Mecanismo de autenticación híbrido basado en contraseña gráfica y descartable.

Arcentales Venegas, Daniel Alejandro

Departamento de Ciencias de la Computación

Ingeniería de Sistemas e Informática

Trabajo de titulación, previo a la obtención del título de Ingeniero en Sistemas e Informática

PHD. Gualotuña Alvarez, Tatiana Marisol

23 de enero del 2020

URKUND

Document Information

Analyzed document	TesisArcentalesDaniel.docx (D64079918)
Submitted	2/18/2020 9:52:00 PM
Submitted by	
Submitter email	jbolanos@difusion.com.mx
Similarity	0%
Analysis address	jbolanos.GDC@analysis.urkund.com

Sources included in the report

SA	Tesis Pregrado.docx Document Tesis Pregrado.docx (D47219544)	1

Firma:

.....

PHD. Gualotuña Alvarez, Tatiana Marisol

DIRECTOR

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÒN

CARRERA DE INGENIERÌA DE SISTEMAS E INFORMÀTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Mecanismo de autenticación híbrido basado en contraseña gráfica y descartable**" fue realizado por el señor **Arcentales Venegas, Daniel Alejandro** el cual ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 23 enero del 2020

Firma:

.....

PHD. Gualotuña Alvarez, Tatiana Marisol

C. C. 1711498418

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÒN

CARRERA DE INGENIERÌA DE SISTEMAS E INFORMÀTICA

RESPONSABILIDAD DE AUTORÍA

Yo, **Arcentales Venegas, Daniel Alejandro**, con cédula de ciudadanía n°1721594446, declaro/declaramos que el contenido, ideas y criterios del trabajo de titulación: **"Mecanismo de autenticación híbrido basado en contraseña gráfica y descartable"** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 23 enero 2020.

Firma

.....

Arcentales Venegas, Daniel Alejandro

C.C.: 1721594446

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÒN

CARRERA DE INGENIERÌA DE SISTEMAS E INFORMÀTICA

AUTORIZACIÓN DE PUBLICACIÓN

Yo **Arcentales Venegas, Daniel Alejandro,** con cédula de ciudadanía n°1721594446, autorizo la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Mecanismo de autenticación híbrido basado en contraseña gráfica y descartable"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 23 enero 2020.

Firma

.....

Arcentales Venegas, Daniel Alejandro

C.C.: 1721594446

Dedicatoria

Dedico mi tesis a Dios, porque aunque he estado alejado de él, nunca me ha dado la espalda y siempre ha estado presente en mi vida, a mis amados padres, que siempre han sido mi guía y soporte, a mis hermanas que siempre me han apoyado y aconsejado, y finalmente a mi sobrina la cual se ha convertido en una hija para mí y me ha enseñado a ser padre, todos ellos son indispensables para mí y me han permitido llegar a este punto.

Daniel Arcentales

Agradecimiento

Un agradecimiento especial a mis profesores Tatiana, Diego y Rodrigo, los cuales estuvieron presentes en mi vida universitaria, donde no solo se limitaron a ser mis maestros, se convirtieron en grandes amigos, donde sus consejos me han permitido crecer de manera personal y profesional, siempre fomentándome el trabajo en equipo, investigación y valores.

Agradezco a todas las personas que estuvieron presentes en mi vida universitaria, ya que, de alguna u otra manera me enseñaron diferentes cosas que me han forjado como persona.

Daniel Arcentales

Tabla de contenidos

Índice de tablas

Índice de figuras

Resumen

La información digital en la actualidad es uno de los recursos más importantes de las personas y empresas, el cibercrimen se presenta como una problemática ya que se dedica a la sustracción de este recurso y ha ido incrementando a través de los años, por ende es primordial implementar en los sistemas informáticos estrategias que mitiguen el robo de datos, frente a esta realidad el presente estudio tiene como objetivo proponer un sistema de autenticación híbrido, agrupando las ventajas de las contraseñas gráficas y las contraseñas de un solo, planteando un mecanismo de autenticación alternativo basado en contraseñas gráficas descartables, sustentado mediante un algoritmo que genera secuencias randómicas, validado por el test de rachas que verifica la aleatoriedad de dichas secuencias y evaluado contra los ataques de robo de credenciales tales como Keylogger, ataque de fuerza bruta o de diccionario y Shoulder Surfing las cuales se presentan como técnicas sencillas de comprender y aplicar para el robo de credenciales, conjuntamente se realizó un proceso de evaluación de usabilidad donde se refleja un 92% de aceptación del mecanismo propuesto, el esquema se desarrolló tomando en cuenta las buenas prácticas y los aspectos de usabilidad que propone el NIST en su publicación SP-800-63.

Palabras clave:

- **CIBERSEGURIDAD**
- **CONTRASEÑAS GRÁFICAS**
- **CIBERSEGURIDAD**
- **AUTENTICACIÓN**

Abstract

Nowadays the digital information is one of the most important resources of people and companies, the cybercrime is presented as a problem because it is dedicated to the subtraction of this resource and has been increasing over the years, therefore is essential to implement in the computer systems strategies that mitigate data theft, in view of this reality the present study aims to propose a hybrid authentication system, to group the advantages of graphic passwords and single passwords, proposing an alternative authentication mechanism based on disposable graphic passwords, supported by an algorithm that generates randomic sequences, validated by the streak test that verifies the randomness of sequences of sequences and evaluated against theft attacks of credentials such as Keylogger, brute force or dictionary attack and shoulder Surf which are presented as simple techniques of application For the theft of credentials, you can carry out a usability evaluation process where 92% acceptance of the proposed mechanism is reflected, the scheme must take into account the good practices and usability aspects proposed by the NIST in its publication SP -800-63.

Keywords:

- **CYBER SECURITY**
- **GRAPHIC PASSWORDS**
- **CYBER SECURITY**
- **AUTHENTICATION**

Capítulo I - Introducción

Antecedentes

La fase de autenticación dentro de los sistemas de información siempre se ha presentado como un problema de alto riesgo en la seguridad de la información dentro de una organización (Ghazi Kalayeh, Nik, & Kordestani, 2013).

Bajo este contexto se ha introducido un gran número de diferentes métodos, los cuales se encuentran implementados en diferentes sistemas de información, entre estos se tiene: las contraseñas basadas en texto (Han, Cao, & Lei, 2011), los métodos biométricos (Haque, Khan, & Khatoon, 2016), contraseñas de un solo uso (Srivastava & Sivasankar, 2017), contraseñas gráficas (Herzberg & Margulies, 2012) o sistemas que implementan una combinación de las antes mencionadas (Khan, Xiang, Aalsalem, & Arshad, 2011).

La autenticación, de manera similar a la mayoría de los aspectos de seguridad de la información, debe comprometerse entre usabilidad y seguridad (Ghazi Kalayeh et al., 2013).

A pesar de que existen una gran cantidad de opciones disponibles para la autenticación, la basada en texto sigue siendo la más común, por su facilidad de uso, familiaridad con el usuario, su fácil y económica implementación (Han et al., 2011).

Para superar los problemas de seguridad de las contraseñas de texto, la idea de la contraseña gráfica fue propuesta por Greg Blonder en 1996 lo cual permitió que se propongan numerosos esquemas gráficos de contraseñas, que consisten en el uso de imágenes como contraseñas, parte de imágenes, siluetas o

bocetos. Los estudios de psicología demuestran que el cerebro humano es mejor reconociendo imágenes que recordando un texto (Saeed & Umar, 2015).

En los últimos años, los investigadores han propuesto varios métodos alternativos de autenticación que faciliten a los usuarios el proceso de autenticación, entre ellos, se destaca uno: La contraseña de un solo uso (One-Time-Password, OTP), conocida como contraseña dinámica o descartable (Srivastava & Sivasankar, 2017).

Los mecanismos de autenticación que se basan en OTP se enfocan en generar las contraseñas del lado del servidor y enviársela al usuario, de modo que el usuario utilice la contraseña recibida para completar la autenticación con éxito. Incluso si un atacante o intruso adquiere una o más de estas contraseñas es posible que no pueda predecir la próxima contraseña. Esto reduce en gran medida el riesgo que el intruso obtenga acceso a la cuenta. Una de las ventajas más relevantes de las contraseñas descartables o dinámicas frente a las contraseñas estáticas es que no son vulnerables a los ataques más conocidos para el acceso fraudulento a los sistemas (Srivastava & Sivasankar, 2017), entre ellos: la ingeniería social, ataque de fuerza bruta, ataque de diccionario, Phishing, Keylogger o el ataque de repetición.

Planteamiento del problema

El avance tecnológico actual ha permitido que cada día sean más las tareas cotidianas que se encuentran migrando a un ambiente online (Yao, 2011). Las personas pueden encontrar información, administrar cuentas de bancos, pagar facturas, comprar objetos, adquirir servicios y otra serie de actividades que

utilizan la Web como medio de comunicación y transacción. Muchas actividades en línea implican un intercambio de información personal o sensible, donde la autenticación del usuario es indispensable (Yao, 2011).

Tradicionalmente, los sistemas de autenticación basados en contraseñas alfanuméricas son los más comunes, al ser versátiles y fáciles de implementar (Umar & Rafiq, 2012).

Se requieren contraseñas alfanuméricas para satisfacer dos requisitos contradictorios. Deben ser fáciles de recordar, pero al mismo tiempo deben ser difíciles de adivinar (Umar & Rafiq, 2012). Se sabe que los usuarios eligen contraseñas de texto fáciles de adivinar y/o cortas, que son un blanco sencillo de ataques como Brute-Forced Attacks, Dictionary Attacks o ingeniería social. La implementación de una política de contraseña segura dentro de las organizaciones en la mayoría de los casos produce un efecto opuesto, porque al ser una contraseña difícil suele ser más complicado de rememorar y los usuarios pueden recurrir a escribir sus contraseñas en notas adhesivas, cuadernos u hojas sueltas, las cuales son colocadas cerca del computador donde se realiza la autenticación, exponiéndolos a una sustracción directa de sus credenciales de acceso al sistema (Umar & Rafiq, 2012).

Justificación

El uso de aplicativos Web para poder realizar transacciones cada día es más común, y esto va de la mano con el incremento de vulnerabilidades. Por ejemplo Symantec mantiene una de las bases de datos de vulnerabilidades más

amplia del mundo, actualmente compuesta por más de 95.800 vulnerabilidades (Symantec, 2018).

Puntualmente se podría hablar del Phishing, una técnica que simula el login de una empresa para que el usuario ingrese sus credenciales y así sustraerlas, Symantec menciona que en el 2017 lograron bloquear las estafas de tipo BEC (Business Email Compromise) que podrían haber afectado potencialmente a 7700 organizaciones, lo relevante aquí, es que estos ataques fueron efectuados para diferentes sectores como: Agricultura, forestal y pesca, administración pública, minería, servicios, finanzas, comercio minorista, comercio mayorista y negocios no clasificables (Symantec, 2018). Esto nos demuestra claramente en que ningún sector económico está exento de posibles ataques para robo de credenciales.

Otro ataque bastante común es el de fuerza bruta, un grupo de investigación realizó un experimento en una organización, donde aplicaron un algoritmo para búsqueda de contraseñas de los usuarios de dicha empresa. Obtuvieron un 70% de efectividad y el tiempo promedio fue de 3 segundos para encontrar cada contraseña, cabe recalcar, que esta empresa utilizan la autenticación basada en usuario y contraseña (Tabrez, 2017).

En base a esto el presente proyecto de investigación propone un método de autenticación híbrido basado en contraseñas gráficas descartables que mitigue las siguientes técnicas de sustracción de credenciales basadas en texto: Keylogger, ataque de fuerza bruta, ataque de diccionario, Phishing y Shoulder Surfing.

Objetivos

Objetivo General

Plantear un nuevo método de autenticación basado en contraseña gráfica y descartable, con el propósito de obtener una autenticación más segura que mitigue el mayor número de técnicas de robo de credenciales y se base en las directrices propuestas por el NIST en su publicación SP-800-63.

Objetivos Específicos

Aplicar una revisión básica de literatura que permita identificar y analizar los esquemas existentes de autenticación basados en contraseñas gráficas y descartables mediante una búsqueda en las bases digitales.

Diseñar e implementar un esquema híbrido basado en Drag & Drop como contraseña gráfica y un algoritmo generador de secuencias randómicas como OTP para generar un esquema robusto que resista diferentes técnicas de vulneración basándose en las buenas practicas que propone el NIST en su publicación SP-800-63.

Definir los parámetros de usabilidad y seguridad basándose en lo que propone el NIST en su publicación SP-800-63 y otras investigaciones para evaluar el esquema propuesto.

Alcance

La investigación se enfocará en desarrollar un método de autenticación híbrido basado en contraseña gráfica, usando Drag & Drop, y un algoritmo generador de contraseñas dinámicas.

Para comprender de mejor manera el alcance de la investigación se propone las siguientes preguntas de investigación, las cuales se encuentran asociadas con los objetivos específicos.

RQ1 ¿Qué métodos de autenticación basada en contraseñas gráficas han sido propuestos?

RQ2 ¿Qué métodos de autenticación basada en contraseñas dinámicas han sido propuestos?

RQ3 ¿Qué métodos de autenticación basada en contraseñas gráficas dinámicas han sido propuestos?

RQ4 ¿En qué cosiste el desarrollo de un esquema basado en autenticación gráfica?

RQ5 ¿En qué cosiste el desarrollo de un esquema basado en contraseñas dinámicas o de un solo uso?

RQ6 ¿Qué estipula el NIST para el desarrollo de un esquema basado en contraseñas dinámicas o de un solo uso?

RQ7 ¿Qué parámetros de usabilidad son indispensables considerar para evaluar un esquema de autenticación basado en contraseñas gráficas?

RQ8 ¿Qué parámetros de usabilidad son indispensables considerar para evaluar un esquema de autenticación basado en contraseñas dinámicas?

RQ9 ¿En base a qué directrices de seguridad se evalúa un esquema de autenticación basado en contraseñas gráficas?

RQ10 ¿En base qué directrices de seguridad se evalúa un esquema de autenticación basado en contraseñas dinámicas?

RQ11 ¿Qué parámetros propone el NIST para evaluar un esquema de autenticación?

Hipótesis

La implementación de un método de autenticación híbrida basada en contraseña gráfica y descartable evitará la sustracción de credenciales ocasionada por diferentes técnicas de vulneración tales como Keylogger, ataque de fuerza bruta, ataque de diccionario y Shoulder Surfing

En base a esta hipótesis se identificó las siguientes variables:

Variable independiente: Contraseña gráfica descartable.

Variable dependiente: Sustracción de credenciales.

Capítulo II - Marco metodológico

Estado Del Arte.

Con el objetivo de identificar y analizar los métodos existentes para autenticación, se procedió a realizar una revisión de literatura preliminar.

El proceso tendrá las siguientes fases: (1) planteamiento del proceso, (2) selección de artículos para el grupo de control y extracción de palabras claves, (3) creación y pilotaje de la cadena de búsqueda, (4) selección de artículos primarios y ,(5) elaboración del estado del arte.

Planteamiento del Proceso

Como primer paso se definió un grupo de control que permitió extraer las palabras claves necesarias para obtener una cadena de control lo más exacta posible, que permitió encontrar los artículos primarios.

Selección de Artículos y Extracción de Palabras Claves

En esta fase se procedió a identificar los estudios relevantes para poder extraer los términos necesarios con el objetivo de poder armar una cadena de búsqueda óptima. Estos artículos se obtuvieron de diferentes fuentes de información, especialmente de las librerías digitales.

Tras una lectura completa de los diferentes artículos encontrados en las diferentes bases digitales se seleccionó 4 artículos científicos que se consideraron los más relevantes y van aportar lo necesario para dirigir correctamente la investigación.

Los artículos seleccionados para formar el grupo de control y palabras claves obtenidas de cada estudio se detallan en la siguiente tabla:

Tabla 1 *Artículos Primarios y Palabras Claves*

ID	Título	Cita	Palabras clave
EC1	Analysis of knowledge base graphical password authentication	(Agarwal, Singh, & Indian, 2011)	“graphical password”, “authentication”, “security”, “systems”
EC2	A Hybrid Graphical User Authentication Scheme	(Saeed & Umar, 2015)	“graphical password”, “dynamic”, “authentication”, “systems”
EC3	Design of Two-Way One-Time-Password Authentication Scheme Based On True Random Numbers	(Fan & Su, 2009)	“OTP”, “One-Time-Password”, “dynamic”, “ authentication”, “security”, , “systems”
EC4	ImagePass - Designing Graphical Authentication for Security	(Mihajlov, 2011)	“graphical authentication”, “graphical password”, “security”, “system”

Creación y Pilotaje de la Cadena de Búsqueda

En base a las palabras claves obtenidas en el grupo de control, es necesario armar y pilotar las cadenas de búsqueda, en esta investigación la cadena se formó en la base digital de la IEEE.

Cadena Versión 1. Esta cadena se la configuró para que se busque en todo modo de todo el texto: (('graphical password' OR "dynamic password" OR "OTP") AND ('authentication') AND ("security"))

Esta cadena reflejo 5118 artículos, es decir, que la cadena no es la indicada, por el número excedido de artículos obtenidos.

Cadena Versión 2. La cadena versión 2 se la configuró para que se busque solo en los metadatos: (('graphical password' OR "dynamic password" OR "OTP") AND ('authentication') AND ("security"))

Esta cadena reflejo 370 artículos, esta cadena ofrece un número manejable de artículos pero puede ser mejorada.

Cadena Versión 3. Para esta versión de la cadena de búsqueda se agregó los siguientes términos “system” y “systems”: (('graphical password' OR "dynamic password" OR "OTP") AND ('authentication') AND ("security") AND (“system” OR “systems”)

Esta cadena reflejo 272 artículos, esta cadena ofrece un número manejable de artículos

Cadena Versión 4. A la cadena versión cuadro se le añadió un nuevo filtro, el de años de publicación, es necesario encontrar artículos que sean de los últimos 10 años, para poder encontrar información nueva y acorde a la tecnología

actual. (('graphical password' OR "dynamic password" OR "OTP") AND ('authentication') AND ("security") AND (“system” OR “systems”)

Esta cadena reflejo 250 artículos, donde se encontró un número manejable de artículos y se también están presentes los artículos del grupo de control

Todas las cadenas se las realizo con el uso de la herramienta “Advance Search” que ofrece la interfaz Web de la IEEE

Selección de Artículos Primarios

De los 250 artículos obtenidos, se realizó la lectura a nivel de Titulo y Abstract con el objetivo de escoger los artículos primarios para la investigación.

Los artículos primarios que se seleccionaron se muestran en la siguiente tabla:

Tabla 2 *Artículos Primarios*

Código	**Título**	**Cita**
EP1	DPASS – Dynamic Password Authentication and Security System using Grid Analysis	(Balaji & Roopak, 2011)
EP2	Enhancement of Password Authentication System Using Graphical Images	(Bhand & Shirke, 2015)
EP3	A Novel Shoulder-Surfing Resistant Graphical Authentication Scheme.	(Siddiqui & Umar, 2018)
EP4	Pass-Matrix authentication	(Tabrez, 2017)

Código	Título	Cita
EP5	Adding Persuasive features in Graphical Password to increase the capacity of KBAM	(Yadav, 2013)
EP6	Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique	(Hafiz, Abdullah, Ithnin, & Mammi, 2008)

Elaboración del Estado del Arte

EP1 DPASS – Dynamic Password Authentication and Security System using Grid Analysis (Balaji & Roopak, 2011). El artículo "DPASS – Dynamic Password Authentication and Security System using Grid Analysis" propone una solución nueva, factible y eficiente para combinar el uso de un sistema de contraseñas dinámicas y manejo de contraseña gráfica, en este caso, el uso de una matriz. El esquema propuesto en este artículo busca resistir los diferentes ataques existentes para la sustracción de credenciales de sistemas de autenticación basados en texto y/o contraseñas estáticas. Hace un análisis del esquema propuesto donde lo evalúa frente a varios parámetros para justificar que el esquema es robusto.

EP2 Enhancement of Password Authentication System Using Graphical Images (Bhand & Shirke, 2015). En este estudio se hace un análisis comparativo entre como el cerebro humano puede recordar contraseñas gráficas y

recordar contraseñas basadas en texto. Presenta las diferencias y ventajas las contraseñas gráficas de tipo Cued Click Point (CCP). Y propone un modelo de autenticación que se basa en CCP pero con el uso de 5 imágenes diferentes, que se van mostrando en el transcurso de autenticación, en base a esto, se justifica que este modelo es bastante seguro y flexible de usar. Presenta una GUI muy atractiva para el usuario, donde hace que el proceso de autenticación sea más "entretenido", estos tipos de autenticación son más económicos que los basados en factores biométricos.

EP3 A Novel Shoulder-Surfing Resistant Graphical Authentication Scheme (Siddiqui & Umar, 2018): Este artículo explica la clasificación de las técnicas de contraseñas gráficas, con ejemplos de los diferentes esquemas existentes. Propone una nueva técnica de contraseña gráfica, que consiste en generar una matriz de imágenes 6*6, en donde el usuario debe autenticarse, deletreando su contraseña mientras va seleccionado las imágenes de la matriz, finalmente justifica que esta propuesta contrarresta al Shoulder Surfing. Esta solución sigue se presenta como una contraseña estática.

EP4 Pass-Matrix authentication (Tabrez, 2017). En este artículo propone un método de autenticación alternativo basado en texto donde enfoca en contrarrestar el Shoulder Surfing. El esquema consiste en generar contraseñas de un solo uso, donde muestra tres imágenes, las cuales están cortadas por líneas horizontales y verticales para formar una matriz, el usuario recibe a su correo las coordenadas que debe seleccionar en cada imagen para poder autenticarse. El estudio muestra que se realizó análisis con herramientas de grabación para poder

sustraer la contraseña y esto demostró que este esquema no es vulnerable al Shoulder Surfing. Justifican que es un sistema fácil de usar y novedoso que puede remplazar a las contraseñas estáticas y/o basadas en texto.

EP5 Adding Persuasive features in Graphical Password to increase the capacity of KBAM (Yadav, 2013). Este estudio propone un esquema de autenticación gráfica basada en hacer clic en diferentes posiciones dentro de una imagen, encripta esta información usando SHA-1 y almacena la contraseña en una base de datos, posteriormente lo evalúa frente a las siguientes técnicas de vulneración: ataque de diccionario, ataque de fuerza bruta, shoulder surfing, spyware e ingeniería social.

EP6 Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique (Hafiz, Abdullah, Ithnin, & Mammi, 2008). Este estudio propone una serie de parámetros para evaluar los diferentes esquemas propuestos para la autenticación gráfica y especifica dos análisis: el de usabilidad donde propone parámetros como: eficiencia del aplicativo, sencillo de entender y divertido de usar. Y el de seguridad, que se enfoca en contraponer los esquemas basados en contraseñas gráficas frente a posibles ataques para sustracción de credenciales.

Características del Estado del Arte

Existen varios artículos que proponen esquemas basados en contraseñas gráficas, donde buscan que exista usabilidad y seguridad, estas contraseñas gráficas se enfocan en que el usuario omita el uso de teclado y la autenticación se

limite al uso del ratón, donde es necesario recordar imágenes o recordar en lugares se realizó un clic al momento de registrarse al sistema.

En base a las contraseñas dinámicas o descartables, es decir, las contraseñas de un solo uso, los investigadores se enfocan en generar algoritmos robustos que permiten que no se generen contraseñas en base a un patrón o repetición, con el objetivo de que sean difíciles de replicar o predecir, permitiendo que la autenticación sea segura.

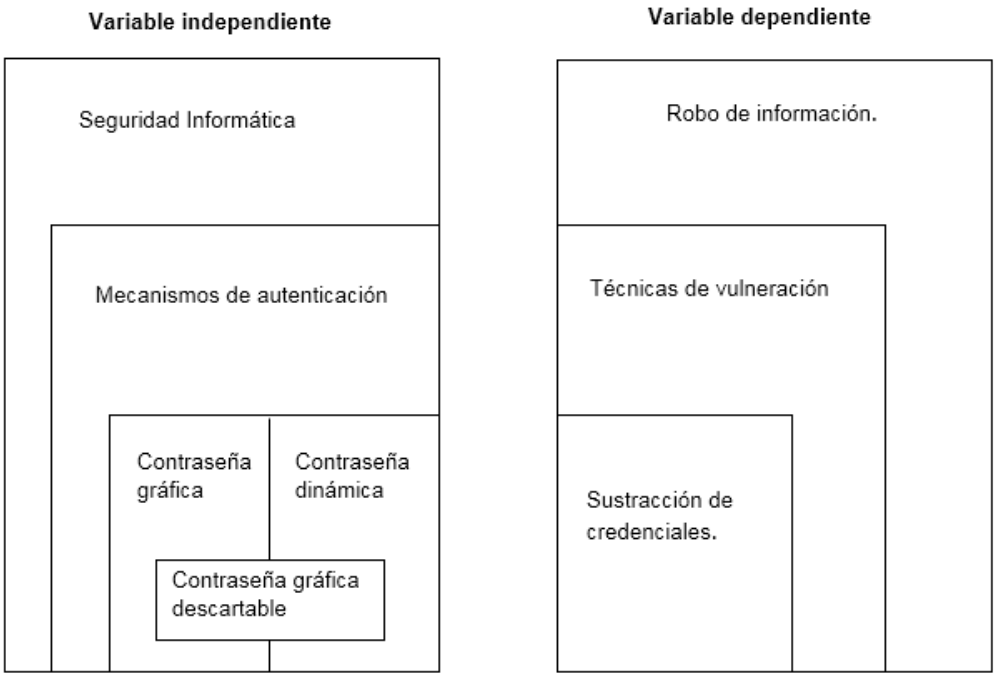
Entre todos los artículos encontrados tan solo uno abarca una contraseña gráfica descartable, donde demuestra que las contraseñas de este tipo son bastante seguras y fáciles de usar.

Marco Teórico

Con el objetivo de comprender el ámbito de estudio de la presente investigación, es necesario estructurar una red de categorías que permiten la explicación y compresión científica del estudio:

Figura 1

Red de Categorías de las Variables de Investigación



Fundamentación Científica de la Variable Independiente.

Seguridad Informática. En la actualidad la mayoría de sectores económicos, y por no decir todos, tienen o están migrando sus sistemas a un ambiente online, por ejemplo comercialización de artículos, servicios de aprendizaje continuo, transacciones bancarias o reserva de libros (Gupta, Vashisht, & Singh, 2016).

Bajo esta realidad se presenta un nuevo escenario para la humanidad, donde el Internet se encuentra en la vida diaria de las personas las cuales por “a” o “b” razón comparten su información pública y privada como: nombre, direcciones, número de celular, cuentas bancarias, etc. En base a este contexto

cada organización debe hacer lo necesario para salvaguardar la información de sus usuarios frente a diferentes ataques cibernéticos (Gupta et al., 2016).

La seguridad de la información en la actualidad es un requisito fundamental de las organizaciones, donde los datos que protegen se han convertido el activo digital más importante (Mir, Wani, & Ibrahim, 2013).

Este aspecto se relaciona directamente con la privacidad de las personas, donde las organizaciones y sus usuarios deben estar totalmente consiente que es su responsabilidad tomar en cuenta las directrices para evitar el robo de la información, de parte de las empresas proponer políticas de seguridad en la creación de contraseñas hasta la correcta protección de los aspectos de seguridad de los servidores y de parte de los usuarios que implica una correcta gestión sus credenciales, las organizaciones y sus usuarios deben trabajar de manera conjunta para poder tener una seguridad informática robusta.

Mecanismos de Autenticación. La autenticación nace como un proceso primordial para verificar que la persona que intenta acceder a un sistema posee el permiso respectivo, donde el sistema mediante reglas valida que la persona es la que dice ser, este procesos busca cumplir dos de los objetivos de seguridad, que es mantener la confidencialidad e integridad de la información del usuario del sistema, la autenticación es el componente central de la seguridad informática (Almuairfi, Veeraraghavan, & Chilamkurti, 2011).

Al pasar de los años se han propuesto un número significativo de mecanismos de autenticación, los cuales se clasifican en tres categorías que responden a tres preguntas ¿Algo que yo sé? ¿Algo que yo poseo? Y ¿Algo que

yo soy? (Lin, Weng, & Huang, 2008) (Almuairfi et al., 2011) (Gao, Liu, Li, & Qiu, 2014):

Autenticación basada en conocimiento. En esta clasificación se encuentran las contraseñas que responden a la pregunta "¿Algo que yo sé?", es decir, que tengo el conocimiento necesario para poder acceder a un sistema, las contraseñas basadas en texto y las contraseñas gráficas se encuentran en esta clasificación (Gao et al., 2014).

Autenticación basada en token. En esta clasificación se encuentran las contraseñas que responden a la pregunta "¿Algo que yo poseo?", es decir, en donde el usuario del sistema tiene un objeto o "token", el cual le va a permitir autenticarse en el sistema, como puede ser una tarjeta inteligente, un tag de proximidad, una tarjeta bancaria, etc (Rajarajan, Prabhu, Palanivel, & Karthikeyan, 2014) (Lin et al., 2008).

Autenticación basada en factores biométricos. En esta clasificación se encuentran las contraseñas que responden a la pregunta "¿Algo que yo soy?", las características biométricas se pueden dividir en dos tipos, los mecanismos de autenticación que se centran en los aspectos físicos, como las huellas digitales, el iris o la retina (Haque et al., 2016). Y los mecanismos de autenticación que se enfocan en los aspectos conductuales, como la forma de firmar, caminar o de escribir en el teclado (Rajarajan et al., 2014).

Contraseñas gráficas. Las contraseñas basadas en texto siempre se han presentado como la manera más sencilla de autenticación, por su fácil y económica implementación, solo es necesario que en el proceso de registro se

escoja un usuario y una contraseña alfanumérica para crear una cuenta en el sistema (Sruthi, 2015).

Con el constante crecimiento de sistemas migrando al Internet, cada persona posee un gran número cuentas para acceder en diferentes sistemas, donde se presenta un problema, los usuarios tienden a escoger contraseñas cortas y simples, las cuales están propensas a ser robadas fácilmente, y por el otro lado, escogen contraseñas seguras, pero también se presentan como un problema ya que son difíciles recordar (Gao et al., 2014).

Bajo este contexto, nacen las contraseñas gráficas, como un método alternativo de autenticación, la principal característica que presenta es que es más fácil para las personas recordar imágenes que texto (Rajarajan et al., 2014) (Zhao & Li, 2007).

Este tipo de contraseñas presentan características que les diferencia de las contraseñas basadas en texto (Herzberg & Margulies, 2012) (Rajarajan et al., 2014):

Son más fáciles de utilizar en dispositivos electrónicos que no posean un teclado, o su teclado virtual sea difícil de manipular, por ejemplo los celulares.

Se presentan como una autenticación más atractiva hacia el usuario, lo que hace que la que esta fase sea más llamativa.

Es más difícil que se las mencione a alguien por error.

Generalmente los mecanismos basados en autenticación gráfica utilizan el mouse o touch para la selección de la contraseña, es decir, que no existe una

necesidad de usar el teclado, lo que les hace completamente resistentes a los Keyloggers.

Contraseñas dinámicas. Las contraseñas basadas en texto y las contraseñas gráficas presentan un problema en común, generalmente son estáticas, lo que ocasiona que si el atacante consigue la contraseña puede acceder al sistema cuando lo desee (Srivastava & Sivasankar, 2017).

Por el constante crecimiento del Internet, se está prestando más atención a la seguridad de la información, donde se proponen diferentes métodos de autenticación, pero no todas las empresas y clientes pueden acceder a los métodos más seguros que son los biométricos y basados en token, ya sea por accesibilidad o por recursos económicos (Liu & Zhang, 2013) .

Las contraseñas dinámicas, de un solo uso o descartables, nacen en 1980 como una forma de autenticación de bajo costo, el principal objetivo de este tipo de autenticación es generar, mediante algoritmos matemáticos o números randómicos, contraseñas que solo sirven para una única sesión, el usuario no necesita saber la contraseña, el sistema es el encargado, mediante el uso de un medio personal, ya sea, correo electrónico o mensaje de texto, de enviarle la contraseña válida para dicha sesión (Liu & Zhang, 2013).

Este tipo de contraseñas se caracteriza principalmente en que si el atacante obtiene una de las contraseñas, va ser difícil que pueda predecir la siguiente contraseña, lo que le hace invulnerable a los ataques de repetición (Srivastava & Sivasankar, 2017).

Fundamentación científica de la variable dependiente.

Robo información. En la actualidad la información se ha convertido en unos de los recursos más importantes de las empresas y manejar esta información de una forma correcta y segura, implica uno de los principales retos de las organizaciones (Mir et al., 2013).

Todos los usuarios están expuestos a la serie de problemas que ocasiona el robo de información, como: suplantación de identidad, transacciones ilegales bajo el nombre de la víctima, fraudes electrónicos, etc. Uno de los ejemplos más claros fue el robo de cuentas de Facebook en el 2018, en donde los criminales obtuvieron información de 50 millones de cuentas (Watchguard, 2018).

La sustracción de credenciales no es el único factor que implica el robo de información, existen más problemas que se identificaron en el 2018 (Watchguard, 2018): El 6.8% del top de los sitios web no tiene los protocolos de seguridad correspondientes, el 20.9% del top de los sitios web no utilizan encriptación, lo que les hace vulnerables a los ataques de intercepción y sitios web presentan scripts de JavasScript que roban datos.

Técnicas para sustracción de credenciales. Si tenemos que poner un punto de partida, referente a la sustracción de credenciales, podríamos empezar mencionando al mejor hacker del mundo Kevin Mitnick, el cual, implemento la primera y más antigua de las técnicas, la ingeniería social, con la que logro engañar a diferentes usuarios autorizados para poder obtener información sensible que le permitiría encontrar huecos de seguridad en un sistema (López Grande & Edgardo, 2015).

En la actualidad existen un número alto de técnicas de sustracción de credenciales, cada una presenta características diferentes, entre estas técnicas tenemos:

Ingeniería social. El atacante interactúa con la víctima, la cual es un usuario autorizado del sistema, en la búsqueda de ganar su confianza, persuadirlo o engañarlo para obtener la información necesaria para adivinar las credenciales de acceso al sistema o encontrar una brecha de seguridad que le permita acceder de manera fraudulenta (Lashkari, Manaf, & Masrom, 2011).

Baiting. Consiste en que el atacante deja una memoria externa, la cual contiene algún tipo de virus, cerca del computador de la víctima, para que cuando la víctima lo encuentre, lo conecte en su computador y automáticamente el virus se inyecte en el sistema y le de algún tipo de control al atacante (López Grande & Edgardo, 2015).

Phising. Conocido como suplantación de identidad, ya que, el atacante mediante un medio de comunicación, como correo electrónico o llamada telefónica, se hace pasar por una empresa legitima, como un banco o entidad del gobierno, y engaña a la víctima, para que le proporcione las credenciales o la información para acceder al sistema, generalmente suelen usar sitios fraudulentos que tienen un parecido bastante alto al original (Gao et al., 2014).

Shoulder-surfing. El atacante se ubica en una posición que le permita tener una visión directa del computador de la víctima, puede también poseer un dispositivo de grabación o visión lejana, con el objetivo de que cuando el usuario

vaya autenticarse en un sistema, el atacante pueda ver sus credenciales de acceso y de esa manera obtenerlas (Goutham, Kim, & Yoo, 2014).

Keylogger. Es un tipo de malware que se enfoca en capturar todas las pulsaciones de teclado, mediante el uso de un tipo de software o hardware (Kolekar & Vaidya, 2016).

Brute Foce Attack – Dictionary Attack. Son ataques de de búsqueda exhaustiva, consiste en que prueban diferentes contraseñas o palabras de una base de datos, de manera sistemática, hasta encontrar la que les permita acceder al sistema (Rajarajan et al., 2014).

Spyware Attack. El ataque consiste en instalar un aplicación en la computadora de la víctima con el objetivo de grabar todo lo que está haciendo como el movimiento del ratón o las pulsaciones de las teclas, esta aplicación tiene la capacidad de almacenar esa información y enviarla al atacante (Lashkari et al., 2011).

Man-in-middle attack. El atacante intercepta la sesión o el canal de comunicación entre el usuario y el servidor, para poder extraer la información necesaria que le permita acceder de manera no autorizada a un sistema (Almuairfi et al., 2011).

Replay Attack. El atacante graba la secuencia de mensajes entre el usuario y el servidor, para posteriormente reproducirlas en el servidor para obtener acceso al sistema (Goutham et al., 2014).

Sustracción de credenciales. Las credenciales, se presentan como el filtro principal para evitar el acceso no autorizado a los sistemas.

En los últimos años la sustracción de credenciales se ha convertido un problema social, donde cualquier sector económico esta propenso a ser vulnerado (Symantec, 2018).

En el 2017 la empresa Watchguard obtuvo las siguientes estadísticas en el ámbito de robo de credenciales (Watchguard, 2017):

200 millones de Yahoo, 159 millones de Hotmail y 90 millones de Gmail.

Se filtraron 375 mil direcciones y contraseñas gubernamentales y más de medio millón de militares.

Su firewall bloqueo 30.3224.010 diferentes variantes de malware y 6.907.718 ataques a la red.

Por otro lado Symantec también nos ofrece estadísticas del 2017 en este ámbito (Symantec, 2018):

Bloquearon un total de 223.066.372 ataques a sitios web, donde en promedio se obtiene que fueron 611.141 ataques diarios

Dedujeron que 7.710 organizaciones son afectadas por estafas para comprometer a la empresa.

Incremento el ataque de Phishing comparado al 2016, en donde 1 de cada 53 usuarios recibió un ataque de este tipo.

Este año se publicó un informe, donde se expone que existió un robo masivo de credenciales, donde se encuentra un total de 2.692.818.23 correos y contraseñas (Hunt, 2019).

Como podemos observar, esto se ha convertido en una constante lucha, donde nadie está a salvo de perder su información o que su información sea

utilizada de manera fraudulenta, mientras incrementan los mecanismos de autenticación crecen de manera paralela las técnicas de vulneración.

Es necesario que las organizaciones y usuarios pongan énfasis en este aspecto, ya que, es necesario que exista una cultura de protección de la información, algo que en la actualidad es un elemento importante.

Metodología de la investigación.

Al ser una investigación orientada a generar un prototipo se seleccionó la metodología de investigación basado en “Acción”, la cual consta de 5 etapas: Diagnosticar, planificar, actuar, observar y reflexionar. Estas etapas se las realiza por iteraciones, de tal manera, que cada iteración se vaya mejorando la investigación, que iría de la mano con el prototipo, hasta llegar a la solución más satisfactoria.

Lo que se destaca de este tipo de investigación es que es recursiva, participativa, cualitativa, reflexiva y transforma teoría y práctica (Rodríguez, Jordi, & Roquet, n.d.).

En base a esto se definición lo siguiente para cada fase:

Diagnosticar: Analizar los métodos existentes basados en contraseñas gráficas o/y contraseñas de un solo uso mediante una revisión preliminar de literatura.

Planificar. Definir los requerimientos y necesidades del usuario para plantear un esquema híbrido basado en contraseñas gráficas descartables, mediante los resultados del estado del arte.

Actuar. Desarrollar el esquema.

Observar. Evaluar el esquema y calificarlo, mediante una definición de parámetros de usabilidad y seguridad.

Reflexionar: Proponer estrategias para que el mecanismo tenga un ambiente óptimo de funcionamiento y establecer directrices para su correcto mantenimiento y actualización.

Capítulo III - Diagnosticar, Planificar y Actuar

En este capítulo se desarrollan las fases de diagnosticar, planificar y actuar en base la metodología seleccionada, con el objetivo de plantear un sistema generador de contraseñas gráficas descartables, el diagnóstico fue realizado en el capítulo 1 y capitulo 2, planificar refleja lo que cumple el mecanismo de autenticación híbrido basado en contraseñas gráficas descartables y el actuar presenta el desarrollo completo del mecanismo, donde encontramos el algoritmo generador de secuencias que es el Core de la presente investigación.

Diagnosticar

En base al estado del arte y el marco teórico presentado en los capítulos anteriores se plantearon requisitos funcionales y no funcionales a nivel de historias de usuarios, los casos de uso y una explicación detalla del algoritmo base.

Planificar

Requisitos identificados.

Con el objetivo de tener una perspectiva más precisa y completa, que permita plantear un sistema robusto que posea un algoritmo generador de contraseña gráficas descartables, se identificó las siguientes historias de usuarios.

Tabla 3

Historia de usuarios

Id	Nombre	Descripción
MAH-HU-01	Mantener autenticación tradicional	Como usuario quiero que el sistema permita como primera fase tener una autenticación basada en usuario y contraseña
MAH-HU-02	Matriz gráfica randómica para autenticación	Como usuario quiero que cada vez que necesite autenticarme se presente una matriz gráfica diferente para una segunda fase de autenticación.
MAH-HU-03	Secuencia gráfica randómica para autenticación.	Como usuario quiero que cada vez que necesite autenticarme se me entregue una secuencia única para poder autenticarme.
MAH-HU-04	Recibir secuencia randómica al correo	Como usuario quiero que la secuencia randómica que me genere el sistema sea enviada a mi correo personal
MAH-HU-04	Recibir secuencia randómica al correo	Como usuario quiero que la secuencia randómica que me genere el sistema sea enviada a mi correo personal

Las historias de usuario permitieron definir que el sistema debe poseer dos fases de autenticación, donde se mantenga la autenticación tradicional pero se la complemente con una contraseña gráfica de un solo uso.

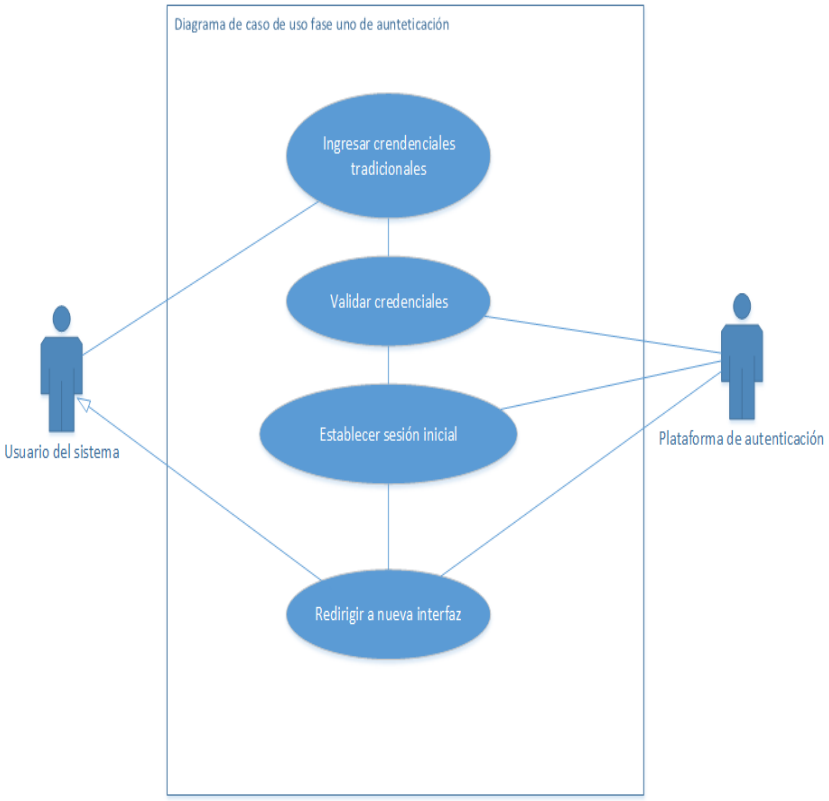
Diagramas de casos de uso

Los diagramas de casos de usos permitirá entender como el usuario interactuará con la plataforma de autenticación generadora de secuencias randómicas, en este caso, al ser un servidor de autenticación, el usuario será presentado como el actor principal y la plataforma de autenticación como actor secundario.

Se consideró dos casos de usos de nivel 0 para cada fase de autenticación:

Figura 2

Diagrama de Caso de Uso de Fase Uno de Autenticación



En las siguientes tablas se detallan los casos de uso de nivel 1

Tabla 4

Casos de Uso MAH-CU-01

Propiedad	Valor
Código	MAH-CU-01
Caso de uso	Ingresar credenciales tradicionales
Actores:	Usuario del sistema
Resumen:	El usuario del sistema debe ingresar sus credenciales de acceso del método tradicional (Nombre de usuario y contraseña)
Precondición	Acceder a la interfaz publicada de la plataforma
Descripción	El sistema presenta una interfaz para el login de la fase 1. En la interfaz se despliegan dos cuadros de ingreso y un botón, un cuadro para el nombre de usuario y otro para la contraseña. El usuario del sistema ingresa la información respectivamente. El usuario da clic en el botón de login.
Pos condición	Validar el ingreso.
Excepciones	Si el usuario presiona el botón de login, sin ingresar las credenciales, se despliega un mensaje de campos requeridos, “Campo obligatorio”.

Tabla 5

Caso de uso MAH-CU-02

Propiedad	Valor
Código	MAH-CU-02
Caso de uso	Validar credenciales
Actores:	Plataforma de autenticación.
Resumen:	La plataforma, mediante los recursos de la base de datos, verifica que las credenciales ingresadas por el usuario sean las correctas.
Precondición	Ingreso de credenciales de acceso tradicional.
Descripción	La plataforma recoge las credenciales ingresadas por el usuario. Las credenciales se verifican con la base de datos. La plataforma autentica al usuario
Pos condición	Establecimiento de la sesión.
Excepciones	Si las credenciales ingresadas por el usuario son incorrectas, se despliega un mensaje de error general “Credenciales no aceptadas”.

Tabla 6

Caso de Uso MAH-CU-03

Propiedad	**Valor**
Código	MAH-CU-03
Caso de uso	Establecer sesión inicial
Actores:	Plataforma de autenticación.
Resumen:	La plataforma establece la sesión inicial de la primera fase de autenticación.
Precondición	Validar las credenciales ingresadas por el usuario.
Descripción	La plataforma de autenticación establece la sesión principal en el servidor.
Pos condición	Validar el ingreso y credenciales.
Excepciones	La sesión solo dura 2 minutos, al acabar este tiempo, se regresa a la interfaz inicial.

Tabla 7

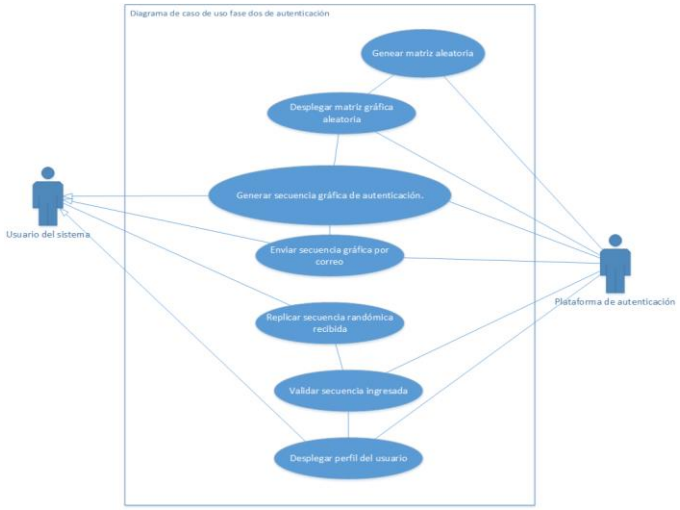
Caso de Uso MAH-CU-04

Propiedad	**Valor**
Código	MAH-CU-04
Caso de uso	Redirigir a nueva interfaz.
Actores:	Usuario del sistema, Plataforma de autenticación.

Propiedad	Valor
Resumen:	La plataforma de autenticación mediante los recursos del servidor genera una nueva interfaz para el usuario del sistema.
Precondición	Sesión inicial establecida
Descripción	La plataforma de autenticación solicita los recursos al servidor. Se redirecciona al usuario a la segunda fase de autenticación.
Pos condición	No aplica
Excepciones	Si lo recursos no están disponibles, la interfaz no se despliega y se notifica al usuario.

Figura 3

Diagrama de caso de uso de fase dos de autenticación



En las siguientes tablas se detallan los casos de uso de nivel 2:

Tabla 8

Caso de Uso MAH-CU-05

Propiedad	**Valor**
Código	MAH-CU-05
Caso de uso	Generar matriz aleatoria.
Actores:	Plataforma de autenticación.
Resumen:	La plataforma de autenticación genera una matriz gráfica aleatoria para que el usuario ingrese la secuencia necesaria para validar su ingreso.
Precondición	Sesión inicial establecida
Descripción	La plataforma de autenticación mediante un algoritmo genera una secuencia de números. Se valida la matriz obtenida, es decir, que no posea repetidos ni un orden especifico. Se envía la matriz final para ser traducida.
Pos condición	Desplegar matriz gráfica aleatoria
Excepciones	No existen excepciones en este caso.

Tabla 9

Caso de Uso MAH-CU-06

Propiedad	**Valor**
Código	MAH-CU-06
Caso de uso	Desplegar matriz gráfica aleatoria

Propiedad	Valor
Actores:	Plataforma de autenticación.
Resumen:	La plataforma obtiene la matriz generada y despliega una interfaz, traduciendo la matriz numérica a imágenes equivalentes.
Precondición	Matriz aleatoria generada.
Descripción	La plataforma obtiene la matriz numérica aleatoria generada. Se traduce los números generados a imágenes. Se despliega una interfaz gráfica con las imágenes obtenidas.
Pos condición	
Excepciones	Al no existir una equivalencia número – gráfico, por un recurso mal cargado o no encontrado, se direccionará a la interfaz inicial y se desplegará el mensaje “Recurso no encontrado comuníquese con el administrador.”

Tabla 10

Caso de Uso MAH-CU-07

Propiedad	Valor
Código	MAH-CU-07
Caso de uso	Generar secuencia de autenticación.
Actores:	Plataforma de autenticación.

Propiedad	Valor
Resumen:	La plataforma genera una secuencia randómica de un solo uso para que el usuario pueda autenticarse en el sistema.
Precondición	Sesión inicial establecida
Descripción	La plataforma de autenticación mediante un algoritmo genera una secuencia de números.
Pos condición	No aplica
Excepciones	No existen excepciones en este caso.

Tabla 11

Caso de Uso MAH-CU-08

Propiedad	Valor
Código	MAH-CU-08
Caso de uso	Enviar secuencia gráfica por correo.
Actores:	Plataforma de autenticación - Usuario del sistema.
Resumen:	La plataforma mediante un servicio de correo envía un mail con la secuencia generada para que el usuario final la reciba.
Precondición	Generar secuencia de autenticación.
Descripción	La plataforma recoge la secuencia de autenticación generada. Obtiene la equivalencia en imágenes de la secuencia.

Propiedad	Valor
	Traduce las imágenes a lenguaje natural. Genera el correo con la secuencia traducida. Envía el correo al usuario.
Pos condición	No aplica
Excepciones	El servicio de correo debe estar activo, caso contrario, no se envía la secuencia al usuario, se direccionará a la interfaz inicial y se desplegará el mensaje “Servicio de correo no disponible comuníquese con el administrador.

Tabla 12

Caso de Uso MAH-CU-09

Propiedad	Valor
Código	MAH-CU-09
Caso de uso	Replicar secuencia randómica recibida.
Actores:	Usuario del sistema
Resumen:	El usuario debe replicar en la interfaz generada la secuencia obtenida por correo.
Precondición	Obtener correo con la secuencia de autenticación.
Descripción	El usuario del sistema obtiene el correo con la secuencia randómica. Se debe replicar la secuencia en la interfaz generada. Al finalizar la replicación debe solicitar la verificación de su autenticación.

Propiedad	Valor
Pos condición	Validar secuencia ingresada.
Excepciones	El correo debe ser válido para poder recibir la secuencia generada por el sistema.

Tabla 13

Caso de Uso MAH-CU-10

Propiedad	Valor
Código	MAH-CU-10
Caso de uso	Validar secuencia ingresada.
Actores:	Plataforma de autenticación
Resumen:	La plataforma debe verificar que la secuencia ingresada por el usuario sea la correcta para poder avanzar al despliegue del perfil del usuario.
Precondición	Secuencia ingresada por el usuario
Descripción	La plataforma obtiene la secuencia ingresada por el usuario. Se compara la secuencia ingresada por la secuencia generada. Se autoriza el ingreso al sistema.
Pos condición	No aplica
Excepciones	Si el usuario falla en tres ocasiones se direccionará a la interfaz inicial y se desplegará el mensaje “Secuencia mal ingresada, no se logró autenticar”.

Tabla 14

Caso de Uso MAH-CU-11

Propiedad	**Valor**
Código	MAH-CU-11
Caso de uso	Desplegar perfil del usuario.
Actores:	Plataforma de autenticación
Resumen:	La plataforma obtiene la información del usuario y la despliega en una nueva interfaz.
Precondición	Secuencia correcta ingresada.
Descripción	La plataforma obtiene la información del usuario. Genera una interfaz con la información obtenida.
Pos condición	No aplica
Excepciones	No existen excepciones en este caso.

Los casos de uso reflejan los estados que se debe cumplir con sus respectivas excepciones para la autenticación en el mecanismo basado en contraseñas gráficas descartables, donde se observa las dos fases identificadas en el diagnóstico, que consiste en que el usuario debe cumplir la autenticación tradicional y posteriormente obtendrá lo necesario para superar la autenticación gráfica, el flujo completo de los casos de usos en detalle se ven reflejados en el diagrama de secuencia.

Diagramas de secuencia

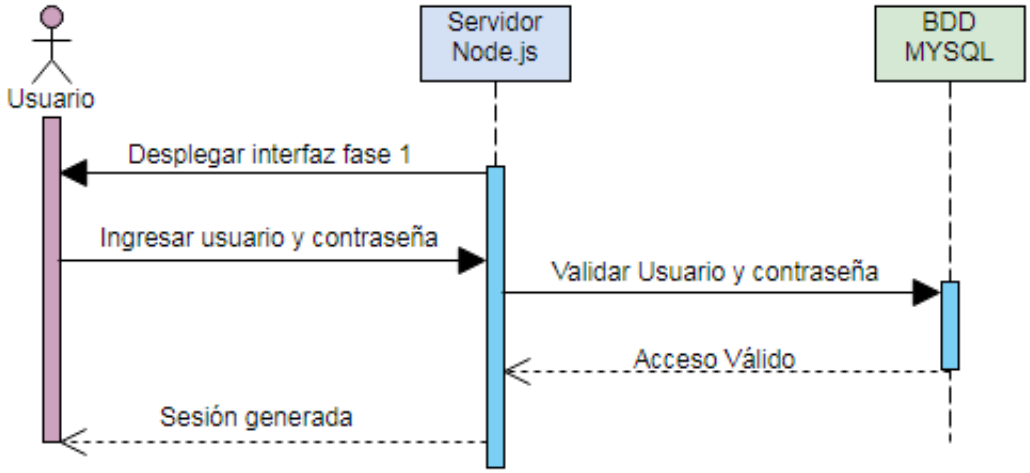
El sistema de autenticación basado en contraseñas gráficas descartables posee dos interfaces independientes, es necesario que el usuario interactúe con las mismas con el fin de poder autenticarse en el sistema, en las figuras 5 y 6 podemos visualizar la

interacción entre el usuario, el servidor de aplicaciones en Node.js que posee los algoritmos necesarios para la autenticación y el servicio de correo.

El sistema despliega la interfaz de autenticación de la fase uno, en esta interfaz existen dos campos, el primero para el nombre de usuario y el segundo para la contraseña, el sistema verifica con la base de datos MYSQL que las credenciales de acceso ingresadas por el usuario sean las correctas y responde al servidor de Node.js, en este punto se establece una sesión inicial que es necesaria para proceder a la segunda fase de autenticación.

Figura 4

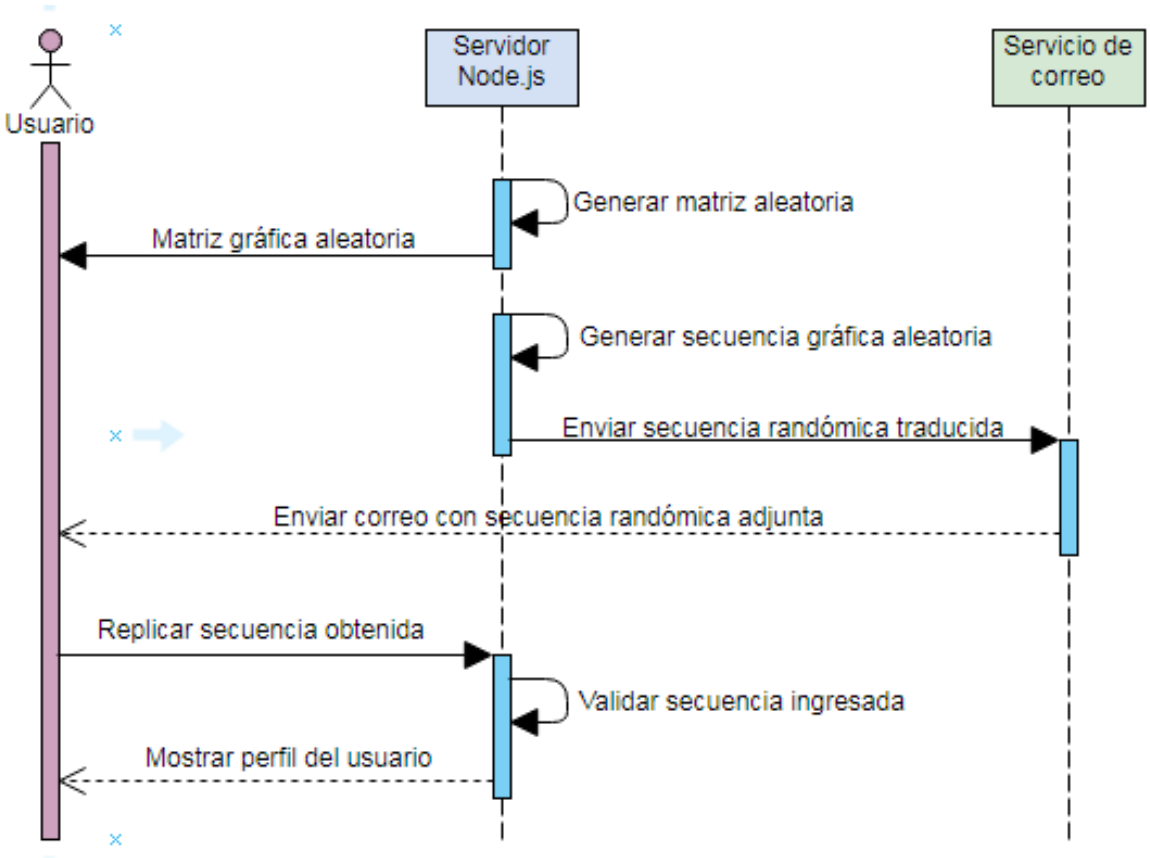
Diagrama de Secuencia de Fase 1 De Autenticación



El sistema genera una matriz aleatoria y obtiene sus equivalentes en imágenes para poder desplegar una interfaz usable para el usuario, el servidor de aplicaciones genera una secuencia randómica, la traduce en lenguaje natural, se la envía al servidor de correos que a su vez crea y envía el correo al usuario, el usuario procede a ingresar la secuencia obtenida en el correo y espera a que el sistema valide la secuencia ingresada, finalmente si la secuencia es la correcta se genera un interfaz con toda la información del usuario.

Figura 5

Diagrama de Secuencia de la Fase 2 de Autenticación.



Actuar

Diagrama de arquitectura

La figura 4 indica cómo se encuentra diseñada la arquitectura del mecanismo de autenticación generador de contraseñas gráficas descartables.

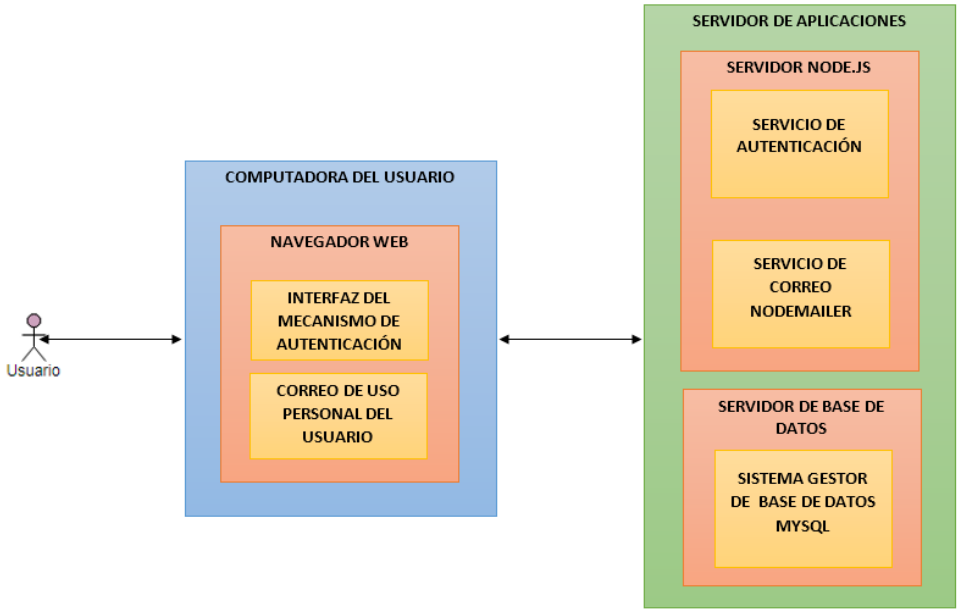
El usuario debe interactuar desde su computador, mediante un navegador web, con el sistema, donde visualizará la interfaz de autenticación y tendrá acceso a su correo para poder recibir y replicar la secuencia generada por el servidor.

El servidor de aplicaciones posee un servidor Node.js el mismo que está encargado de ofrecer dos tareas principales: el servicio de autenticación, que se ejecuta después de que el usuario ingreso sus credenciales tradicionales correctamente, que se presenta como el Core de la arquitectura al ser el encargado de generar las secuencias aleatorias y desplegar las interfaces necesarias para la interacción con el usuario y el servicio de correo NODEMAILER encargado de armar el correo en base la información obtenida desde el servicio de autenticación y enviarla al usuario.

Conjuntamente el servidor de aplicaciones abarca un servidor de base de datos donde esta almacenada la información del usuario para poder validar la autenticación en la fase uno y el correo del usuario donde recibirá la secuencia generada para la sesión.

Figura 6

Diagrama de Arquitectura del Mecanismo de Autenticación.

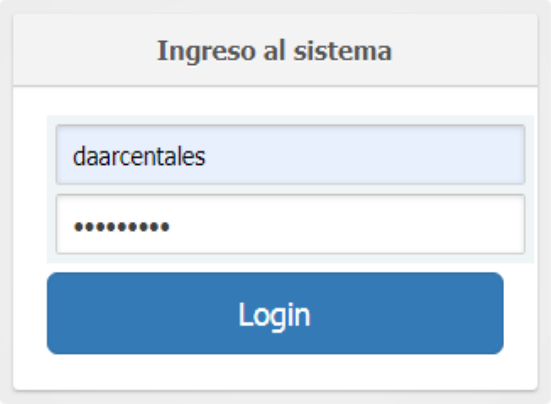


Mecanismo de autenticación

El mecanismo consta de dos fases de autenticación: la fase uno se presenta como una interfaz básica que posee dos campos de ingreso y un botón para el login, el sistema valida los datos en la base MYSQL y establece una sesión inicial, este método de autenticación es el tradicional.

Figura 7

Cuadro de Ingreso de Credenciales Tradicionales



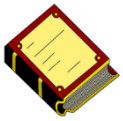
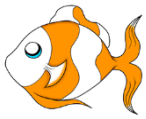
La segunda fase de autenticación consta de una matriz de imágenes, para comprender en su totalidad esta fase es necesario entender los siguientes puntos:

Equivalencia gráfica de números:

Cada número que se obtiene del algoritmo generador de secuencias randómicas, posee una equivalencia gráfica, para esto se seleccionó nueve imágenes con el objetivo de obtener matrices de tres por tres, las imágenes necesariamente son generales y entendibles, con el objetivo de que sean identificadas por cualquier tipo de usuario, en la tabla 18 se detallan los gráficos elegidos, su equivalencia numérica y su equivalente en texto:

Tabla 15

Imágenes Seleccionadas y su Respectiva Equivalencia.

Numero	Equivalencia en imagen	Equivalencia en texto
1		Tacón
2		Gorra
3		Vestido
4		Taza
5		Libro
6		Carta
7		Pez
8		Balón
9		Foco

Notación

Para poder describir los pasos necesarios para poder autenticarse en la fase dos es necesario establecer una notación que permita entender cómo funciona los algoritmos

Tabla 16

Notaciones

Notación	Descripción
SP	Semilla principal
LLANR	Llave alfanumérica randómica
HMAC(*,*)	Función de encriptación de HMAC
EXNUM(*)	Función de extracción de números
CADAU	Cadena de caracteres para extraer matriz y secuencia de autenticación
CADAUF	Cadena de caracteres de autenticación sin letras.
EXALE(*,*)	Función para extraer posiciones aleatorias de una cadena de caracteres numéricos.
MATAU	Matriz para la autenticación
SECAU	Secuencia de autenticación

Algoritmo propuesto

Paso 1: Después de cumplir la primera fase de autenticación se obtiene la SP, la SP consiste en un numero de diez dígitos, con el cual mediante la LLANR y la función HMAC, de la librería “CRYPTO" del servidor, se genera la CADAU.

CDAU = HMAC(SP,LLANR).

Paso 2: La CADAU es alfanumérica, para poder extraer la matriz y la secuencia de autenticación, es necesario utilizar la función EXNUM, la cual permitirá tener una cadena de solo números, los números serán remplazados por sus imágenes equivalentes para desplegar la matriz que visualizara el usuario.

CADAUF = EXNUM(CDAU)

Paso 3: Se genera una matriz randómica mediante el propio módulo de randómicos del servidor y se obtiene la MATAU

Paso 4: La MATAU permite generar la interfaz que el usuario visualizará para poder autenticarse.

Paso 5: Mediante la función EXALE se obtiene la secuencia randómica de autenticación.

SECAU = EXALE(CADAUF,3)

Paso 7: Se genera un digito más, que es el encargado de definir porque columna o fila se debe realizar la autenticación.

Paso 8: Se despliega una interfaz con la MATAU con su respectiva equivalencia en imágenes.

Paso 9: Se genera un correo donde está la información de autenticación, es decir, que se obtiene los nombres de la SECAU en lenguaje natural y se lo envía al usuario.

Con este algoritmo tenemos todo lo necesario para que el usuario se pueda autenticarse.

Cabe recalcar que el algoritmo en ejecución cumple los siguientes parámetros definidos por la NIST para generadores OTP basados en Software:

La CADAU presenta una dificultad alta para su replicación, donde el servidor posee la llave para su generación.

Como el algoritmo HMAC se basa en el tiempo es necesario que la contraseña presente una validez de 2 minutos.

Se configuró un límite de intentos para fallar en la autenticación.

Con esta configuración se puede calcular el número de posibles contraseñas utilizando la fórmula de permutación sin repetición.

$$\frac{n!}{(n-r)!}$$

Donde n es el rango de números que tenemos en la matriz y r el rango de la secuencia:

$$\frac{9!}{(9-3)!} = 504$$

Y el número obtenido lo multiplicamos por las posibles formas de ordenarse en la matriz.

$$6 * 504 = 3024$$

En total poseemos 3024 posibles formas de autenticarse.

Evaluación del algoritmo

Es necesario que el algoritmo generador de secuencias randómicas, cumpla aleatoriedad, donde las secuencias generadas no presenten ningún tipo de patrón alternante, periódico o de tendencia.

Para poder validar la aleatoriedad del algoritmo se aplicó el test de rachas con un nivel de confianza de 99% que consiste un valor crítico de Z.99%=2.58:

Generamos 25 secuencias en el sistema

Tabla 17

Pruebas del Algoritmo Obtenidas

Numero de prueba	Valor obtenido
1	618
2	137
3	783

Numero de prueba	Valor obtenido
4	689
5	273
6	369
7	921
8	295
9	192
10	864
11	389
12	547
13	653
14	934
15	396
16	469
17	517
18	581
19	976
20	269
21	968
22	938
23	951
24	173
25	594

El valor de la mediana de las secuencias es 581, el valor de la racha es negativa cuando la secuencia es menor y positiva cuando es mayor o igual a la mediana, el conteo consiste en que se añade uno cuando la racha cambia de estado.

En la tabla 21 podemos observar el conteo de las rachas y la el cambio de estado.

Tabla 18

Conteo de Rachas.

Valor de la secuencia	Racha	Conteo de rachas
618	+	1
137	-	2
783	+	3
689	+	3
273	-	4
369	-	4
921	+	5
295	-	6
192	-	6
864	+	7
389	-	8
547	-	8
653	+	9
934	+	9
396	-	10
469	-	10

Valor de la secuencia	Racha	Conteo de rachas
517	-	10
581	+	11
976	+	11
269	-	12
968	+	13
938	+	13
951	+	13
173	-	14
594	+	14

Contabilizamos los datos para poder calcular la normal de las medias, la varianza y Z

Tabla 19

Datos obtenidos del Test de Rachas.

Operación	Total
Valor de la mediana	581
Casos < Valor de la prueba	12
Casos > = Valor de la prueba	12
Casos en total	25
Numero de rachas	14
Normal de media (u_r)	13
Varianza (σ_r)	2.395648229
Z	0.417423555

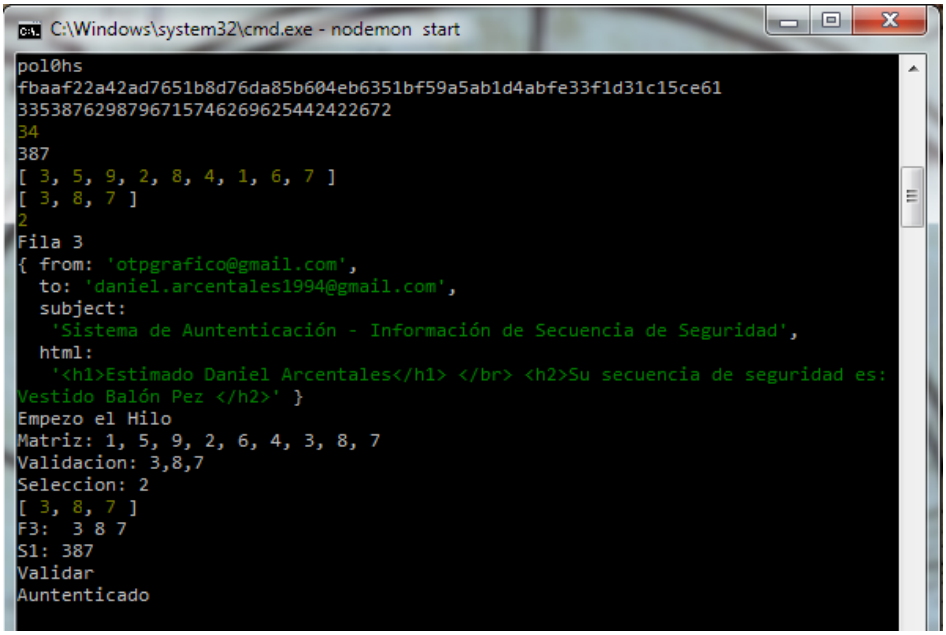
En conclusión el valor de z de 0.417423555 se encuentra en el rango de -2.58 y 2.58, es decir, que el algoritmo si es aleatorio, dando robustez al sistema y evitando que exista algún tipo de predicción frente a las claves que se pueden generar.

Ejecución de prueba

Cuando se supera la fase de autenticación tradicional, el servidor de aplicaciones ejecuta el algoritmo y obtiene lo siguiente:

Figura 8

Log del Servidor con los Datos Obtenidos.



En base a la notación explicada en el la sección 3.3.2.2 obtenemos la siguiente tabla:

Tabla 20

Notación obtenida en la Ejecución de Prueba

Notación	Descripción
SP	1721594446

Notación	Descripción
LLANR	pol0hs
CADAU	fbaaf22a42ad7651b8d76da85b604eb6351bf59a5ab1d4abfe3 3f1d31c15ce61
CADAUF	335387629879671574626962544242267 2
MATAU	[3, 5, 9, 2, 8, 4, 1, 6, 7]
SECAU	[3, 8, 7]
SECAU Traducida	Vestido Balón Pez

Y obtenemos la interfaz desplegada en la figura 9.

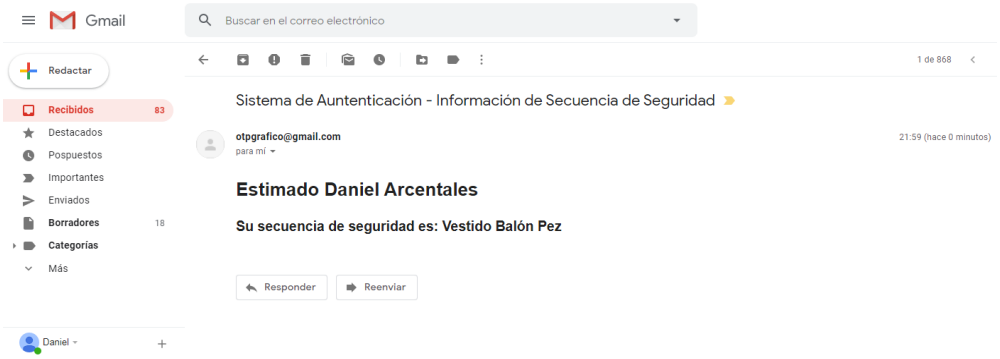
Figura 9

Matriz de 3x3 Generada por el Sistema de Autenticación

Correo recibido correctamente

Figura 10

Correo Obtenido por El Usuario



Se ordena correctamente la secuencia en base a la información obtenida en el correo.

Figura 11

Matriz de 3x3 con la Secuencia Correctamente Ordenada

Y finalmente podemos acceder al perfil del usuario autenticado.

Figura 12

Interfaz con la Información del Usuario

Reflexionar

Es necesario tener todos los componentes actualizados con el objetivo que las tecnologías que se muestran en el diagrama de arquitectura funcionen correctamente y posean todos los parches de seguridad distribuidos por sus creadores permitiendo tener un ambiente óptimo para el mecanismo de autenticación propuesto.

Para darle versatilidad y mantenimiento al aplicativo es necesario realizar cambios constantes de imágenes, considerando su usabilidad y entendimiento, si se realiza este proceso es indispensable que no presenten ambigüedad y sean fácil de entender.

Esta solución es enfocada a un ambiente web, si se buscar dar compatibilidad con dispositivos móviles es necesario definir nuevos requerimientos, es decir, repetir toda la metodología de la investigación basada en acción.

Capítulo IV - Evaluación de Seguridad y Usabilidad

Este capítulo muestra y analiza dos aspectos fundamentales que debe cumplir un mecanismo de autenticación, en el aspecto de seguridad, se configuró un entorno de pruebas para evaluar cómo el mecanismo contrarresta los siguientes ataques para la sustracción de credenciales: Keylogger, fuerza bruta, diccionario y Shoulder Surfing. El segundo aspecto considerado es el de usabilidad, donde se presenta estadísticas de aceptación de potenciales usuarios del aplicativo, cabe recalcar que este mecanismo no tiene un target específico y lo que se busca es que sea entendible para diferentes tipos de usuarios.

Para cada ataque seleccionado, se realizó pruebas y se verificó la resistencia del algoritmo frente a las diferentes técnicas para sustracción y vulneración de credenciales.

El sistema controla que solo se realice tres intentos, es decir, los ataques sólo poseen tres intentos para adivinar la contraseña.

Análisis de seguridad

Preparación del entorno

Esta evaluación consiste en usar software malicioso para la sustracción de credenciales, para esto se preparó un entorno local, que contiene las siguientes características y configuración:

Servidor. Máquina virtual con 2GB de Ram, 10Gb de almacenamiento y un adaptador de red tipo puente, Linux con sistema operativo Ubuntu versión 18.04.02 LTS, base de datos MYSQL 14.4. y servidor Node.js versión 8.10.

Cliente de pruebas. Máquina virtual de 4GB de Ram, 10Gb de almacenamiento y adaptador de red tipo puente, sistema operativo Windows 7 y navegador web Google Chrome.

Ataque de fuerza bruta y diccionario

Software seleccionado. CRUNCH

Funcionamiento. Este software malicioso permite configurar una fuente de datos, conocido como diccionario, mediante el cual realiza las combinaciones necesarias para predecir la contraseña del usuario, en este caso la secuencia.

Ejecución del ataque. Se configuro una base de información con las palabras previamente seleccionadas y se ejecutó el programa malicioso, donde se obtuvo posibles combinaciones para predecir la contraseña generada por el algoritmo.

Figura 13

Interfaz de la Herramienta CRUCH para Obtener Secuencias

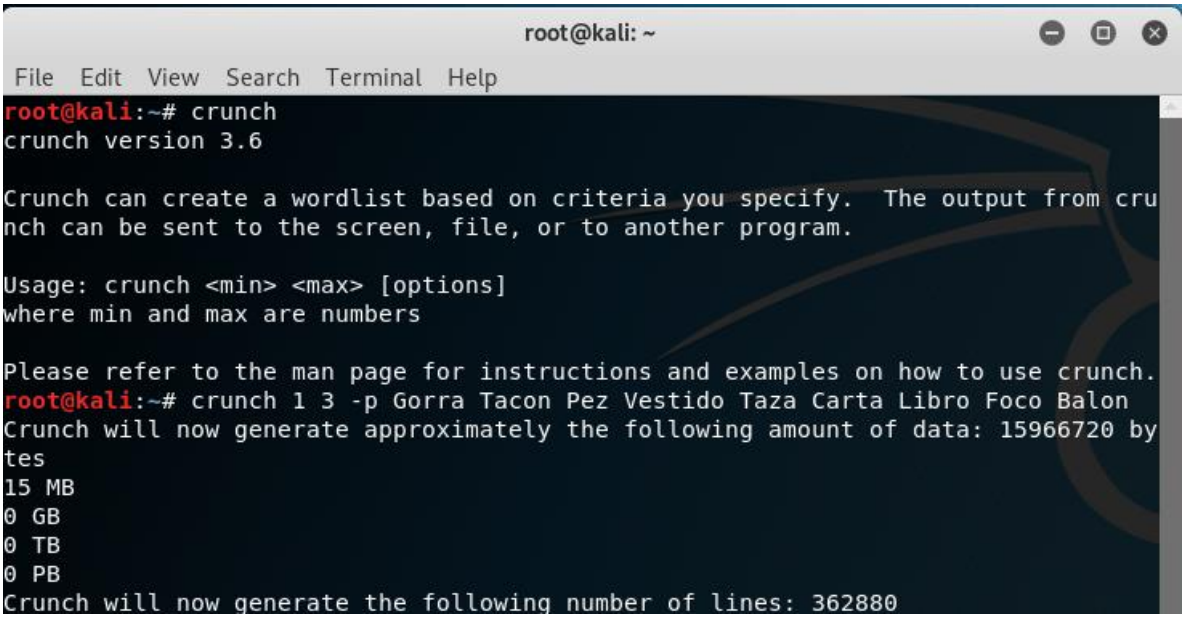


Tabla 21

Tabla de Ejecución de Pruebas CRUCH

Prueba	CRUCH	SECAU Traducida	Resultado
1	1: Gorra Tacón Pez 2: Gorra Vestido Taza	Libro Tacón Pez	No se pudo autenticar

Prueba	CRUCH	SECAU Traducida	Resultado
	3: Gorra Zapato Carta		
2	1: Libro Carta Libro 2: Libro Taza Tacón 3: Libro Taza Foco	Carta Tacón Vestido	No se pudo autenticar.
3	1: Carta Balón Gorra 2: Carta Taza Libro 3: Carta Vestido Libro	Libro Foco Carta	No se pudo autenticar
4	1: Foco Balón Taza 2: Foco Libro Taza 3: Foco Taza Gorra	Carta Balón Libro	No se pudo autenticar
5	1: Vestido Tacón Pez 2: Vestido Tacón Pez 3: Vestido Gorra Pez	Foco Taza Gorra	No se pudo autenticar

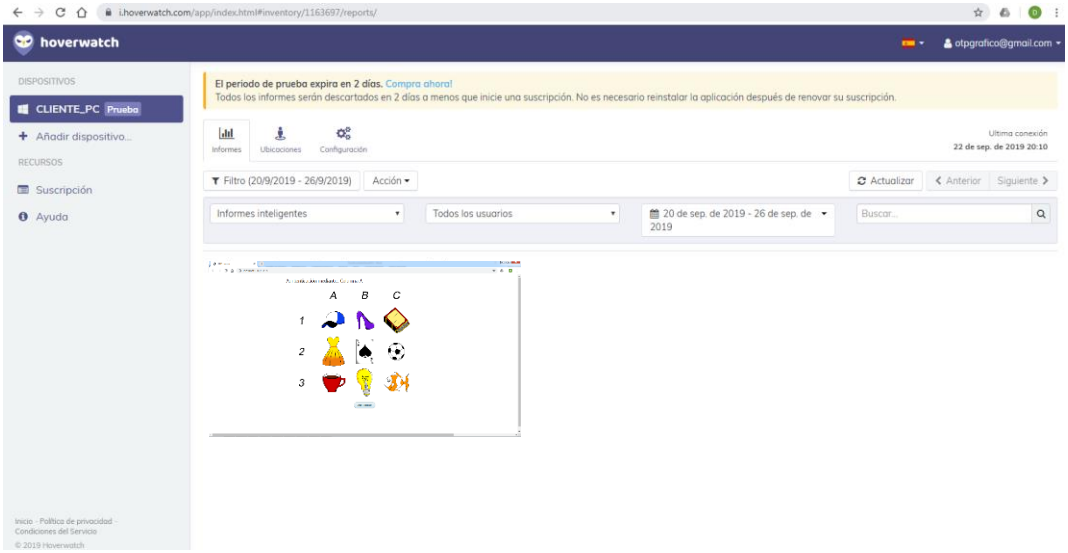
Ataque de Keylogger

Software seleccionado. Hoverwatch

Funcionamiento. Es un software completo para monitorear un computador, entre sus principales características son: Grabar todo lo que se ingresa por el teclado, Captura de pantallas del computador y visualización de historial de navegación de manera remota.

Figura 14

Interfaz de la herramienta Hoverwatch.



Ejecución del ataque. El ataque logró tomar las capturas de pantalla del ordenamiento realizado por el usuario y obtuvo la secuencia “Vestido Balón Pez” al intentar ingresar nuevamente en otra sesión el algoritmo generó una nueva contraseña, en este caso “Carta Balón Gorra”, dejando a la obtenida por el keylogger inservible.

Ataque de Shoulder Surfing

Software escogido. No necesita software.

Funcionamiento. Se simuló un atacante con el objetivo de receptar las secuencias ingresadas e intentar predecir la siguiente secuencia.

Ejecución del ataque. En este caso el atacante se posicionó en una línea de visión directa hacia la pantalla de la víctima y logró anotar la secuencia ingresada por el usuario en este caso “Gorra Vestido Taza”, el atacante busca replicar la secuencia en una nueva sesión, pero el sistema generó una nueva contraseña “Vestido Balón Pez”, en este caso el atacante no logra ingresar al sistema, reflejando que el algoritmo es robusto frente al Shoulder Surfing.

Como se puede observar los ataques seleccionados para esta evaluación, son fáciles de aplicar y no necesitan conocimientos avanzados en computación, es decir, cualquier persona puede aplicar estas técnicas para sustraer credenciales de acceso a diferentes sistemas.

En base a las pruebas realizadas podemos concluir que una solución que ofrece contraseñas gráficas de un solo uso presenta una seguridad robusta, mitigando las principales técnicas para la sustracción de credenciales.

Análisis de usabilidad

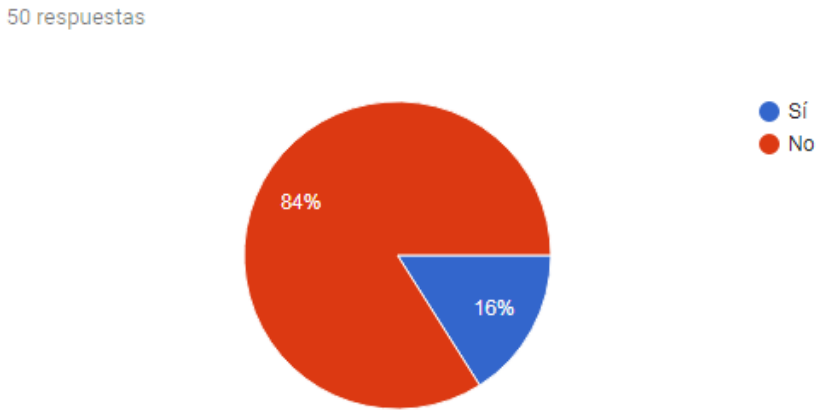
El NIST en su publicación SP-800-63 en el apartado de usabilidad propone que un sistema debe ser fácil de usar y fácil de entender, bajo este principio se planteó una encuesta, que permitió concluir si el aplicativo entrega un aporte de usabilidad al usuario final y cumple los factores mencionados, la encuesta se realizó a 50 personas de edades entre 19 y 60 años con conocimientos básicos en el uso de computadoras, la encuesta consiste en dos partes, la primera se enfoca en si el usuario posee algún conocimiento sobre los ataques evaluados en esta autenticación y la segunda parte abarca la aceptación del mecanismo de autenticación propuesto.

¿Conoce para qué sirve un Keylogger?

Se observa que el 84% de los encuestados desconoce que es un Keylogger por ende son vulnerables a un ataque de sustracción de credenciales mediante esta técnica, es un dato preocupante, ya que, en la actualidad, existe mucho software malicioso que se encarga de capturar las pulsaciones del teclado, es muy fácil de usar y adquirir.

Figura 15

Gráfico de Encuestados que Conocen Keylogger.

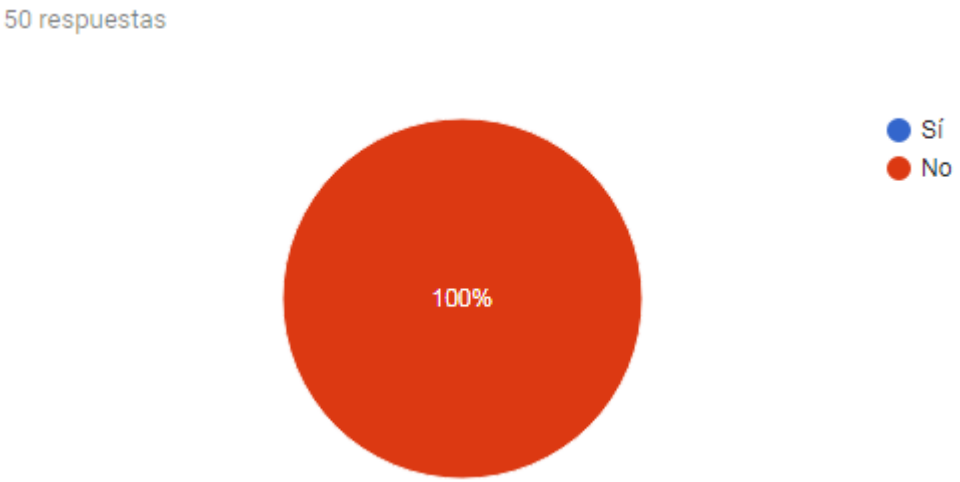


¿Sabe que es Shoulder Surfing?

El Shoulder Surfing es una de las técnicas más fáciles y sencillas de aplicar, ya que no depende de conocimientos altos en informática, ni es necesario tener algún software específico para aplicarlo, el 100% de los encuestados no conoce está técnica, es decir, que sus credenciales tradicionales están expuestas a este método de sustracción.

Figura 16

Gráfico de encuestados que conocen Shoulder Surfing.

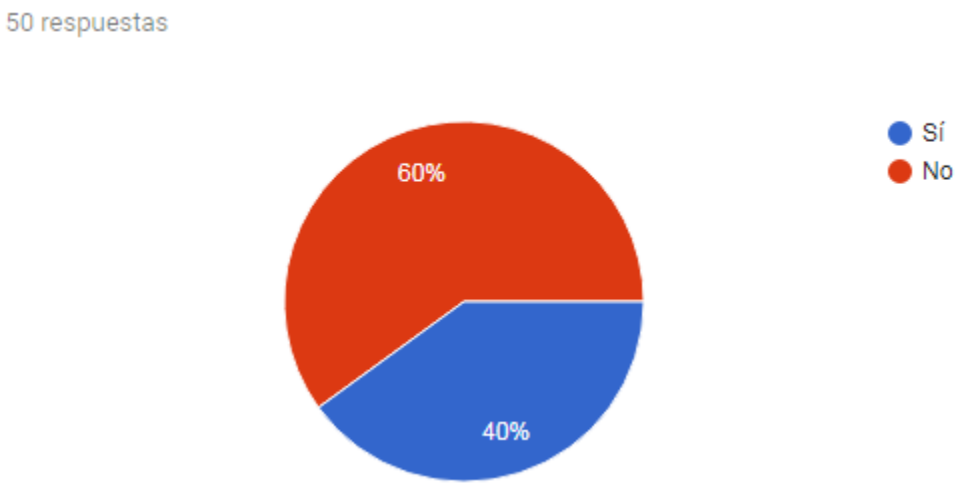


¿Conoce qué es Phishing?

En esta pregunta podemos observar que un buen porcentaje de los encuestados conoce lo que es Phishing, esto se debe a que es una de las técnicas más usadas para robar credenciales en la banca, donde el atacantes simula la interfaz de login y se la envía mediante correo electrónico a la víctima para que ingrese sus credenciales, los bancos han tratado de mitigar esta técnica educando a sus usuarios a lo largo de este tiempo con el objetivo de que no caigan en este método de sustracción.

Figura 17

Gráfico de Encuestados que Conocen Phising

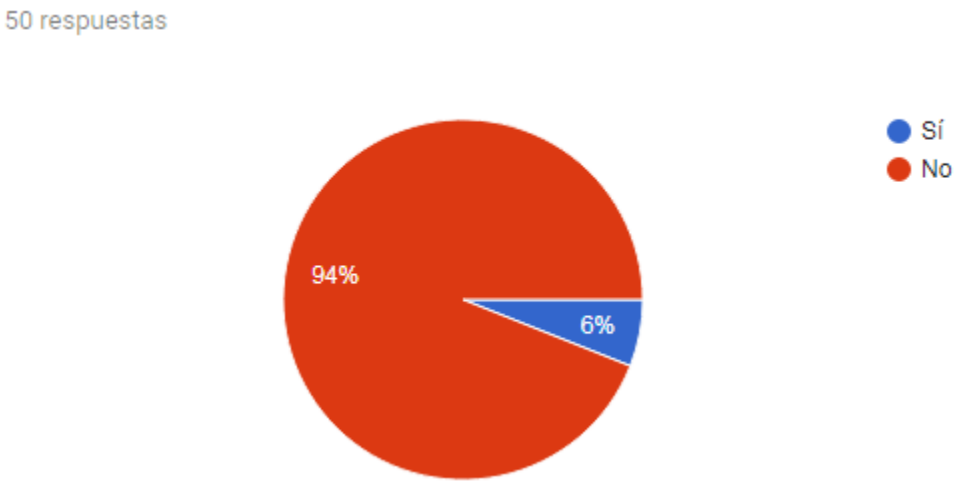


¿Sabe que es un ataque de diccionario?

El 94% de los encuestados no conoce este tipo de ataque, el cual se encarga de armar diferentes tipos de contraseña en base a información básica del usuario (nombre, fechas, características) con el objetivo de adivinar la clave, esta técnica es muy efectiva, ya que, los usuarios utilizan combinación de palabras conocidas para ellos, con el objetivo de no olvidar sus credenciales, por ende, con cierta información del usuario, su contraseña es fácil de sustraer.

Figura 18

Gráfico de Encuestados que conocen el Ataque de Diccionario

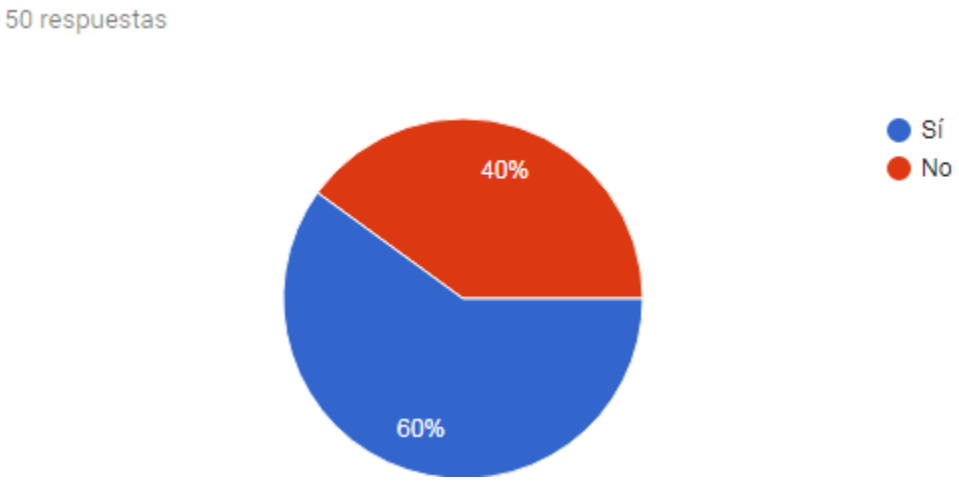


¿Sabe que es una contraseña gráfica?

El 60% de los encuestados conoce lo que es una contraseña gráfica, esto se debe a que diferentes sistemas implementan contraseñas gráficas como mecanismo de autenticación complementario al tradicional.

Figura 19

Gráfico de Encuestados Sobre Conocimiento de Contraseñas Gráficas

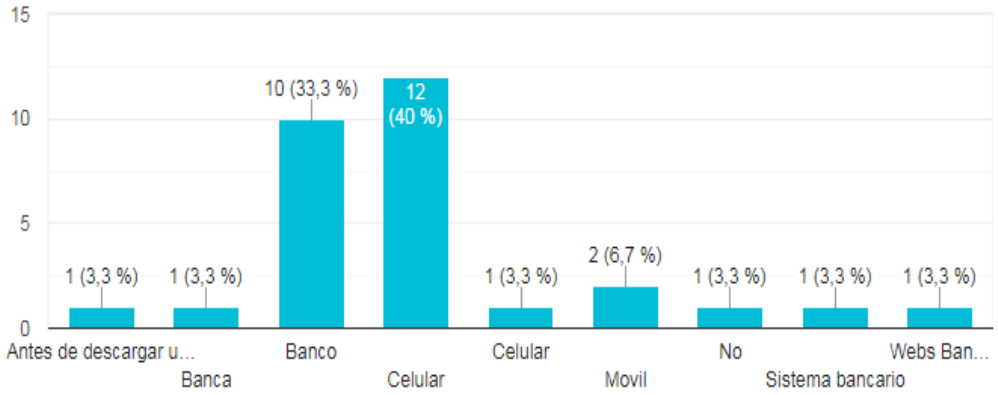


¿Si la respuesta es sí, dónde ha utilizado una contraseña gráfica?

La mayoría de los encuestados coincidieron en 2 áreas fundamentales en donde encontramos implementados contraseñas gráficas, en el móvil, dónde utilizan contraseñas gráficas de tipo patrón, consiste en que el usuario debe unir una serie de puntos, esta contraseña es vulnerable frente al Shoulder Surfing, la otra área es la banca, estos sistemas usan la contraseña gráfica para mecanismos de autenticación con doble fase de autenticación, para hacer el acceso al sistema más robusto, el grave problema de estas contraseñas gráficas es que son estáticas, por ende, si el atacante logra sustraer las contraseña, se pierde toda la seguridad del sistema.

Figura 20

Gráfico de Lugar de Uso de las Contraseñas Gráficas



¿Alguna vez se autenticado en un sistema ordenando una secuencia de imágenes, si la respuesta es sí, en qué sistema?

49 de los encuestados no se han autenticado mediante el ordenamiento de secuencias, esto refleja que el sistema presenta una idea diferente a las soluciones actuales de contraseñas gráficas estáticas.

Una persona afirmó que sí, pero no colocó el nombre del sistema para poder contrastar las diferencias con el sistema propuesto

¿Usted comprende las imágenes colocadas en esta matriz?

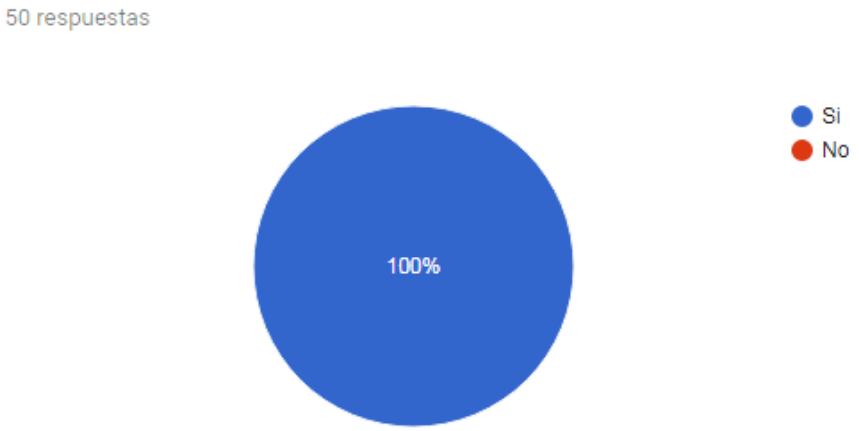
Figura 21

Ejemplo de una Matriz de Imágenes Generada por el Sistema.

El 100% de los encuestados logró comprender las imágenes, esto refleja que las imágenes es un factor importante en el mecanismo propuesto, ya que, si las imágenes no son entendidas por el usuario, puede producir ambigüedad ocasionando que el usuario no pueda autenticarse.

Figura 22

Gráfico de Encuestados que Comprendieron las Imágenes.

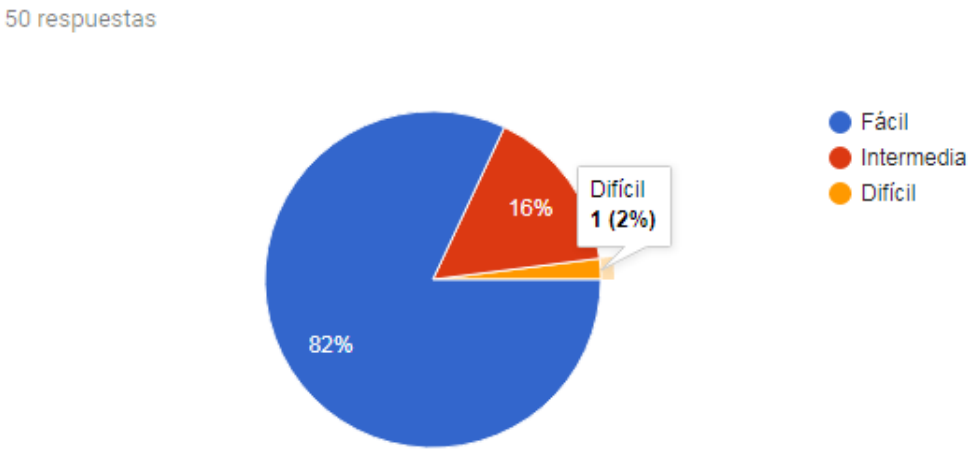


En base a la imagen de la anterior pregunta, si se le pidiera que ordene 3 imágenes en una fila o columna, este proceso tendría una dificultad:

82% de los encuestado concluyeron que el procedimiento de autenticación es sencillo, es decir, es fácil de usar, tan solo un encuestado no comprendió el proceso, esto puede ser revisado, con el objetivo de hacer un mecanismo completamente usable para cualquier usuario.

Figura 23

Gráfico de Compresión del Procedimiento Base del Algoritmo

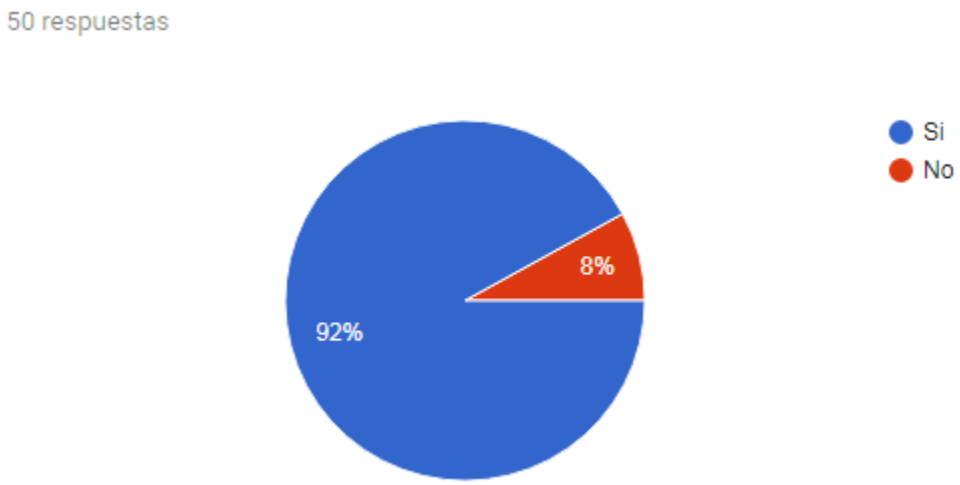


Utilizaría este método para autenticarse en el algún sistema, por ejemplo el banco, conociendo que cada vez se le entregará secuencias diferentes para ingresar al sistema.

Podemos concluir que el mecanismo de autenticación posee un porcentaje notable de aceptación, donde los usuarios lo utilizarían para poder autenticarse de manera segura en algún sistema.

Figura 24

Gráfico de aceptación de la Solución Propuesta



Capítulo V - Conclusiones, recomendaciones y líneas de trabajo futuro

Conclusiones

La revisión básica de literatura realizada permitió identificar diferentes mecanismos propuestos de contraseñas de un solo uso y contraseñas gráficas, de manera independiente, donde la solución propuesta agrupa las ventajas destacables de dichos métodos, permitiendo que el sistema generador de contraseñas gráficas descartables sea fácil de usar, de entender e implementar.

El algoritmo generador de contraseñas gráficas descartables cumple lo establecido por la NIST en donde se detalla cómo debe ser un software generador OTP, esto permite que el sistema no genere contraseñas predecibles, con algún patrón alternante, periódico o de tendencia, reflejando que el algoritmo generador es robusto.

Los parámetros seleccionados en base a lo propuesto por la NIST en la publicación SP-800-63 permitieron analizar la seguridad y usabilidad de sistema híbrido basado en Drag & Drop como contraseña gráfica y algoritmo generador de secuencias randómicas permitieron que sea correctamente evaluado concluyendo que si cumple como una solución alternativa de autenticación y podría ser implementado en cualquier ámbito donde sea necesaria una verificación de identidades digitales.

Recomendaciones

Los sistemas de autenticación deben cumplir de manera primordial dos características; deben ser usables y robustos, estos dos aspectos van de la mano, y el éxito del sistema es que se cumplan de manera conjunta, un error común que suele presentarse es que un mecanismo bastante robusto es poco usable o su contra parte, que es muy usable pero carece de robustez.

Es necesario que los mecanismos de autenticación vayan de la mano con una correcta cultura de seguridad informática, ya que los sistemas pueden presentar una

robustez alta pero el usuario, al ser el eslabón más débil del sistema, puede ocasionar una brecha de seguridad.

El cibercrimen crece de manera exponencial, las estadísticas de diferentes empresas proveedoras de seguridad informática lo corroboran, bajo esta realidad, es necesario que las empresas busquen estrategias para poder proteger su información y nosotros como investigadores proponer nuevos mecanismos de autenticación que utilicen en varios factores, presenten diferentes fases y posean una usabilidad alta con el objetivo de mitigar el mayor número de técnicas de sustracción de credenciales y salvaguardando la información de las personas.

Finalmente es importante considerar el entorno, conocer frente a que ataques es más vulnerable o que le hace falta para que sea robusto y usable, y en base a esto concluir si es necesario cambiar el mecanismo de autenticación o mejorarlo, definiendo las estrategias necesarias para proponer una solución óptima.

Líneas de trabajo futuro

El mecanismo de autenticación actual puede ser complementado con un aplicativo móvil, el cual, debe tener la capacidad de replicar el algoritmo generador de secuencias randómicas o tener una línea de comunicación segura con el servidor, para agregar otro factor de autenticación al sistema y por ende hacer más robusto al mecanismo, en este caso.

El mecanismo puede presentar mejoras y robustez, si se lo enlaza con un diccionario de palabras y un catálogo de imágenes, donde no solo la secuencia presente aleatoriedad, es decir, la matriz y sus imágenes sean completamente diferentes en cada sesión de autenticación.

Bibliografía

Agarwal, G., Singh, S., & Indian, A. (2011). Analysis of knowledge base graphical password authentication. *The 6th International Conference on Computer Science & Education (ICCSE 2011)*, (Iccse), 6–9.

Almuairfi, S., Veeraraghavan, P., & Chilamkurti, N. (2011). IPAS: Implicit password authentication system. *Proceedings - 25th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2011*, 430–435. http://doi.org/10.1109/WAINA.2011.36

Arunprakash, M., & Gokul, T. R. (2011). Network security-overcome password hacking through graphical password authentication. *Proceedings of National Conference on Innovations in Emerging Technology, NCOIET'11*, 43–48. http://doi.org/10.1109/NCOIET.2011.5738831

Balaji, R., & Roopak, V. (2011). DPASS - Dynamic password authentication and security system using grid analysis. *ICECT 2011 - 2011 3rd International Conference on Electronics Computer Technology*, *2*, 250–253. http://doi.org/10.1109/ICECTECH.2011.5941695

Bhand, A., & Shirke, S. (2015). Enhancement of Password Authentication System Using Graphical Images. *International Conference on Information Processing*, 217–219.

Divya, R., & Muthukumarasamy, S. (2015). An impervious QR-based visual authentication protocols to prevent black-bag cryptanalysis. *Proceedings of 2015 IEEE 9th International Conference on Intelligent Systems and Control, ISCO 2015*. http://doi.org/10.1109/ISCO.2015.7282330

Fan, Y. T., & Su, G. P. (2009). Design of two-way one-time-password authentication scheme based on true random numbers. *2nd International Workshop on*

Computer Science and Engineering, WCSE 2009, *1*, 11–14. http://doi.org/10.1109/WCSE.2009.611

Gao, H., Liu, N., Li, K., & Qiu, J. (2014). Usability and security of the recall-based graphical password schemes. *Proceedings - 2013 IEEE International Conference on High Performance Computing and Communications, HPCC 2013 and 2013 IEEE International Conference on Embedded and Ubiquitous Computing, EUC 2013*, (60903198), 2237–2244. http://doi.org/10.1109/HPCC.and.EUC.2013.321

Ghazi Kalayeh, M. R., Nik, M. H., & Kordestani, H. (2013). Using template-based passwords for authentication in e-banking. *2013 7th Intenational Conference on E-Commerce in Developing Countries: With Focus on e-Security, ECDC 2013*, (Figure 1), 1–9. http://doi.org/10.1109/ECDC.2013.6556746

Goutham, R. A., Kim, D.-S., & Yoo, K.-Y. (2014). Implicit Graphical Password Mutual Authentication Using Mirror-image Encryption. *Proceedings of the 2014 Conference on Research in Adaptive and Convergent Systems*, 218–223. http://doi.org/10.1145/2663761.2664194

Gupta, S., Vashisht, S., & Singh, D. (2016). A CANVASS on cyber security attacks and countermeasures. *2016 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016*, (Iciccs), 31–35. http://doi.org/10.1109/ICICCS.2016.7542335

Hafiz, M. D., Abdullah, A. H., Ithnin, N., & Mammi, H. K. (2008). Towards identifying usability and security features of graphical password in knowledge based authentication technique. *Proceedings - 2nd Asia International Conference on Modelling and Simulation, AMS 2008*, 396–403. http://doi.org/10.1109/AMS.2008.136

Han, W., Cao, Y., & Lei, C. (2011). Using a smart phone to strengthen password-based authentication. *Proceedings - 2011 IEEE International Conferences on Internet of*

Things and Cyber, Physical and Social Computing, IThings/CPSCom 2011, 372–379. http://doi.org/10.1109/iThings/CPSCom.2011.64

Haque, M. A., Khan, N. Z., & Khatoon, G. (2016). Authentication through keystrokes: What you type and how you type. *Proceedings of 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks, ICRCICN 2015*, 257–261. http://doi.org/10.1109/ICRCICN.2015.7434246

Herzberg, A., & Margulies, R. (2012). My authentication album: Adaptive images-based login mechanism. *IFIP Advances in Information and Communication Technology*, *376 AICT*, 315–326. http://doi.org/10.1007/978-3-642-30436-1_26

Hunt, T. (2019). The 773 Million Record " Collection # 1 " Data Breach. Retrieved from https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Khan, W. Z., Xiang, Y., Aalsalem, M. Y., & Arshad, Q. (2011). A hybrid graphical password based system. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7017 LNCS*(PART 2), 153–164. http://doi.org/10.1007/978-3-642-24669-2_15

Kolekar, V. K., & Vaidya, M. B. (2016). Click and session based - Captcha as graphical password authentication schemes for smart phone and web. *Proceedings - IEEE International Conference on Information Processing, ICIP 2015*, 669–674. http://doi.org/10.1109/INFOP.2015.7489467

Lashkari, A. H., Manaf, A. A., & Masrom, M. (2011). A secure recognition based Graphical Password by watermarking. *Proceedings - 11th IEEE International Conference on Computer and Information Technology, CIT 2011*, *07*(1), 164–170. http://doi.org/10.1109/CIT.2011.29

Lin, P. L., Weng, L. T., & Huang, P. W. (2008). Graphical passwords using images with random tracks of geometric shapes. *Proceedings - 1st International*

Congress on Image and Signal Processing, CISP 2008, *3*, 27–31. http://doi.org/10.1109/CISP.2008.603

Liu, H., & Zhang, Y. (2013). An improved one-time password authentication scheme. *International Conference on Communication Technology Proceedings, ICCT*, 1–5. http://doi.org/10.1109/ICCT.2013.6820340

López Grande, C. E., & Edgardo, C. (2015). Ingeniería social: el ataque silencioso, (1). Retrieved from http://www.redicces.org.sv/jspui/handle/10972/2910

Mihajlov, M. (2011). ImagePass - Designing Graphical Authentication for Security, 262–267.

Mir, M. S., Wani, S., & Ibrahim, J. (2013). Critical information security challenges: An appraisal. *2013 5th International Conference on Information and Communication Technology for the Muslim World, ICT4M 2013*. http://doi.org/10.1109/ICT4M.2013.6518890

Rajarajan, S., Prabhu, M., Palanivel, S., & Karthikeyan, M. P. (2014). Gramap: Three stage graphical password authentication scheme. *Journal of Theoretical and Applied Information Technology*, *61*(2), 262–269.

Rodríguez, D., Jordi, G., & Roquet, V. (n.d.). Metodología de la investigación.

Saeed, S., & Umar, M. S. (2015). A Hybrid Graphical User Authentication Scheme. *International Conference on Communication, Control and Intelligent Systsems*. http://doi.org/10.1109/CCIntelS.2015.7437951

Srivastava, S., & Sivasankar, M. (2017). On the generation of alphanumeric one time passwords. *Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016*, *1*(i), 1–3. http://doi.org/10.1109/INVENTIVE.2016.7823287

Sruthi. (2015). Shoulder Surfing attack. *IEEE Transactions on Information Forensics and Security*.

Symantec. (2018). Informes sobre las Amenazas para la Seguridad en Internet. *Physical Review B*, *72*(10), 1–13.

Tabrez, S. (2017). Pass-Matrix authentication, 776–781.

Umar, M. S., & Rafiq, M. Q. (2012). Select-to-Spawn: A novel recognition-based graphical user authentication scheme. *2012 IEEE International Conference on Signal Processing, Computing and Control, ISPCC 2012*, 0–4. http://doi.org/10.1109/ISPCC.2012.6224382

Watchguard. (2017). Internet Security Report - Q4 2017. Retrieved from https://www.watchguard.com/wgrd-resource-center/security-report-q4-2017

Yadav, U. D. (2013). to increase the capacity of KBAM, (Iceccn), 513–517.

Yao. (2011). Direct location of amino acid phenylthiohydantoins on paper chromatograms with ultraviolet light. *Analytical Biochemistry*, *21*(3), 472–474. http://doi.org/10.1109/SERA.2011.18

Zhao, H., & Li, X. (2007). S3PAS : A Scalable Shoulder-Surfing Resistant Textual-Graphical Password.