene la funcionalidad de acceder a las sesiones guardadas por el usuario.

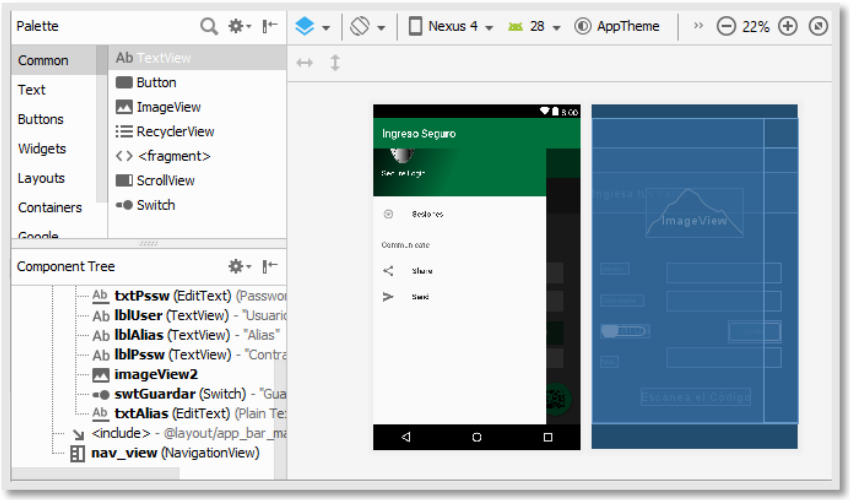

Figura 14. Menú lateral izquierdo

En la Figura 15 se muestra la vista del formulario para la creación y modificación de nuevas sesiones.

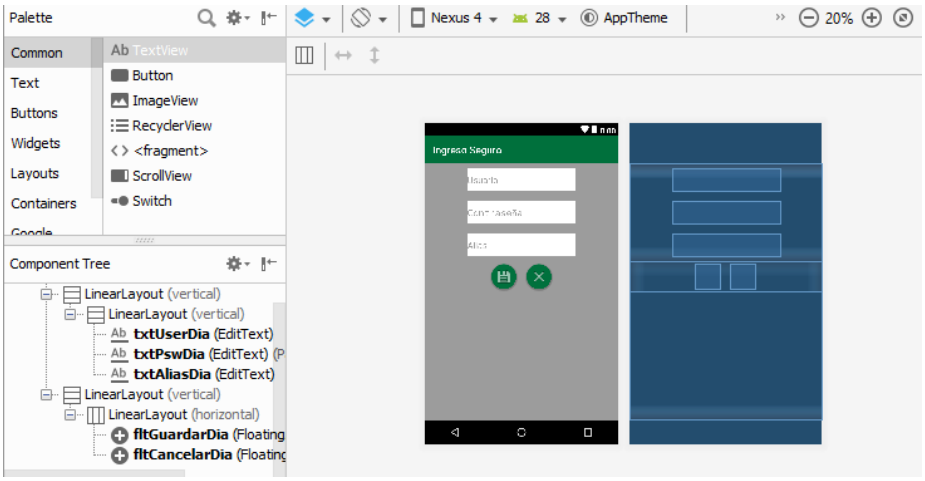

Figura 15. Formulario de creación y modificación de credenciales

5.3.5 Interacción de componentes

Finalizando el desarrollo e implementación de los componentes del método alternativo de ingreso de credenciales propuesto, se realizó la demostración de los requisitos completos, mediante la comprobación de las comunicaciones entre los componentes y la verificación de cada funcionalidad establecida en las historias de usuario.

HU01 Escanear código QR de identificación de acceso alternativo

Iniciando la aplicación en el dispositivo móvil se procede a leer el codigo QR que se genera en el sitio web como se muestra en la Figura 16. La aplicación verifica la conexión de red y el permiso de acceder a los recursos de la cámara en tiempo de ejecución (los cuales son mandatorios para continuar con el proceso). Para la primera conexión entre la aplicación y el sitio web se consume un servicio rest enviando como parámetro el valor del código QR escaneado, el resultado de esto se muestra un ícono de espera como se muestra en la Figura 17.

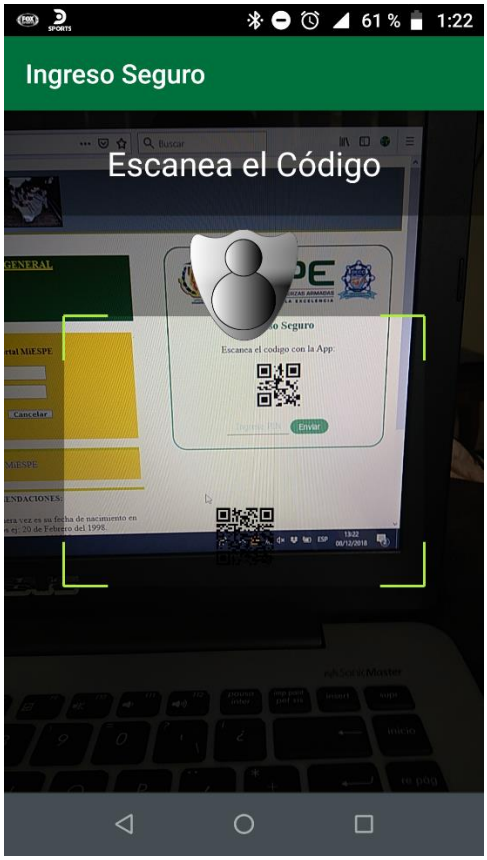

Figura 16. Escaneo del código QR desde la aplicación móvil

El sitio web ya conoce el usuario en el primer acercamiento, por lo cual está a la espera del envío de credenciales por parte de la aplicación móvil.

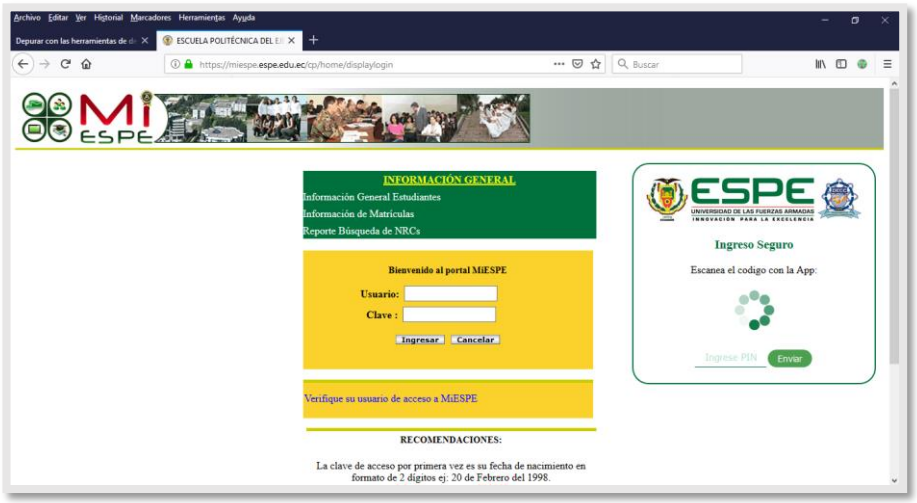

Figura 17. Resultado del proceso de escaneo del código QR en el sitio web

HU02 Enviar credenciales de acceso al sistema

Cumpliendo con la fase anterior se despliega un formulario como se muestra en la Figura 18. Aquí se deben completar los campos de usuario y contraseña con el objetivo de obtener un código de 4 digitos (OTP), el cual será ingresado en el sitio web para cumplir con la autenticación de una forma segura y desde un dispositivo de confianza.

Una vez completos los campos, se procede a presionar el boton de login y se consume un servicio rest donde la respuesta del servidor node es un objeto de tipo json.

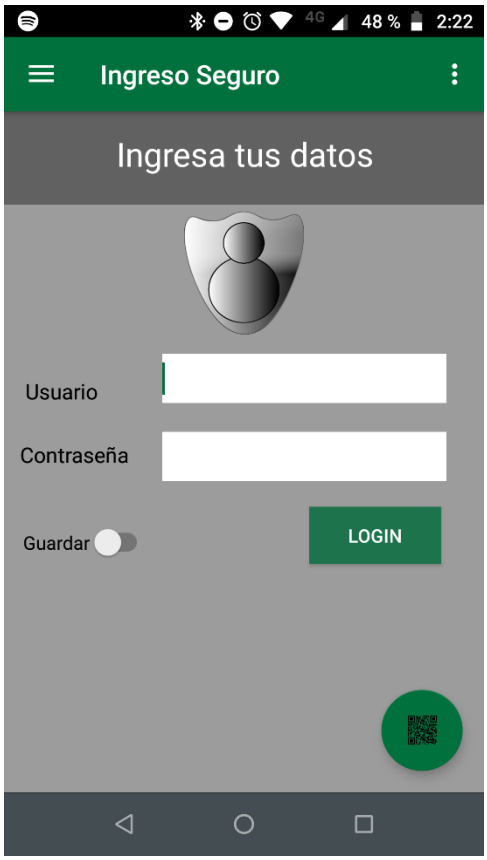

Figura 18. Formulario de acceso en la aplicación móvil

HU03 Recibir PIN temporal de acceso al sistema

Al enviar la petición al servidor, la respuesta es inmediata obteniendo el PIN que se muestra en la pantalla, ver Figura 19. Este PIN debe ser ingresado en la aplicación web para validar si es correcto y permitir el acceso a los servicios del aplicativo web Mi ESPE.

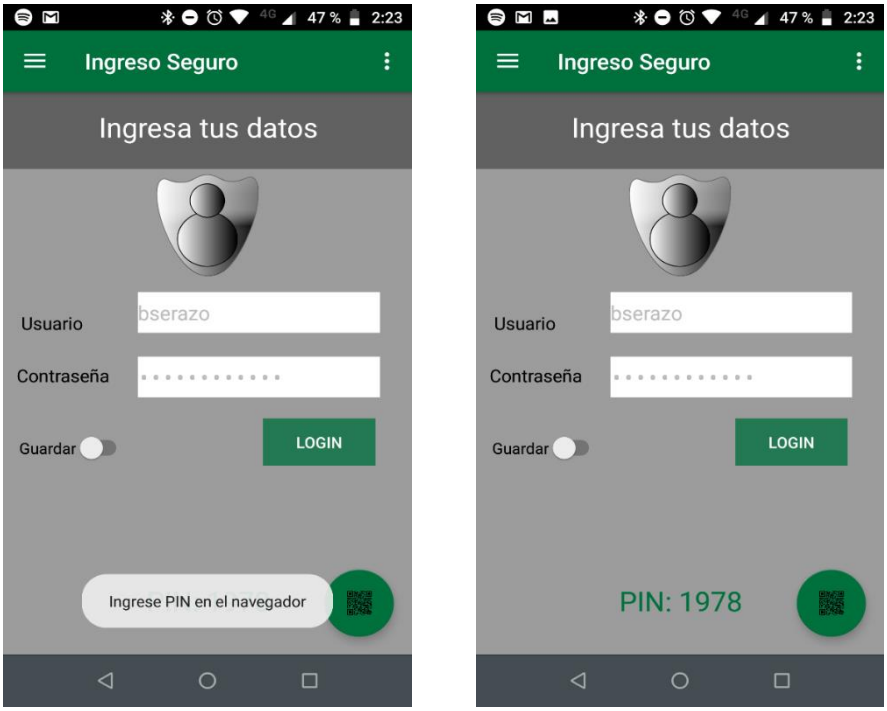

Figura 19. Obtención del pin (OTP)

HU04 Enviar PIN temporal de ingreso al sistema

Una vez recibido el PIN como OTP en la aplicación móvil, este debe ser ingresado en el elemento agregado por la extensión del navegador que se puede observar en la Figura 20 y enviado al servidor, el cual se encargará de encontrar las credenciales relacionadas con el PIN recibido y enviarlas a la extensión para que esta pueda realizar el proceso de inicio de sesión en el sistema académico Mi ESPE.

Figura 20. Ingreso y envío de PIN como OTP.

CAPÍTULO VI

EVALUACIÓN

Esta sección muestra la configuración del experimento y los resultados de las pruebas realizadas con el propósito de medir la cantidad de credenciales que pueden ser obtenidas por medio del uso de keyloggers en un determinado periodo de tiempo y grupo de personas, también presenta información acerca de las preferencias de uso de los diferentes web browsers. Adicionalmente se presentan estadísticas de aceptación y usabilidad por parte de los estudiantes de la Universidad de las Fuerzas Armadas ESPE, quienes son los usuarios potenciales en el caso de estudio del método propuesto.

6.1 Configuración del experimento

Para la configuración del experimento donde el objetivo principal es la obtención de credenciales con el uso del spyware keylogger, se planteó un escenario controlado para la ejecución. En este escenario se utilizó computadores de acceso público pertenecientes a un establecimiento que oferta servicios de internet, ubicado en los alrededores de la Universidad de las Fuerzas Armadas ESPE. En dichos equipos, se instaló la herramienta de spyware denominada “Revealer Keylogger” en su versión básica, la misma que permitió a los investigadores conseguir las capturas de pulsaciones de teclado realizadas por los usuarios y con esta información obtener los resultados que se presentan a continuación.

6.1.1 Condiciones del experimento

Para medir la obtención de credenciales de acceso por medio de spyware keylogger se realizaron pruebas en un ambiente controlado donde varios estudiantes de la Universidad de las Fuerzas Armadas ESPE consintieron ser parte del experimento. En la **Tabla 10** se presenta la descripción de las condiciones.

Tabla 10
Descripción de las condiciones en el ambiente controlado

Condiciones	Descripción
Número de participantes	50
Edad	Entre 19 y 25 años.
Nivel	3ro, 4to, 5to, 6to, 7mo, 8vo y 9no.
Carrera	Ingenierías: Sistemas, Electrónica, Civil, Mecatrónica, Mercadotecnia y Comercial.
Número de equipos	2
Spyware keylogger	Revealer Keylogger versión básica.

6.1.2 Resultados

La Tabla 11 resume la cantidad de credenciales obtenidas por la herramienta keylogger en el primer computador objeto de prueba, mismo que permitió la obtención de 17 credenciales de usuario, de las cuales 9 fueron usadas para ingresar al portal web académico Mi ESPE.

Tabla 11
Credenciales obtenidas en computador 1

Web Browser	Credenciales	Credenciales Mi ESPE
Google Chrome	12	6
Mozilla Firefox	5	3
TOTAL	17	9

La Tabla 12 muestra la cantidad de credenciales obtenidas por la herramienta keylogger en el segundo computador objeto de prueba, el mismo que permitió recuperar 23 credenciales de usuario, de las cuales 10 fueron usadas para ingresar al portal web académico Mi ESPE.

Tabla 12
Credenciales obtenidas en computador 2

Web Browser	Credenciales	Credenciales Mi ESPE
Google Chrome	16	7
Mozilla Firefox	7	3
TOTAL	23	10

La Figura 21 muestra el porcentaje de credenciales obtenidas por navegador, indicando que en el web browser Mozilla Firefox, seleccionado como navegador sobre el cual se ejecuta la extensión que forma parte del método propuesto, se ingresaron el 30% de las credenciales obtenidas en las pruebas.

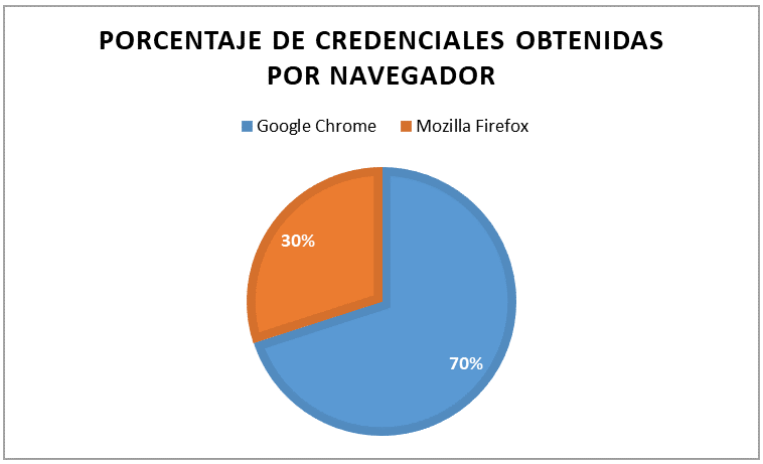

Figura 21. Porcentaje de credenciales por navegador.

La Figura 22 muestra el porcentaje de credenciales al portal web académico Mi ESPE obtenidas, en relación al total de credenciales de usuario capturadas por el keylogger. Esta mediada señala que tras una semana de pruebas en los dos computadores mencionados anteriormente se consiguieron un total de 19 credenciales de acceso válidas para la investigación.

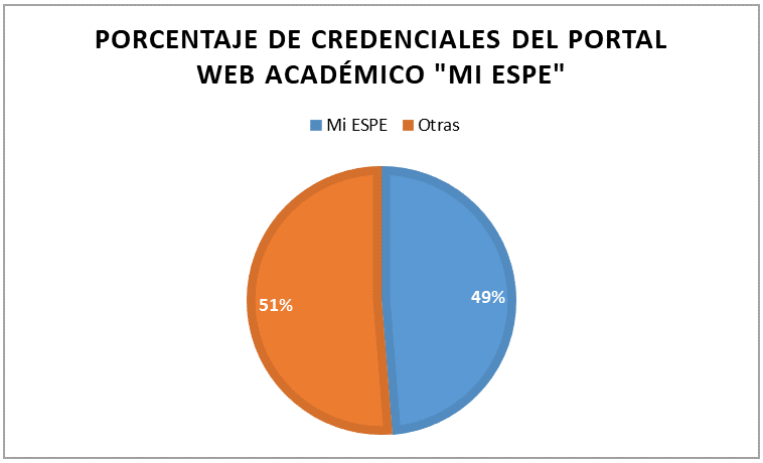

Figura 22. Porcentaje de credenciales del portal Mi ESPE.

6.1.3 Análisis de resultados

Los resultados arrojados por las pruebas realizadas, reflejan el gran peligro de robo de credenciales de acceso que se genera al utilizar equipos de uso público y, la necesidad de contar con un método alternativo de ingreso de credenciales que permita realizar el procedimiento de autenticación desde un dispositivo de confianza.

Si bien las cifras presentadas como resultado de estas pruebas no muestran grandes cantidades de credenciales obtenidas, es importante resaltar las limitaciones del escenario planteado ya que al proyectar estos resultados a los cientos de equipos que forman parte de laboratorios, bibliotecas y demás centros públicos de cómputo, las cifras serían realmente alarmantes.

Una vez terminado el experimento, se explicó el funcionamiento del método propuesto a los participantes, quienes decidieron usarlo para su inicio de sesión y de esta manera verificar que el spyware keylogger instalado en las máquinas de prueba no pudo capturar ninguna credencial de acceso, es decir, la cantidad de contraseñas expuestas fue cero.

6.2 Encuesta

En este apartado se analizó la información recolectada de las encuestas, se evidencia el número de accesos a los equipos informáticos de uso público en conjunto con la frecuencia de uso de la plataforma web Mi ESPE, también se realizaron preguntas acerca del spyware keylogger por otra parte se mostró de forma interactiva el uso del método propuesto utilizando una animación, de modo que facilite su entendimiento para evaluar la usabilidad, la encuesta está dividida en dos partes, la primera en la frecuencia de uso de equipos públicos para acceder al sitio web Mi ESPE que se encuentra en la sección 6.2.1 y la segunda para la aceptación y usabilidad del método propuesto ver sección 6.2.2.

En la Tabla 13 se detallan las características demográficas de los encuestados que corresponden a un grupo de estudiantes de la carrera de ingeniería de sistemas e informática de la Universidad de la Fuerzas Armadas ESPE.

Tabla 13
Características demográficas de los encuestados

Características	**Descripción**
Número de encuestados	56
Género	Masculino y Femenino
Edad	Entre 21 y 26 años.
Nivel	7^{mo}, 8^{vo} y 9^{no}.
Carrera	Ingeniería en Sistemas e Informática

6.2.1 Frecuencia de uso de equipos públicos para acceder al sitio web Mi ESPE

Esta sección de la encuesta está centrada en la obtención de las frecuencias del uso de las computadoras púbicas para ingresar al sitio web Mi ESPE, en el siguiente cuestionario están las preguntas que se usaron para obtener los datos.

Cuestionario

1. **Genero**
   - Masculino
   - Femenino
2. **¿Qué nivel que está cursando?**
   - 7mo
   - 8vo
   - 9no
3. **¿Cuantas veces a la semana accede a la página Mi ESPE en los equipos de los laboratorios de computación? Responda entre el valor de 1 y 10.**

   _____
4. **¿Cuantas veces a la semana accede a la página Mi ESPE en los equipos de la biblioteca? Responda entre el valor de 1 y 10.**

   _____
5. **¿Cuantas veces a la semana accede a la página Mi ESPE en los equipos de los almacenes que se encuentran en los exteriores del campus? Responda entre el valor de 1 y 10.**

   _____

6.2.1.1 Análisis y resultados

Para analizar los resultados de la primera parte se tienen los siguientes datos, en la Figura 23 se muestra el porcentaje según el género de los estudiantes encuestados pertenecientes a la Universidad de las Fuerzas Armadas ESPE, específicamente en la carrera de Ingeniería de Sistemas, teniendo como resultado un 86% de hombres y 14% de mujeres.

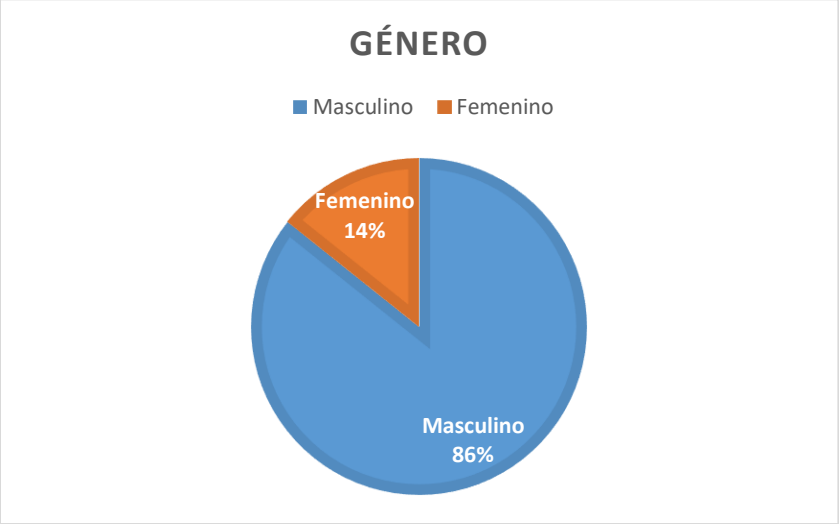

Figura 23. Clasificación de género

En la Figura 24 se muestra el nivel académico de los participantes, destacando al noveno nivel como aquel con el mayor porcentaje de participantes (75%).

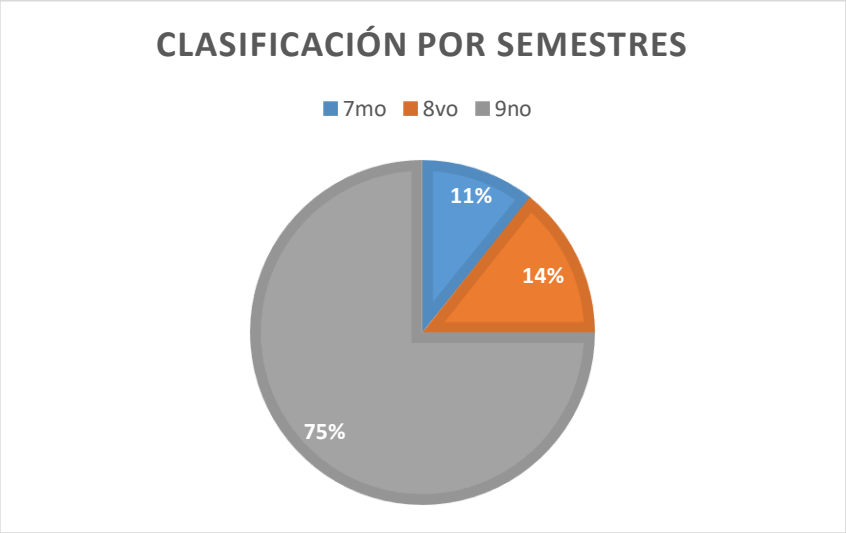

Figura 24. Porcentajes por semestres

Por otra parte, teniendo ya una clasificación entre género y nivel, se procede a detallar el porcentaje de ingresos que se realizan al sitio web Mi ESPE en una semana (cabe mencionar que el ingreso se hace a través de los equipos de los laboratorios de la universidad).

El 24% (ver Figura 25) de los encuestados ingresan al menos 10 veces al sitio, teniendo alta probabilidad de ser víctima a un ataque del spyware keylogger

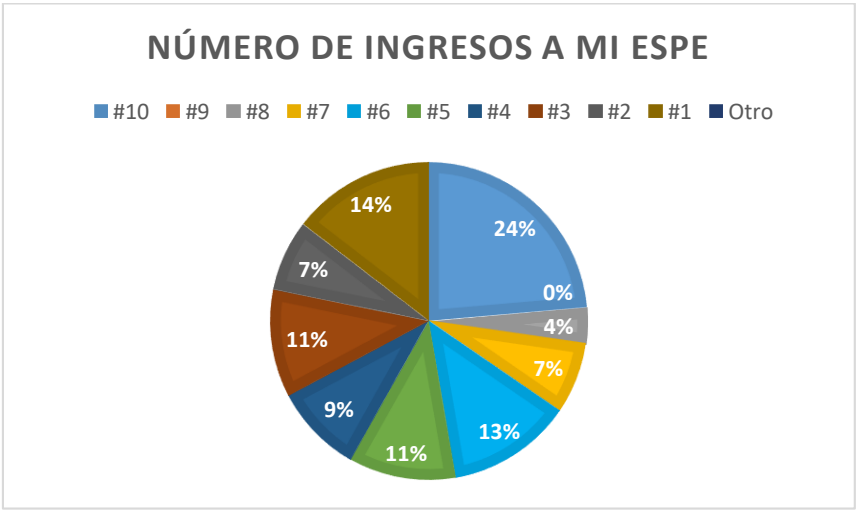

Figura 25. Cantidad de ingresos al sitio Mi ESPE en los laboratorios

El grupo encuestado en su mayoría, con el 71%, no utiliza los equipos de la biblioteca para acceder a la página web de Mi ESPE, lo que significa que la biblioteca no es un punto vulnerable para los estudiantes, ver Figura 26.

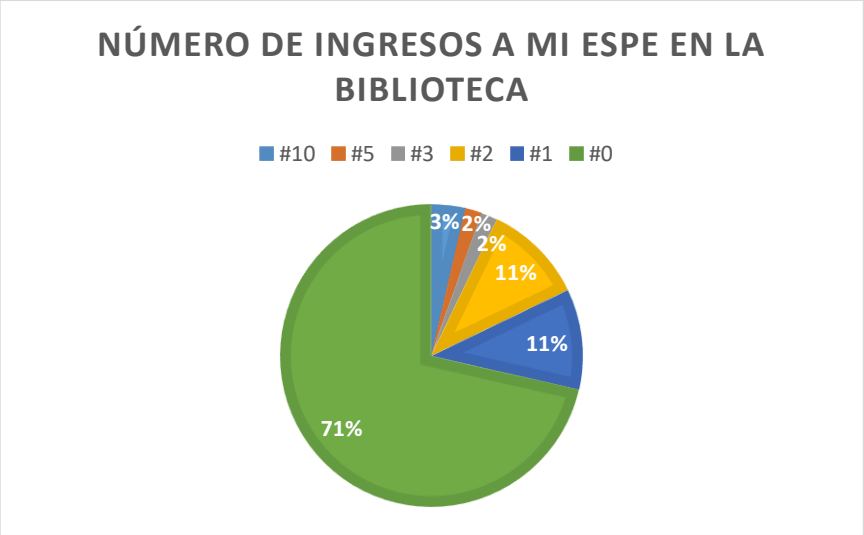

Figura 26. Cantidad de ingresos al sitio Mi ESPE en la biblioteca

Así mismo más del 50 % (ver Figura 27) de estudiantes no utiliza las computadoras en los exteriores de campus, el 18 % del grupo seleccionado indican que al menos una vez por semana ingresan al sitio de Mi ESPE y el 21% accede entre 2 y 4 veces siendo las posibles víctimas de robo de credenciales.

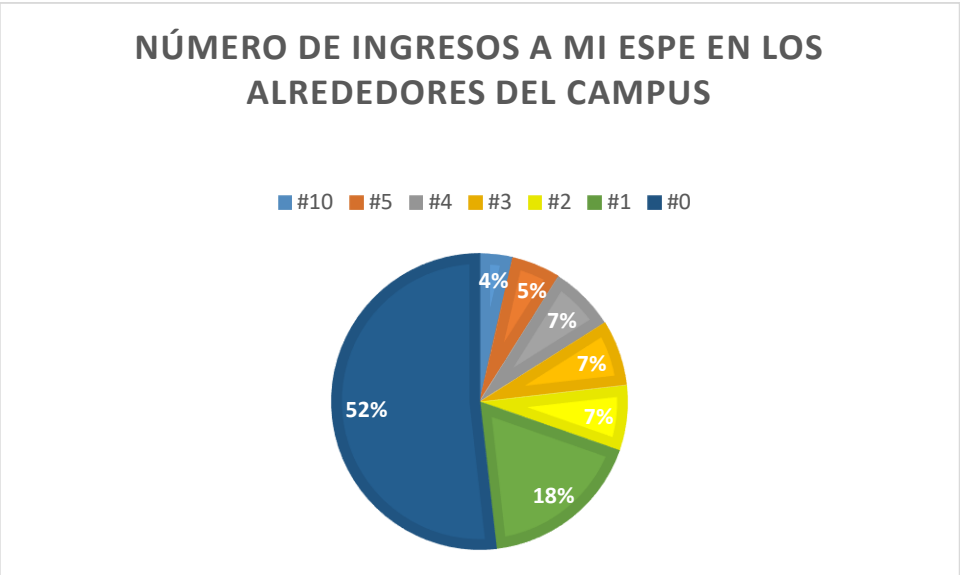

Figura 27. Cantidad de ingresos al sitio Mi ESPE alrededor del campus.

6.2.2 Aceptación y usabilidad del método propuesto

Para la ejecución de la segunda parte de la encuesta se utilizó una animación de modo que facilite el entendimiento del método desarrollado, también se tomó en cuenta el grupo de estudiantes seleccionados el cual pertenece a la carrera de ingeniería de sistemas e informática que cursan los niveles entre 7^{mo} y 9^{no} con el objetivo de obtener información de la aceptación y usabilidad de dicho método, a continuación se muestran las preguntas planteadas.

Cuestionario

1. **¿Conoce el Spyware Keylogger?**
   - Si
   - No
2. **En el caso de responder "Si" la anterior pregunta detalle cual es función principal del malware Keylogger:**

   _____

   _____

   _____

3. **Ver método propuesto en el siguiente link y comente su criterio del método si es usable o no: http://redlinehuasi.com/giftesis/final.gif**

   _____

   _____

   _____

4. **¿Al utilizar el método propuesto la seguridad es?**
   - Baja

- Media
- Alta

5. **Utilizaría el método propuesto para la autenticación en el sitio web Mi ESPE?**
    - Si
    - No
    - Talvez

6.2.2.1 Análisis y resultados

Para comenzar el análisis se planteó la siguiente pregunta: ¿Conoce el Spyware Keylogger? (Si o No), cuyo objetivo es determinar el conocimiento del grupo encuestado sobre este tipo de malware, arrojando los siguientes resultados positivos con el 75% de 56 estudiantes, ver

Figura ***28***. También se realizó la segunda pregunta: ¿Cuál es la función principal del malware Keylogger?, obteniendo en su mayoría definiciones acertadas del funcionamiento de los keyloggers, a continuación se muestran algunas definiciones recolectadas.

Definición de la función del keylogger por parte de los estudiantes

- Almacenar todo lo que se digita en el teclado.
- Es un software que guarda todo lo que se escribe en un teclado.
- Registrar lo que se digita en el teclado.
- Capturar las teclas presionadas.
- Registrar las pulsaciones del teclado y enviarlas a un equipo externo o simplemente grabarlas en la computadora localmente.

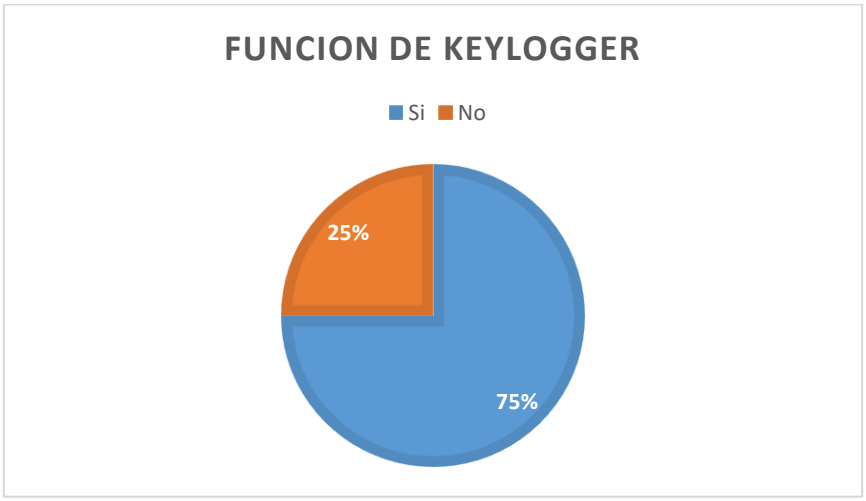

Figura 28. Porcentaje de conocimiento acerca de los keyloggers

Para establecer el nivel de aceptación una vez ya entendido el funcionamiento del método se realizó la pregunta: ¿Utilizaría el método en el sitio Mi ESPE?, teniendo un porcentaje considerable de aceptación con el 72% (ver Figura 29) de los encuestados.

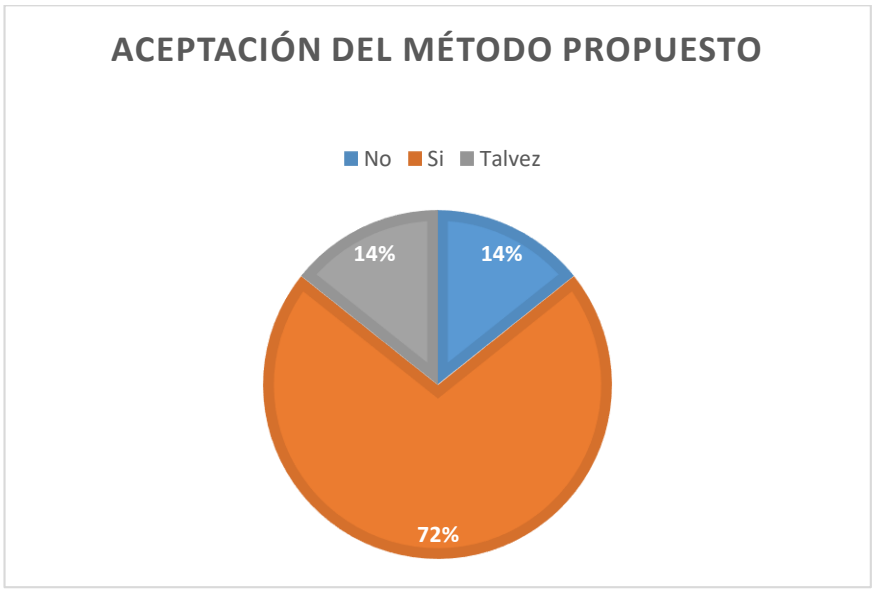

Figura 29. Porcentaje de aceptación del método propuesto

Para la usabilidad del método se utilizó un escala de calificación de entre 1 y 5, donde el 1 se considera fácil de usar y 5 una dificultad alta, con los datos recolectados el 32% de los

estudiantes define en la escala el número 2, seguidamente el 30% considera fácil de utilizar el método.

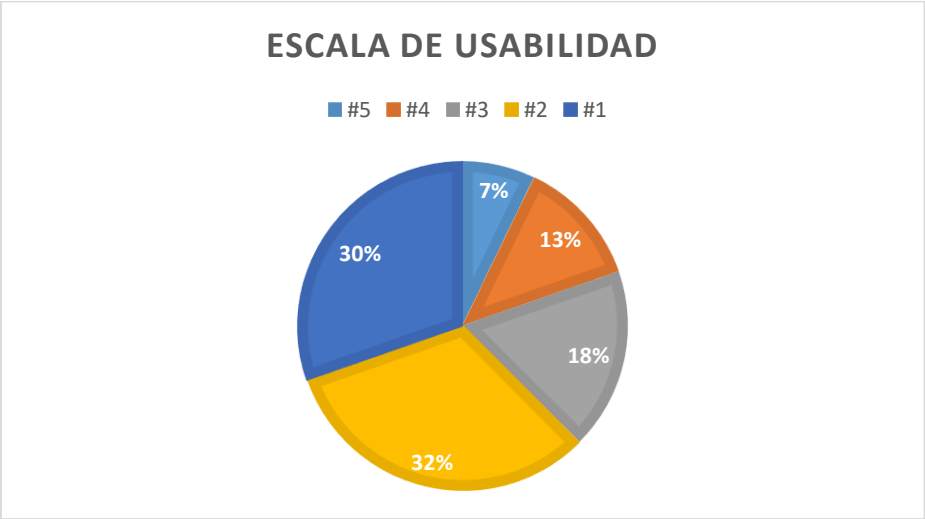

Figura 30. Escala de usabilidad del método propuesto

Para finalizar el análisis tenemos las estadísticas recolectadas en cuanto a la consideración de seguridad que implementa el método propuesto, el 55% de los estudiantes dice que la seguridad que se evidencia es alta, el 43% menciona un nivel de seguridad media seguidamente con el 2% de baja, ver Figura 31.

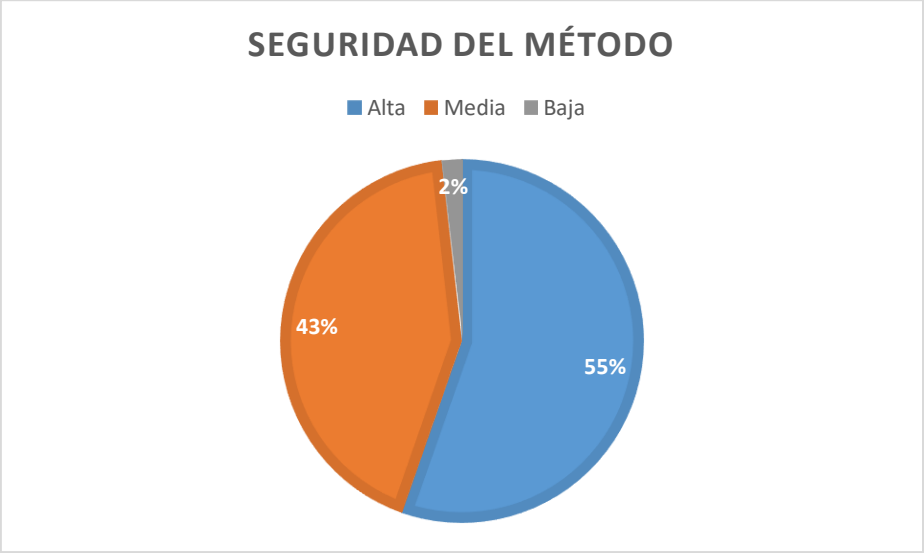

Figura 31. Nivel de seguridad del método planteado

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1 Conclusiones

El continuo y preocupante crecimiento de los ciberataques con el fin de obtener información confidencial de las personas que permita a los delincuentes informáticos acceder a sus cuentas de usuario en los distintos sistemas de información, hace imprescindible la búsqueda y utilización de métodos enfocados en salvaguardar la confidencialidad de las credenciales de acceso a los mismos, con el fin de evitar fraudes e incluso delitos de suplantación de identidad.

El presente trabajo muestra un método alternativo de ingreso de credenciales enfocado en evitar el robo de estas mediante herramientas de spyware conocidas como keylogger. Para cumplir con este propósito se diseñó un prototipo basado en una aplicación para dispositivos móviles Android y una extensión del web browser Mozilla Firefox.

El prototipo desarrollado cumple con los requerimientos funcionales establecidos en el método propuesto y fue realizado bajo la metodología de desarrollo tradicional basada en prototipos, la cual es ideal para proyectos de corto alcance que cuentan con los requerimientos totalmente definidos y permite la generación de versiones del proyecto como prototipos hasta llegar a una versión final, verificada y aceptada.

La definición y el diseño del método propuesto fue resultado de una revisión de literatura que permitió identificar y solucionar las falencias de otros métodos que comparten el mismo objetivo y han sido presentados por varios investigadores alrededor del mundo.

La implementación del prototipo en un ambiente experimental controlado y una encuesta de aceptación del método propuesto, permitieron comprobar la eficiencia del

aplicativo desarrollado y demostrar que con este se evita el robo u obtención de credenciales de acceso por herramientas o dispositivos de spyware keyloggers.

7.2 Recomendaciones

Se recomienda a los usuarios tomar conciencia de los daños que puede ocasionarles el ser víctimas del robo de sus credenciales de acceso a los distintos sistemas de información. Es responsabilidad de todos estar constantemente informados de las medidas que se deben tomar en cuenta para evitar el cometimiento de estos delitos.

Es importante continuar con la búsqueda y uso de distintos métodos de seguridad que contemplen los demás tipos de ciberataques relacionados con la obtención no autorizada de información sensible y aseguren al menos el cumplimiento de los principios básicos de la seguridad informática.

Finalmente, se recomienda la creación de herramientas de seguridad más generales, considerando las distintas plataformas de ejecución y los diferentes protocolos por los cuales se transmite la información, permitiendo así un mayor alcance en cantidad de usuarios beneficiados y protegidos por estas.

REFERENCIAS BIBLIOGRÁFICAS

Abril, A. (2013). Análisis de riesgos en seguridad de la información. *Revista Ciencia, Innovación y Tecnología (RCIYT*, 41.

Addae, J., Radenkovic, M., Sun, X., & Towey, D. (2016). An Augmented Cybersecurity Behavioural Research Model. *2016 IEEE 40th Annual Computer Software and Applications Conference* (págs. 602-603). Atlanta: IEEE.

Alsaiari, H., Papadaki, M., & Dowland, P. (2016). Graphical One-Time Password (GOTPass): A usability evaluation. *Information Security Journal: A Global Perspective*.

Arora, M., Sharma, K. K., & Chauhan, S. (2016). Cyber Crime Combating Using KeyLog Detector tool. *International Journal of Recent Research Aspects*, 1-5.

Baca, G. (2016). *Introducción a la Seguridad Informática.* Mexico: Grupo Editorial Patria.

Baskerville, R. (1999). Grounded action research: a method for understanding IT in practice. *Accouting, Management Technologies*, 1-23.

Blauw, F., & Von Solms, S. (2014). Streamlined approach to online banking authentication in South Africa and Europe. *2014 IST-Africa Conference Proceedings* (págs. 1-10). Mauritius: IEEE.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *2012 IEEE Symposium on Security and Privacy* (págs. 553-567). San Francisco: IEEE.

Booch, G. (1999). *El lenguaje unificado de modelado.* Madrid: Addison Wesley.

Chien-Wei, H., Fu-Hau, H., & Shih-Jen, C. (2013). Defend a System against Keyloggers with a Privilege-limited Account. *Applied Mechanics and Materials*.

Connell, D. (19 de Octubre de 2017). *Solve It.* Obtenido de How cybercriminals can make money from your data: http://www.solveit.ie/how-hackers-monetise-data/

Cullina, M. (9 de Septiembre de 2013). *Cyber Scout.* Obtenido de Internet users don´t understan internet risks: https://cyberscout.com/education/blog/young-internet-users-dont-understand-internet-risks

Diario el Telégrafo. (16 de Agosto de 2016). *El Telégrafo*. Obtenido de https://www.eltelegrafo.com.ec/noticias/judicial/13/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

Fojón, E., & Sanz, Á. (18 de Junio de 2010). Ciberseguridad en España: una propuesta para su gestión. *Elcano Newsletter*.

François, J. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Barcelona: Ediciones ENI.

Ganpatrao, R., & Dani, A. R. (2012). Comparative Study of Prototype Model for Software Engineering With System Development Life Cycle. *IOSR Journal of Engineering*, 21-24.

Google. (25 de 04 de 2018). *Android Studio*. Obtenido de Andorid Studio: https://developer.android.com/studio/intro/?hl=es-419

Gowraj, N., Avireddy, S., & Prabhu, S. (2013). GAS A novel grid based authentication system. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 578-590 .

Gowraj, N., Avireddy, S., Ravi, P. V., Subramanian, R. B., & Prabhu, S. (2013). SAFE Shoulder-surfing attack filibustered with ease. *International Conference on Dependable Systems and Networks.* Budapest: IEEE.

Gutiérrez, D. (Julio de 2011). *Métodos de desarrollo de software.* Obtenido de https://mimateriaenlinea.unid.edu.mx/dts_cursos_mdl/pos/TI/IS/AM/02/Metodos_de_dersarrollo.pdf

Heroku. (19 de 01 de 2018). *Heroku: Producto.* Obtenido de https://www.heroku.com/

Hung, C.-W., Hsu, F.-h., Chen, S.-J., Tso, C.-K., Hwang, Y.-L., Lin, P.-C., & Hsu, L.-P. (2012). A QTE-based Solution to Keylogger Attacks. *The Sixth International Conference on Emerging Security Information, Systems and Technologies* (págs. 62-67). Roma: IARIA XPS.

Hung, C.-W., Hsu, F.-h., Chen, S.-J., Tso, C.-K., Hwang, Y.-L., Lin, P.-C., & Hsu, L.-P. (2013). Defend a System against Keyloggers with a Privilege limited Account. *Applied Mechanics and Materials*, 3385-3389.

Information Security . (12 de Julio de 2016). *StackExchange.* Obtenido de Information Security : https://security.stackexchange.com/questions/129800/does-the-use-of-an-on-screen-keyboard-give-a-false-sense-of-security-or-protect

Iskandar, A., Fahlepi, M., Syamsu, S., Mansyur, M., Listyorini, T., Sallu, S., . . . Rahim, R. (2018). Web based testing application security system using semantic comparison method. *IOP Conference Series: Materials Science and Engineering.* Pavlov: MSE.

Jaballah, W. B., Meddeb, A., & Youssef, H. (2010). An efficient source authentication scheme in wireless sensor networks. *The 8th ACS/IEEE International Conference on Computer Systems and Applications.* Hammamet: ACS.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 973-993.

Jesudoss, A., & Subramaniam, N. (2016). EAM: Architecting Efficient Authentication Model for Internet Security using Image-Based One Time Password Technique. *Indian Journal of Science and Technology*.

Jesudoss, A., & Subramaniam, N. (2016). Securing cloud - based healthcare information systems using enhanced password-based authentication scheme. *Asian Journal of Information Technology*, 2457-2463.

Kaspersky. (08 de Agosto de 2018). *Kaspersky*. Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/definitions/keylogger

Kheder, W. (2018). Improved keylogging and shoulder-surfing resistant visual two-factor authentication protocol. *Journal of Information Security and Applications.*

Kitchenham, B., & Charters, S. (2007). Guidelines for Performing Systematic Literature. *Software Engineering Group*.

Kriz, D. (2011). Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity. *2011 Second Worldwide Cybersecurity Summit (WCS)* (págs. 1-3). London: IEEE.

Kumar, R., & Khurshid, F. (2014). Performance analysis of enhanced secure socket layer protocol. *2014 International Conference on Communication and Network Technologies* (págs. 319-323). Sivakasi: IEEE.

Kwak, D. H., McAlister, D., & Jung, E. (2011). Spyware Knowledge in Anti-Spyware Program Adoption: Effects on Risk, Trust, and Intention to Use. *2011 44th Hawaii International Conference on System Sciences* (págs. 1-10). Kauai: IEEE.

Ladakis, E., Koromilas, L., Vasiliadis, G., Polychronakis, M., & Ioannidis, S. (2013). You can type, but you can't hide: A stealthy GPU-based keylogger. *Proceedings of the 6th European Workshop on System Security (EuroSec).* Praga.

Levac, D., & Colquhoun, H. (2010). Scoping studies: advancing the methodology. *Implementation science*.

López, J. (Junio de 2015). *Universidad de Jaen*. Obtenido de Universidad de Jaen: http://tauja.ujaen.es/jspui/bitstream/10953.1/2643/1/JOS%C3%89%20L%C3%93PEZ%20EXPOSITO.pdf

López, M., Vargas, M., Reyes, B., & Vidal, O. (2011). Sistema de Información para el Control de Inventarios del Almacén del ITS. *Conciencia Tecnológica*, 41-46.

Mayhew, P., & Worsley, C. (1992). Software prototyping: the management implications. *IEE Colloquium on Software Prototyping and Evolutionary Development* (págs. 1-5). Londres: IET.

MDN Web Docs. (25 de Octubre de 2018). *Developer Mozilla*. Obtenido de WebExtension: https://developer.mozilla.org/es/docs/Mozilla/Add-ons/WebExtensions/Que_son_las_WebExtensions

Méndez, E. (2006). *Modelo de evaluación de metodologías para el desarrollo de software.* Caracas.

Mieres, J. (2009). Ataques informáticos. En J. Mieres, *Debilidades de seguridad comúnmente explotadas* (pág. 17).

Misbahuddin, M., Bindhumadhava, B. S., & Dheeptha, B. (2017). Design of a risk based authentication system using machine learning techniques. *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)* (págs. 1-6). San Francisco: IEEE.

Mollo, J. (2013). KeyLogger. *Revista de Información, Tecnología y Sociedad*, 44-45.

Monaco, J. V. (2018). SoK Keylogging Side Channels. *2018 IEEE Symposium on Security and Privacy* (págs. 211-228). San Francisco: IEEE.

Morales, A., Fierrez, J., Vera, R., & Ortega, J. (2015). Biometric Student Authentication for e-Learning Platforms. *III Congreso Internacional sobre Aprendizaje, Innovación y Competitividad (CINAIC 2015)*.

Morán, O. (2003). *Criptografia Moderna*. Obtenido de UNL: http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/1181/1/188232.pdf

Moses, S., Mercado, J., Larson, A., & Rowe, D. (2015). Touch interface and keylogging malware. *2015 11th International Conference on Innovations in Information Technology (IIT)* (págs. 86-91). Dubai: IEEE.

Mylrea, M., Gupta, S. N., & Nicholls, A. (2017). An Introduction to Buildings Cybersecurity Framework. *2017 IEEE Symposium Series on Computational Intelligence (SSCI)* (págs. 1-7). Honolulu: IEEE.

Neenu, N. (2015). On screen randomized blank keyboard. *RAECE 2015*, (págs. 80-84). Roorkee.

Node.js, F. (2018). *Node.js*. Obtenido de Node.js: https://nodejs.org/es/about/

Nyang, D., Mohaisen, A., & Kang, J. (2014). Keylogging-resistant visual authentication protocols. *IEEE TRANSACTIONS ON MOBILE COMPUTING*, 2566-2579.

Oracle. (Marzo de 2012). *Administración de Oracle Solaris: servicios de seguridad*. Obtenido de ORACLE: https://docs.oracle.com/cd/E26921_01/html/E25886/concept-28.html

Parekh, G., DeLatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., & Sherman, A. T. (2018). Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Transactions on Education*, 11-20.

Pathak, N., Pawar, A., & Patil, B. (2015). A Survey on Keylogger: A malicious Attack. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 1465-1469.

Plaza, P. (2014). *Métodos de Ataque Informáticos.* Iquitos: UNAP.

Pressman, R. (2010). *Ingeniería del software un enfoque práctico.* Mëxico: The McGraw-Hill.

Pressman, R. (2010). *Software Engineering: A Practitioner's Approach.* New York: McGraw-Hill.

Rahim, R., Nurdiyanto, H., Saleh, A., Abdullah, D., Hartama, D., & Napitupulu, D. (2018). Keylogger Application to Monitoring Users Activity. *Journal of of Physics: Conference Series*.

Ranganadham, R., & Ravi, K. (2016). A Novel Method for Authentication Protocol using Barcode Generator. *International Journal of Innovative Techonologies* .

Raúl J. Martelo, L. C. (2018). Modelo Básico de Seguridad Lógica. *Información Tecnológica*, 8.

Raza, M., Iqbal, M., Sharif, M., & Haider , W. (2012). A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. *World Applied Sciences Journal*, 439-444.

Rodriguez, H., & Ochoa, J. (2016). Protected Implementation of Pairing Based Two. *IEEE Latin America Transactions*, 2-4.

Solairaj, A. (2016). Keyloggers software detection techniques. *Intelligent Systems and Control (ISCO), 2016 10th International Conference on*, 2-3.

Stewin, P., & Bystrov, I. (2013). Understanding DMA Malware. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 21-41.

Sukhram, D. (2017). KeyStroke Logs: Are Strong Passwords Enough? . *Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017 IEEE 8th Annual*, 6.

Susman, G. (1978). An Assessment of the Scientific Merits of Action Research. *Administrative Science Quarterly*, 582.

Symantec. (22 de Enero de 2018). *Comunicados de Prensa*. Obtenido de https://www.symantec.com/about/newsroom/press-releases/2018/symantec_0122_01

Symantec. (2018). *Internet Security Threat Report.*

Tasabeeh, O., Omer, S., & Abeer, E. (2016). Random Multiple Layouts Keylogger Prevention Technique. *Conference of Basic Sciences and Engineering Studies* .

Tenstep. (23 de Marzo de 2014). *Historias de Usuario.*

Thomas, K. (2017). Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials. *CCS'17*, 7-13.

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., . . . Bursztein, E. (2017). Data Breaches, phishing, or malware understanding the risks of stolen credentials. *ACM Conference on Computer and Communications Security* (págs. 1421-1434). Dallas: ACM.

Venkatesh, G., Gopal, S. V., Meduri, M., & Sindhu, C. (2017). Application of session login and one time password in fund transfer system using RSA algorithm. *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)* (págs. 732-738). Coimbatore: IEEE.

Waheed, A., Shah, M. A., & Khan, A. (2016). Secure login protocols An analysis on modern attacks and solutions. *2016 22nd International Conference on Automation and Computing, ICAC 2016: Tackling the New Challenges in Automation and Computing* (págs. 535-541). Colchester: IEEE.

Wazid, M., Katal, A., Goudar, R. H., Singh, D., Tyagi, A., Sharma, R., & Bhakuni, P. (2013). A framework for detection and prevention of novel keylogger spyware attacks. *2013 7th International Conference on Intelligent Systems and Control (ISCO)* (págs. 433-438). Coimbatore: IEEE.

Wilcox, H., & Bhattacharya, M. (2016). A framework to mitigate social engineering through social media within the enterprise. *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)* (págs. 1039-1044). Hefei: IEEE.

Wilfred , A. A., & Skarbek, W. (2018). Image steganography for increasing security of OTP authentication. *SPIE - The International Society for Optical Engineering.* SPIE.

Wohlin, C., & Runeson, P. (2013). On the reliability of mapping studies in software engineering. *The Journal of Systems and Software*.

Wu, D.-h., Chen, S.-l., Liu, W.-y., & Liu, J.-l. (2010). Research on Mining Recycling Economy Spatial Decision Support System Based on Prototyping. *2010 Second International Workshop on Education Technology and Computer Science* (págs. 543-546). Wuhan: IEEE.

Yan, Q., Han, J., Li, Y., Zhou, J., & Deng, R. H. (2013). Designing leakage-resilient password entry on touchscreen mobile devices. *8th ACM SIGSAC Symposium on Information, Computer and Communications Security* (págs. 37-48). Hangzhou: ACM.

Zapata, L. (2012). Evaluación y mitigación de ataques reales a redes ip utilizando tecnologías de virtualización de libre distribución. *Ingenius*, 11-19.