"DESARROLLO DE UN SISTEMA DE AUTENTICACIÓN GRÁFICA BASADO EN DRAG&DROP PARA AMBIENTE WEB".

CRISTHIAN JAVIER DUARTE BOGADO

Trabajo de Grado presentado a la Facultad de Ciencias y Tecnología de la Universidad Nacional de Caaguazú, como requisito para la obtención del título de Ingeniero en Informática.

UNIVERSIDAD NACIONAL DEL CAAGUAZÚ

FACULTAD DE CIENCIAS Y TECNOLOGÍA

Carrera de Ingeniería en Informática

Coronel Oviedo, Paraguay

2018

"DESARROLLO DE UN SISTEMA DE AUTENTICACION GRAFICA BASADO EN DRAG&DROP PARA AMBIENTE WEB"

CRISTHIAN JAVIER DUARTE BOGADO

Orientador Académico de Proyecto de Fin de Grado:

Prof. Ing. Héctor Estigarribia

Responsable Académico de Proyecto de Fin de Grado:

Prof. Ing. Maira Santacruz Bogado

Cotutor de Proyecto de Fin de Grado:

Ing. Andrea Leiva Lugo

Trabajo de Grado presentado a la Facultad de Ciencias y Tecnología de la Universidad Nacional de Caaguazú, como requisito para la obtención del título de Ingeniero en Informática.

UNIVERSIDAD NACIONAL DEL CAAGUAZÚ
FACULTAD DE CIENCIAS Y TECNOLOGÍA
Carrera de Ingeniería en Informática
Coronel Oviedo, Paraguay
2018

PÁGINA DE APROBACIÓN

MESA EXAMINADORA DE SUSTENTACIÓN DE TESIS DE GRADO

Carrera de Ingeniería en Informática

Título de la Tesis: "DESARROLLO, IMPLEMENTACIÓN Y EVALUACIÓN DE UN SISTEMA DE AUTENTICACIÓN GRAFICO PARA AMBIENTES WEB".

Calificación Obtenida: _____

_____ Miembro

_____ Miembro

_____ Miembro

_____ Miembro

_____ Presidente

Acta Nº: _____
Fecha: _____

DEDICATORIA

Esta Tesis va dedicada a Dios por haberme brindado fortaleza en innumerables situaciones en el trascurso de los años de mi carrera universitaria.

A mi familia, que en donde sea que se encuentren, sé que siempre estarán apoyándome para seguir adelante con mis metas.

A todos y cada uno de mis compañeros de la carrera, por ser buenos camaradas en las clases, y amigos en todo momento.

A todos y cada uno de mis profesores, por haberme compartido sus conocimientos y hacer que este trabajo sea posible.

A todos aquellos que promueven el desarrollo de software libre.

AGRADECIMIENTO

Antes que nada, primeramente, agradecerle a Dios, por saber conducirme tras complicadas situaciones en estos últimos años.

A mi madre por todo, absolutamente todo lo que me brindó.

A mis hermanos por el apoyo constante brindado.

A mis compañeros por estar acompañando aquellos días de clase.

A todos quienes contribuyeron a la conclusión de este trabajo.

DESARROLLO DE UN SISTEMA DE AUTENTICACIÓN GRÁFICO BASADO EN LA API DRAG&DROP DE HTML5 PARA AMBIENTE WEB

RESUMEN

En el presente trabajo, se planteó el diseño y desarrollo de un sistema de autenticación basado en imágenes y métodos de encriptación híbrida como elementos de la contraseña y los eventos del API HTML5 de Drag&Drop como alternativa en primer lugar a los esquemas de logueo seguro actualmente en el ambiente web.

Para llegar a dicho fin, se realizó una recopilación de los esquemas de autenticación gráficos desarrollados hasta la actualidad, además de métodos de autenticación seguros implementados por sitios web cuya información podría ser sensible o comprometedora, con esto último se efectuó una comparativa, destacando ventajas y desventajas en frente del esquema propuesto.

Además, se procedió a hacer una evaluación del sistema desarrollado dando como resultado según la investigación realizada un sistema de autenticación mucho más seguro ante la mayoría de formas de ataques de robo de contraseña, al mismo tiempo resulta en un proceso mas amigable de realizar por parte del usuario en comparación con otros esquemas de logueo seguro del mercado actual.

Sin embargo, una vez realizado un análisis de rendimiento del método desarrollado, se evidenció una carga tanto en el lado del servidor como del cliente, provocados por el esquema de encriptación utilizado y la carga simultanea de imágenes respectivamente, dicha carga puede ser considerable al compararla con el mismo procedimiento de logueo en sistemas convencional

de contraseñas a base de texto, además eventualmente se deberá tener en cuenta las capacidades del sistema propuesto en ámbitos de su accesibilidad.

Palabras claves: contraseña, ciberseguridad, internet, innovación, HTML, JavaScript, php, desarrollo web.

ABSTRACT

In the present work presented, is proposed the design and development of an authentication system based on images and hybrid encryption methods as components of a password and the use of the HTML5 API of Drag & Drop events, this as an alternative in the first place to the secure login schemes currently in the web environment

To achieve this goal, a compilation of the graphic authentication schemes developed to date is made, in addition to secure authentication methods implemented by websites whose information could be sensitive or compromising, with the latter a comparison is made, highlighting advantages and disadvantages in front of the scheme to propose.

In addition, an evaluation of the system developed was carried out, resulting in a much more secure authentication system based on the research carried out in the face of most forms of password theft attacks, at the same time resulting in a more user-friendly process, compared to other secure login schemes of the current market.

However, once a performance analysis of the developed method was performed, a load was evidenced in both sides, on the server side and the client one, caused by the encryption scheme used and the simultaneous loading of images, respectively. This load is considerable when compared with the same procedure of authentication in conventional systems of passwords based on text, in addition eventually it should be taken into account the capabilities of the proposed system of its accessibility.

Key words: password, cybersecurity, internet, innovation, html, JavaScript, php, web development.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad se puede observar un gran y creciente vinculo de los usuarios con la tecnología en lo que respecta a medios de comunicación e información digitales, día a día cada persona pone mas y mas información personal en la web, por otra parte, las empresas que prestan el servicio tienen la importante tarea de salvaguardar esta información.

Para los efectos, son desarrollados diferentes mecanismos de seguridad, entre los que podemos destacar sistemas de autenticación, sistemas de comprobación de usuarios humanos, esquemas de encriptación sofisticados y muchos otros mas, a pesar de que todas estas tecnologías signifiquen un importante aporte a la seguridad de estos sistemas, se podría destacar el importante papel de los sistemas de autenticación ya que estos son le dan al usuario la propiedad por decirlo así de su información.

Este trabajo busca desarrollar, implementar y evaluar una nueva propuesta de Autenticación en el ambiente web, con el afán de poder dar a usuarios y empresas un sistema fácil de usar y a la vez seguro contra el mayor número de amenazas posible, de ahí en más es que se optó por un esquema basado en imágenes y en gestos del usuario por encima sistemas convencionales de tipeo de caracteres normalmente conocido.

Partiendo de esta premisa el presente Proyecto de Fin de Grado irá describiendo los procedimientos aplicados en la concreción del Sistema de Autenticación de la siguiente forma:

CAPÍTULO I

1. MARCO INTRODUCTORIO

1.1. PLANTEAMIENTO DEL PROBLEMA

Las contraseñas son las claves secretas del siglo XXI, actualmente son ampliamente utilizadas alrededor de todo el internet, ya que estas sirven como medios de autenticación de individuos, para su acceso a casi cualquier sistema de información, red social, o cuenta privada en línea. Su implementación en el área de las TICs actualmente abarca varias plataformas, como son entornos web, entornos de escritorio y dispositivos móviles, en donde su rol es el de proteger los datos e información del usuario.

Es justamente su rol protector y secreto el que les otorga a las contraseñas su gran vulnerabilidad, desde donde nacen las problemáticas de las contraseñas, esto hace que el robo de contraseñas sea una de las principales actividades de los atacantes informáticos de hoy en día, todo esto con el único objetivo de obtener estas claves secretas, de manera a que los atacantes puedan tener acceso a los datos e informaciones personales que las contraseñas protegen.

Muchas empresas del rubro de la Seguridad Informática buscan cada día manera de hacer de los procesos de autenticación mas seguros, en el caso especial de este proyecto, busca diseñar, desarrollar y poner a prueba un modulo de autenticación en donde en vez de realizar la digitación de la contraseña, el usuario tenga que “arrastrar” símbolos que representen su contraseña hasta una parte de la pantalla.

1.2. DELIMITACIÓN Y ALCANCE

Lo más importante para este proyecto es el desarrollo de un sistema de autenticación gráfica a base del API Drag&Drop de HTML5 e imágenes de conocimiento por parte de los usuarios para ambientes web.

Este esquema estará caracterizado por dos de los aspectos mas importantes para los sistemas de autenticación; los cuales son: la seguridad, y la facilidad de uso por parte del usuario. Lo cual dota al presente de un gran atractivo, ya que hoy en día aquellos sistemas de autenticación que implementan varios mecanismos de seguridad albergan una gran complejidad de uso, por otra parte, aquellos sistemas que podrían considerarse fáciles de usar son aquellos que menor seguridad.

Este método de autenticación podrá ayudar a aquellas empresas y/o particulares que deseen implementar en sus sitios web un sistema de autenticación fuera de lo convencional, fácil de usar y por sobre todas las cosas seguro para los usuarios.

1.3. PREGUNTA DE INVESTIGACIÓN

En los marcos de las observaciones anteriores se puede formular la siguiente pregunta: ¿Representa una mejora en la seguridad y experiencia de usuario la implementación de contraseñas gráficas en reemplazo de las convencionales?

1.4. OBJETIVOS

1.4.1. OBJETIVO GENERAL

- Desarrollar un Sistema de autenticación gráfico a base del API Drag&Drop de HTML5 e imágenes.

1.4.2. OBJETIVOS ESPECÍFICOS

- Verificar cuales son los sistemas de autenticación más utilizados en la actualidad para servicios en internet.
- Diseñar un esquema de recuerdo de imágenes considerando los principales requerimientos de seguridad de autenticación ante posibles formas de robo de contraseñas.
- Evaluar las características de rendimiento del método propuesto.

1.5. JUSTIFICACIÓN

La razón que motivó este proyecto fue el analizar los grandes problemas de los usuarios con las contraseñas: frecuentemente olvidadas y en algunos casos robadas, y precisamente el aporte del módulo propuesto en el presente trabajo se enfoca a solucionar esas grandes falencias, es decir, apunta a hacer que las contraseñas sean más fáciles de recordar para los usuarios y a la vez hacer más seguro el sistema de autenticación ante las diferentes modalidades de ataques y robos de contraseñas.

Debido a que el proyecto involucraría a toda persona (entiéndase usuario) que tenga una cuenta de usuario en alguna red social, sistema de correo, Banca Web, u otro tipo de sitio en la red que maneje informaciones sensibles de los usuarios, es que el alcance abarcaría a prácticamente más de la mitad de los cibernautas de la actualidad.

CAPÍTULO II

2. MARCO TEÓRICO, CONCEPTUAL, OPERACIONAL Y LEGAL

2.1. ANTECEDENTES

Desde la aparición de los sistemas de información en internet y entornos web cada vez más dinámicos, a la par, desde 1999, se han venido proponiendo una gran cantidad de métodos de autenticación gráfica propulsados por la idea de que la memorización de las contraseñas mejoría y, por ende, la usabilidad, al mismo tiempo de mejorar la resistencia del sistema contra los ataques de fuerza bruta y la posibilidad de que alguien 'adivine' la contraseñas. Al igual que las contraseñas a base de caracteres, las contraseñas gráficas son métodos de autenticación basados en el conocimiento, en los que los usuarios introducen un secreto compartido como evidencia de su identidad [1].

A pesar del gran número de opciones de autenticación, las contraseñas de texto siguen siendo la opción más común por muchas razones [2]. Son fáciles y de bajo costo de implementar, son familiares para la mayor parte de los usuBarios, permiten a los usuarios autenticarse mientras evitan los problemas de privacidad que se han planteado acerca de la Biometría, y tienen la ventaja de portabilidad sin, por ejemplo, tener la necesidad de tener que portar tokens físicos .

A simple lógica idea detrás de las contraseñas gráficas era aprovechar la memoria humana para obtener información visual, con el secreto compartido (contraseña) relacionado o compuesto de imágenes, esto contrasta con las contraseñas a base de texto que incluyen caracteres de teclado alfanuméricos y/o especiales [1].

Lo dicho anteriormente con respecto a la característica de las contraseñas gráficas de poder ser mejor recordadas que cadenas de caracteres, se basa en varios estudios anteriores, como el de Kirkpatrick que sostiene que el cerebro humano puede reconocer y recordar mucho mejor la información visual en oposición a la información verbal o textual, o la teoría más aceptada es la teoría de codificación dual de Paivio, que sugiere que la memoria verbal y no verbal (respectivamente, basada en palabras y basada en imágenes) son procesadas y representadas de manera diferente en la mente. Las imágenes se representan mentalmente de una manera que conserva las características perceptivas que se observan y se les asigna un significado percibido sobre la base de lo que se está observando directamente [1].

Como dijo Raaijmakers las tareas que involucran la memoria visual también pueden variar en dificultad debido a las características particulares del proceso de recuperación. Las contraseñas gráficas pueden clasificarse ampliamente de acuerdo con la tarea de memoria que implica recordar e introducir la contraseña: recuperación, reconocimiento y recuento de indicadores. Además de su facilidad de recordación, las contraseñas gráficas poseen otro aspecto a considerar, su seguridad de uso. Un sistema de autenticación debe proporcionar una seguridad adecuada para su entorno de implementación; de lo contrario, no cumple su objetivo principal. Un sistema propuesto debería evaluarse como mínimo contra ataques comunes para determinar si satisface los requisitos de seguridad [1].

A menudo la codificación desempeña un papel importante relacionado con la seguridad, es decir, permitir la transformación de la entrada del usuario en unidades discretas que pueden ser identificadas por el sistema y utilizadas

para comparación durante la reentrada de contraseña. Como se verá, algunos esquemas requieren que el sistema conserve el conocimiento del secreto exacto (o parte de este), ya sea para mostrar el conjunto correcto de imágenes al usuario o para verificar las entradas de contraseña. En otros casos, las contraseñas codificadas o discretizadas pueden ser hash, utilizando un hash criptográfico unidireccional para proporcionar seguridad adicional en caso de que la contraseña esté comprometida.

Se clasificaran algunos de los métodos de autenticación gráfica ya desarrollados en tres categorías principales, estos basados en el recuerdo, el reconocimiento y el recuerdo con pistas [1].

Los sistemas de contraseñas gráficas basados en el recuerdo se denominan ocasionalmente sistemas Drawmetric [2], porque los usuarios recuerdan y reproducen un dibujo secreto. En estos sistemas, los usuarios típicamente dibujan su contraseña en un lienzo en blanco o en una cuadrícula [2].

Los sistemas basados en el reconocimiento, también conocidos como sistemas cognométricos o los sistemas de búsqueda de datos, por lo general requieren que los usuarios memoricen una cartera de imágenes durante la creación de la contraseña y luego deben reconocer sus imágenes entre señuelos para iniciar sesión [1].

Los sistemas de recuperación de memoria suelen requerir que los usuarios recuerden y apunten ubicaciones específicas dentro de una imagen. Esta característica, destinada a reducir la carga de memoria en los usuarios, es una tarea de memoria más fácil que el recuerdo puro. Tales sistemas también

se llaman locimetric, ya que se basan en la identificación de ubicaciones específicas. Esta tarea de memoria difiere de simplemente reconocer una imagen como un todo. Hollingworth y Henderson muestran que la gente conserva recuerdos visuales precisos y detallados de los objetos a los que previamente asistieron en escenas visuales; Esto sugiere que los usuarios pueden ser capaces de recordar con precisión partes específicas de una imagen como su contraseña si inicialmente se centraron en ellos. En un diseño ideal, la señal en un sistema de autenticación es útil sólo para los usuarios legítimos (no para los atacantes que tratan de adivinar una contraseña) [1].

2.2. BASES TEÓRICAS

2.2.1. CONOCIMIENTOS ASOCIADOS A LAS CONTRASEÑAS Y SU ÁMBITO DE IMPLEMENTACIÓN

En pocas palabras las contraseñas son como las llaves de acceso de los usuarios a sus informaciones almacenadas en la web que dan fe de que estos son quienes dicen que son, a lo largo del desarrollo de la internet, cada vez se fueron sumando mas y mas usuarios a esta red, tanto es asi que la internet es hoy en día (y ya lo ha venido siendo) un lugar donde pueden llevarse varios delitos, es por eso que, mantener mecanismos de seguridad en las contraseñas es crucial en sistemas donde la información sea sensible o afecte el patrimonio de los usuarios. Pero son estos mecanismos los que en muchos casos afectas la usabilidad de los sistemas de autenticación, solicitándole a los usuarios la confección y por ende recuerdo de contraseñas extensas, con caracteres especiales de poco uso por parte del usuario y el uso de mayúsculas.

En pocas palabras mientras mas seguros son los sistemas de autenticación de usuario mas se encarece la usabilidad de estos, lo cual afecta indefectiblemente a la comodidad del usuario, un problema mas grave sería una falta total de los mismos mecanismos de seguridad, por ende, desarrollar sistemas de autenticación seguros y fáciles de usar para los usuarios es un desafío contemporáneo necesario de sobrepasar si se desea un mayor uso de los sistemas de información, redes sociales, etc.

2.2.1.1. LAS CONTRASEÑAS EN REDES SOCIALES Y CORREOS ELECTRÓNICOS

Las contraseñas en redes sociales y sistemas de correo electrónico protegen algo mas que solo información sensible del usuario, protegen la identidad de este, normalmente la mayor parte de las redes sociales como Facebook, Twitter, Instagram no tienen una particular exigencia en la confección de las contraseñas de sus usuarios, además de solicitarle un mínimo de 6 caracteres [3], en sistemas de correo electrónico el esquema exigido es algo parecido, con la diferencia de la implementación de sistemas de apoyos a los procesos de autenticación.

2.2.1.2. LAS CONTRASEÑAS EN EL E-COMMERCE

Los sitios de E-Commerce albergan algo tanto mas delicado que información personal, estos sitios albergan números de tarjetas de créditos y direcciones de sus clientes, es por eso por lo que implementas ciertas políticas en lo que respecta a las contraseñas de sus usuarios. Sitios como amazon.com exigen un mínimo de 6 caracteres, combinando mayúsculas y minúsculas, o ebay.com que además de lo que, comentado, exigen tener al menos un número y un símbolo [3].

2.2.1.3. LAS CONTRASEÑAS EN BANCAS WEB

La mayoría de los Bancos, por no decir la totalidad de ellos, dan a sus clientes la facilidad de la Banca Web, la cual da al cliente la posibilidad de monitorear sus movimientos financieros y realizar una gran variedad de gestiones bancarias desde la comodidad de su hogar, sin ningún otro elemento que una computadora y un acceso a internet.

Esto es en esencia una gran ventaja para los clientes, pero al mismo tiempo una gran oportunidad para que avivados atacantes informáticos puedan tener acceso a su cuenta bancario mediante el robo de su contraseña, razón

por la cual, estas entidades financieras se toman el rol protector de las contraseñas muy seriamente, es asi que muchas bancas web implementan teclados virtuales para prevenir la capturas de las contraseñas mediante los malwares conocidos como keyloggers, o el uso de las contraseñas junto con el de tokens físicos.

2.2.1.4. LAS CONTRASEÑAS EN DISPOSITIVOS MOVILES

En el ámbito de las contraseñas y métodos de autenticación, los dispositivos móviles son unos de los mas dinámicos, día a día las empresas fabricantes buscar innovar cada vez mas con el fin de ofrecer a sus clientes dispositivos mas inteligentes, y si, más seguros.

Es de esa manera que con el pasar de los años hemos visto como dispositivos móviles iban implementando sistemas de autenticación a base de PINs, inclusive un tipo de contraseña gráfica que llegó a ser uno de los mas utilizados hasta la actualidad, el cual es el sistema de autenticación basado en Patrones, implementado por dispositivos Android, y no hay que olvidar el uso de la biometría como método de autenticación en estos dispositivos, con los dispositivos Apple usando las huellas dactilares o el reconocimiento facial.

2.3. ASPECTOS LEGALES

Los aspectos legales de este proyecto solo involucran los de la licencia utilizada que rige el código y derechos de uso de este, dejando claro que el que suscribe el presente trabajo es el creador de método a ser expuesto, otorgándole a este todos los derechos de autoría. La licencia utilizada es la MIT Lisence.

2.3.1. LICENCIA MIT

Una licencia permisiva corta y simple con condiciones que solo requieren la preservación de los avisos de derechos de autor y licencia. Las obras con licencia, las modificaciones y las obras más grandes pueden distribuirse bajo diferentes términos y sin código fuente [4].

Licencia MIT

Copyright (c) 2018 crisDuarte.

Por la presente, se otorga el permiso, sin cargo, a cualquier persona que obtenga una copia de este software y los archivos de documentación asociados (el "Software"), para operar el Software sin restricciones, incluidos, entre otros, los derechos de uso, copia, modificación, fusión. , publicar, distribuir, sublicenciar y / o vender copias del Software, y para permitir que las personas a quienes se suministra el Software lo hagan, sujeto a las siguientes condiciones:

El aviso de copyright anterior y este aviso de permiso se incluirán en todas las Copias o partes sustanciales del Software.

EL SOFTWARE SE PROPORCIONA "TAL CUAL", SIN GARANTÍA DE NINGÚN TIPO, EXPRESO O IMPLÍCITO, INCLUYENDO PERO NO LIMITADO A LAS GARANTÍAS DE COMERCIABILIDAD, IDONEIDAD PARA UN PROPÓSITO PARTICULAR Y NO INCUMPLIMIENTO. EN NINGÚN CASO, LOS AUTORES O TITULARES DE DERECHOS DE AUTOR SERÁN RESPONSABLES POR CUALQUIER RECLAMACIÓN, DAÑOS U OTRAS RESPONSABILIDADES, YA QUE SEA RESPONSABLE DE UN CONTRATO, CORTE U OTRA MANERA, DERIVADOS DE, FUERA O EN CONEXIÓN CON EL SOFTWARE O EL USO U OTRAS REPARACIONES EN EL SOFTWARE [4].

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. TIPO DE INVESTIGACIÓN

Esta investigación se apoya en el enfoque cuali-cuantitativo de manera a poder interpretar los requerimiento de sistemas de autenticación que cumplan con las exigencias de seguridad y facilidad de uso, también este enfoque ayudará a la interpretación de datos numéricos obtenidos del uso del sistema de autenticación consistentes en tiempos y número de eventos, además de poder interpretar lo expresado por las personas sujeto de experimento piloto, como también conductas o sucesos ocurridos durante el experimento. En referencia a esto es pertinente mencionar que El enfoque que el investigador piense que armoniza o se adapta más a su planteamiento del problema. En este sentido, es importante recordar que aquellos problemas que necesitan establecer tendencias se acomodan mejor a un diseño cuantitativo; y los que requieren ser explorados para obtener un entendimiento profundo, empatan más con un diseño cualitativo. Asimismo, cuando el problema o fenómeno es complejo, los métodos mixtos pueden ser la respuesta [5]

3.2. DISEÑO DE INVESTIGACIÓN

La mayor parte del tiempo dedicado a este trabajo fue para desarrollar el sistema basado en imágenes usando la API Drag&Drop, y a definir el esquema de encriptación a utilizar en las contraseñas. Además, una vez terminado el prototipo se llevó a cabo una prueba con un grupo de muestra para probar dicho prototipo.

En función de los objetivos definidos en el presente Proyecto Final de Grado, donde se llevó a cabo el Desarrollo de un Sistema de Autenticación basado en Drag&Drop para ambiente web, para lo cual se emplearon una serie

de técnicas de recolección de datos, orientadas de manera esencial a alcanzar los fines propuestos. Las técnicas de recolección de información que se utilizaron en la investigación se describen a continuación:

Prueba Piloto: Esta técnica se utilizó para conocer y analizar el comportamiento del usuario una vez confrontado con la poca usual experiencia de crear y utilizar una contraseña gráfica, y compararlo con un sistema de autenticación convencional a base de caracteres con las exigencias normales.

Observación Directa: Esta técnica se utilizó para observar características adicionales del sistema de autenticación gráfica propuesto que pudieren redituarle o fortalezas o debilidades. Tener en cuenta es que la observación directa es en el cual el investigador puede observar y recoger datos mediante su propia observación [6].

Entrevista: Esta técnica se utilizó con el fin de recabar las impresiones finales del usuario con respecto a su experiencia en los procesos de experimentación a los cuales se vió sometido con el sistema de autenticación gráfico propuesto. Con respecto a eso la entrevista se puede definir como una comunicación interpersonal a través de una conversación estructurada que configura una relación dinámica y comprensiva desarrollada en un clima de confianza y aceptación, con la finalidad de informar y orientar [7].

3.3. POBLACIÓN Y MUESTRA

La población que se tomó para el estudio de este proyecto de fin de grado es la Universidad Nacional de Caaguazú, tanto alumnos como docentes, considerados heterogéneos en cuanto a sus habilidades con el uso de cuentas de usuario y procesos de autenticación. Según Lepkowski una población es el

conjunto de todos los casos que concuerdan con una serie de especificaciones [5].

Mientras en cuanto a muestra se refiera escogimos a algunos alumnos y docentes, siendo la técnica utilizada la muestra no probabilística, con una cantidad total de 52 individuos, con géneros y edades totalmente aleatorios.

3.4. MÉTODO, TÉCNICAS Y PROCEDIMIENTOS

3.4.1. METODOLOGÍAS PARA EL DESARROLLO DEL SISTEMA

3.4.1.1. SCRUM

Scrum es un proceso en el que se aplican de manera regular un conjunto de buenas prácticas para trabajar colaborativamente, en equipo, y obtener el mejor resultado posible de un proyecto. Estas prácticas se apoyan unas a otras y su selección tiene origen en un estudio de la manera de trabajar de equipos altamente productivos [3].

En Scrum se realizan entregas parciales y regulares del producto final, priorizadas por el beneficio que aportan al receptor del proyecto. Por ello, Scrum está especialmente indicado para proyectos en entornos complejos, donde se necesita obtener resultados pronto, donde los requisitos son cambiantes o poco definidos, donde la innovación, la competitividad, la flexibilidad y la productividad son fundamentales [8].

Scrum también se utiliza para resolver situaciones en que no se está entregando al cliente lo que necesita, cuando las entregas se alargan demasiado, los costes se disparan o la calidad no es aceptable, cuando se necesita capacidad de reacción ante la competencia, cuando la moral de los equipos es baja y la rotación alta, cuando es necesario identificar y solucionar

ineficiencias sistemáticamente o cuando se quiere trabajar utilizando un proceso especializado en el desarrollo de producto [8].

CAPÍTULO IV

4. MARCO ANALÍTICO

4.1. REQUERIMIENTOS

4.1.1. REQUERIMIENTO FUNCIONAL

Sistema de Autenticación Gráfico basado en Drag&Drop para ambiente web podrá:

- Dar al usuario guías de cómo utilizar el mecanismo.
- Implementar mecanismos que fortalezcan la seguridad de sistema frente a las posibles formas de ataque.
- Implementar mecanismos de encriptación.
- Mantener su condición de user-friendly a la par que las mejoras se vayan implementando.
- Ser escalable en el tiempo.
- Poder ser aplicable en los entornos web donde se requiera la autenticación de personas.
- Ser eficiente.
- Usar imágenes de uso común por parte del usuario

4.1.2. REQUERIMIENTO NO FUNCIONAL

- Establecer mecanismos de recuperación de contraseña.
- Exigir el cambio de la contraseña pasado intervalos de tiempo.

4.2. ESTUDIO DE FACTIBILIDAD

La factibilidad se refiere a la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas, es decir, si es posible cumplir con las metas que se tienen en un proyecto, tomando en cuenta los recursos con los que se cuenta para su realización.

En esta sección se detallaran los estudios de factibilidad realizados al proyecto para determinar la viabilidad de la implementación del método de autenticación propuesto en sistemas que involucran manejo de cuentas de usuarios. Los resultados de estos estudios dictaminarán las implicancias de dicha implementación.

4.2.1. FACTIBILIDAD TÉCNICA

El analista debe averiguar si posible actualizar o incrementar los recursos técnicos actuales de tal manera que satisfagan los requerimientos bajo consideración. Sin embargo en ocasiones los agregados a los sistemas existentes son muy costosos y no redituables, simplemente porque no cumplen las necesidades con eficiencia. Si no es posible actualizar los sistemas existentes, la siguiente pregunta es si hay tecnología disponible que cumpla las especificaciones [9].

Lenguaje y Herramientas utilizadas para el desarrollo

Como se mencionó en el marco teórico y como lo evoca el titulo de este trabajo, el proyecto es destinado al ambiente web, por ende, se requieren aquellos lenguajes y herramientas para el desarrollo en este, los cuales incluyen: HTML5 como lenguaje de marcado y diseño de la interfaz, CSS utilizado para añadir estilismo a la interfaz, como también Javascript como lenguaje manipulador de los datos en el lado del cliente, y finalmente Php como

lenguaje manipular de los datos en el lado de servidor y como nexo con el motor de base de datos utilizados.

Como también se puede mencionar la utilización de un editor de texto como herramienta para el desarrollo en los lenguajes mencionados, y a manera de poder visualizar el trabajo realizado, también se puede mencionar al Software Apache Server.

Herramientas utilizadas para la implementación

En el caso de realizar una implementación se debe tener en cuenta de disponer de un servidor con las suficientes características, tanto procesador, memoria RAM como también el servicio de red que lo conecta con los clientes, acordes al trabajo a realizar, que incluyen procesos de encriptación y carga de imágenes de tamaño mayor a lo normal.

4.2.2. FACTIBILIDAD OPERATIVA

La viabilidad operativa depende de los recursos humanos disponibles para el proyecto e implica determinar si el sistema funcionará y será utilizado una vez que se instale. Si los usuarios están contentos con el sistema actual, no tienen problemas con su manejo y por lo general no están involucrados en la solicitud de un nuevo sistema. La determinación de la viabilidad operativa requiere creatividad por parte del analista de sistemas, así como de su capacidad de persuasión para indicarle a los usuarios cuáles son las probables interfaces y cuáles satisfarán sus necesidades. El analista de sistemas también debe escuchar con atención lo que realmente quieren los usuarios y lo que al parecer utilizarán [9].

En cuanto al proyecto, al ser este un método de autenticación poco convencional a lo normal, muchos usuarios se pueden ver acomplejados en la

utilización del mismo, puede esperarse un nivel alto de rechazo, posibles fallos en procesos de autenticación en las primeras oportunidades, como también puede esperarse la necesidad de periodos de adaptación al método propuesto.

4.3. ANÁLISIS

4.3.1. ESCENARIO DE USUARIO

Normalmente en cada proceso de autenticación convencional (a base de texto o caracteres) se le es solicitado al usuario el ingreso de un nombre de usuario o correo electrónico y una contraseña, esto para cada servicio al cual el usuario quiera acceder y al cual este previamente registrado (ya sea alguna red social, correo electrónico, servicio e-commerce etc.).

Este proceso usualmente se lleva a cabo desde una computadora, o un dispositivo móvil, con la salvedad que en el dispositivo móvil normalmente el proceso de autenticación se realiza con mucha menor frecuencia ya que las aplicaciones almacenan los datos del usuario.

Finalmente es de resaltar que, en ambos casos, tanto en una computadora como en un dispositivo móvil, estos son casi en igual medida susceptibles a diferentes tipos de robos de contraseñas, y que en la mayoría de los casos el usuario es quien mantiene un mal hábito para con sus contraseñas.

4.4. DISEÑO

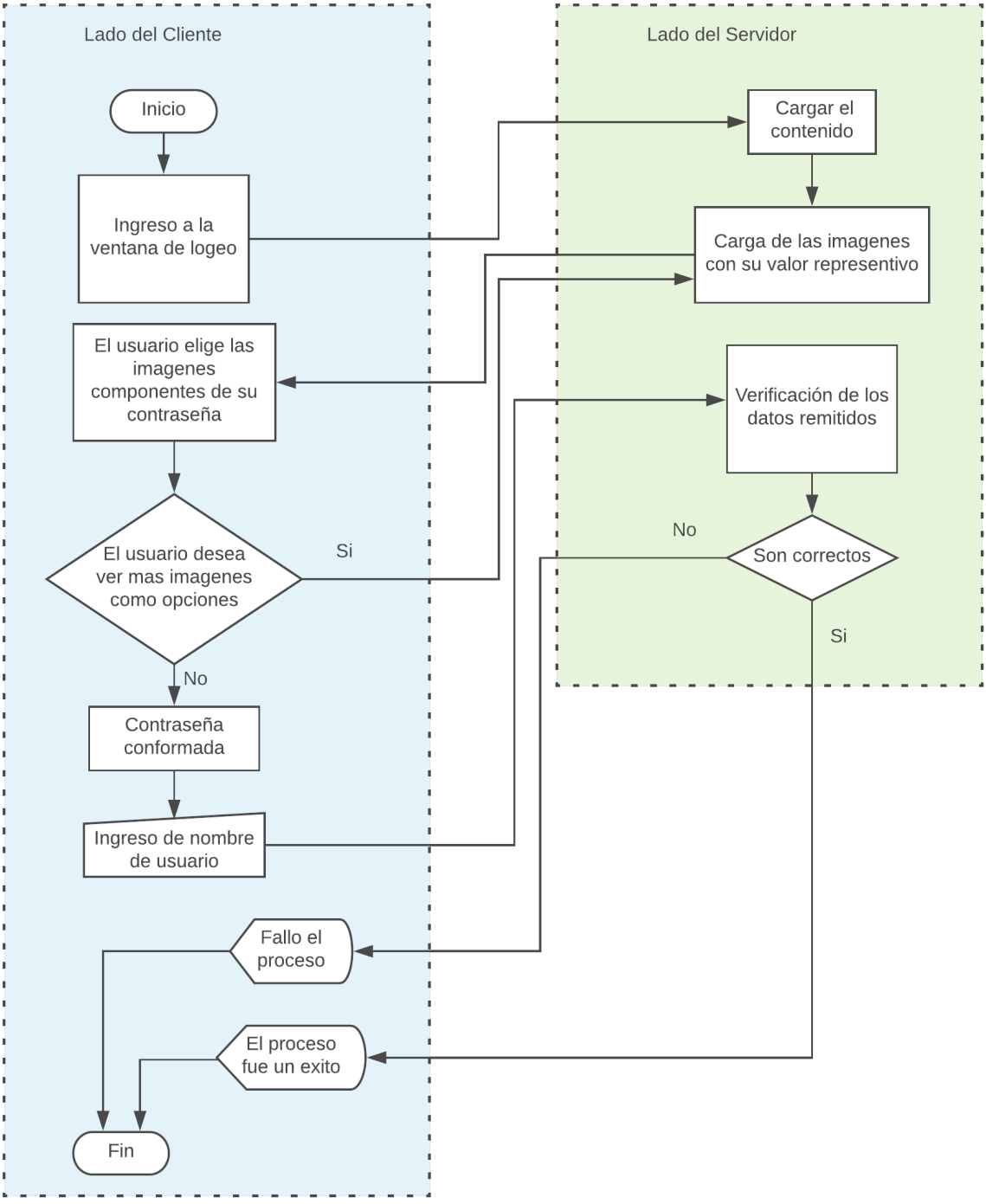


Figura 1: Diagrama General de Sistema de Logueo con Drag&Drop e Imágenes

4.5. CODIFICACIÓN

Una vez esquematizado el accionar básico del sistema de autenticación gráfica se procede su codificación, como el mismo estará en el ambiente web se optó por utilizar la herramienta Sublime Text como editor de código, ya que el mismo tiene grandes bondades como la facilidad de uso y muchas herramientas de apoyo en la codificación.

Al ser el ambiente web el ámbito de desarrollo de este proyecto, se podría dividir la correspondiente codificación en: Lado del Cliente (Front-end) en el cual se codificó la interfaz de usuario y que será la encargada de interactuar con el cliente, y lado del servidor (Back-end) el cual será responsable de la comunicación entre el cliente y el servidor, asi como también manejar procesos de encriptación.

4.5.1. BACKEND

PHP: (acrónimo recursivo de PHP: Hypertext Preprocessor) es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML. Lo que distingue a PHP de algo del lado del cliente como Javascript es que el código es ejecutado en el servidor, generando HTML y enviándolo al cliente. El cliente recibirá el resultado de ejecutar el script, aunque no se sabrá el código subyacente que era. El servidor web puede ser configurado incluso para que procese todos los ficheros HTML con PHP, por lo que no hay manera de que los usuarios puedan saber qué se tiene debajo de la manga. Lo mejor de utilizar PHP es su extrema simplicidad para el principiante, pero a su vez ofrece muchas características avanzadas para los programadores profesionales [10].

4.5.1.1. SISTEMA DE ENCRIPTACIÓN

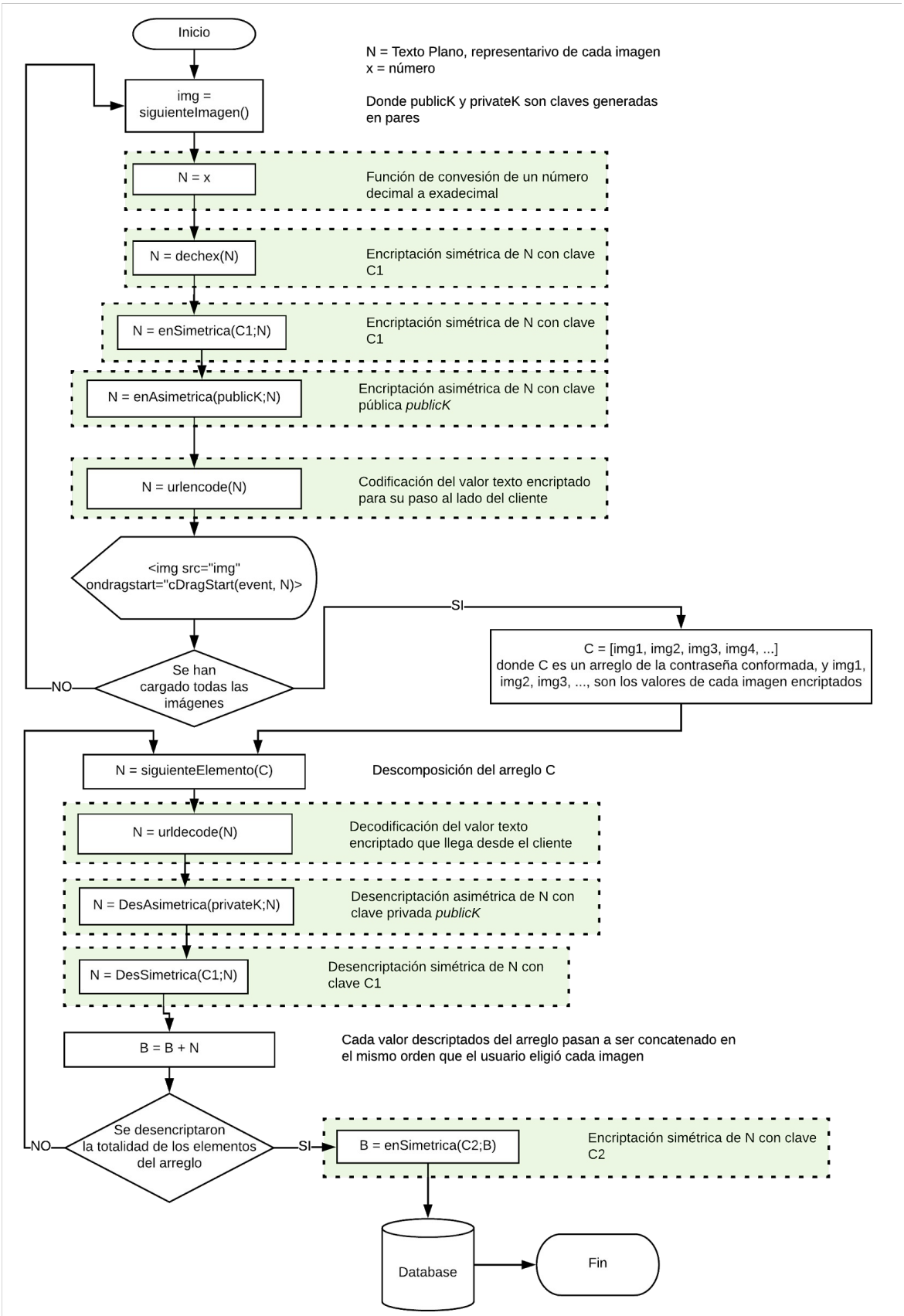


Figura 2: Diagrama del esquema de encriptación implementado

4.5.1.2. ENCRIPTACIÓN DE VALORES REPRESENTATIVOS DE LAS IMÁGENES

A la hora de hablar del desarrollo de contraseñas gráficas se le hace complicado a programar común definir la forma de como representar esta en la base de datos. En el caso de la utilización de imágenes como elementos componentes de la contraseña representa un desafío significa un gran desafío para desarrollar un mecanismo eficaz de guardar la serie de imágenes que un usuario elige, para luego cotejarlo en un posterior proceso de logueo.

En el caso del proyecto propuesto se asignaron valores numéricos hexadecimales elegidos al azar a cada imagen, pero estos no son mostrados a simple vista en el sitio del lado cliente, sino que antes el valor numérico (de cada imagen) es sometido a un proceso de encriptación, en el cual primeramente este valor es cifrado con un algoritmo de encriptación simétrico, y seguidamente se aplica una encriptación asimétrica o de clave pública, finalmente el texto encriptado es sometido a una codificación para que los caracteres generados en el proceso de encriptación no interfiera con el código del frontend, y es el resultado de esta codificación el valor representativo de cada imagen en el lado del cliente.

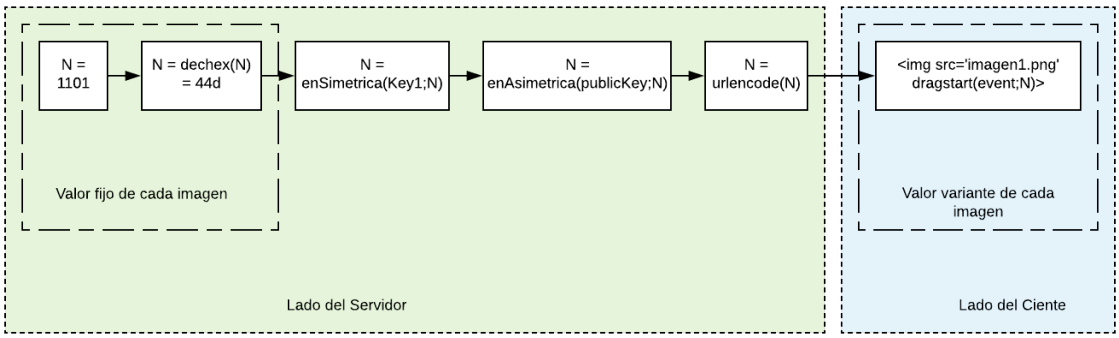


Figura 3: Diagrama simplificado del esquema de encriptación

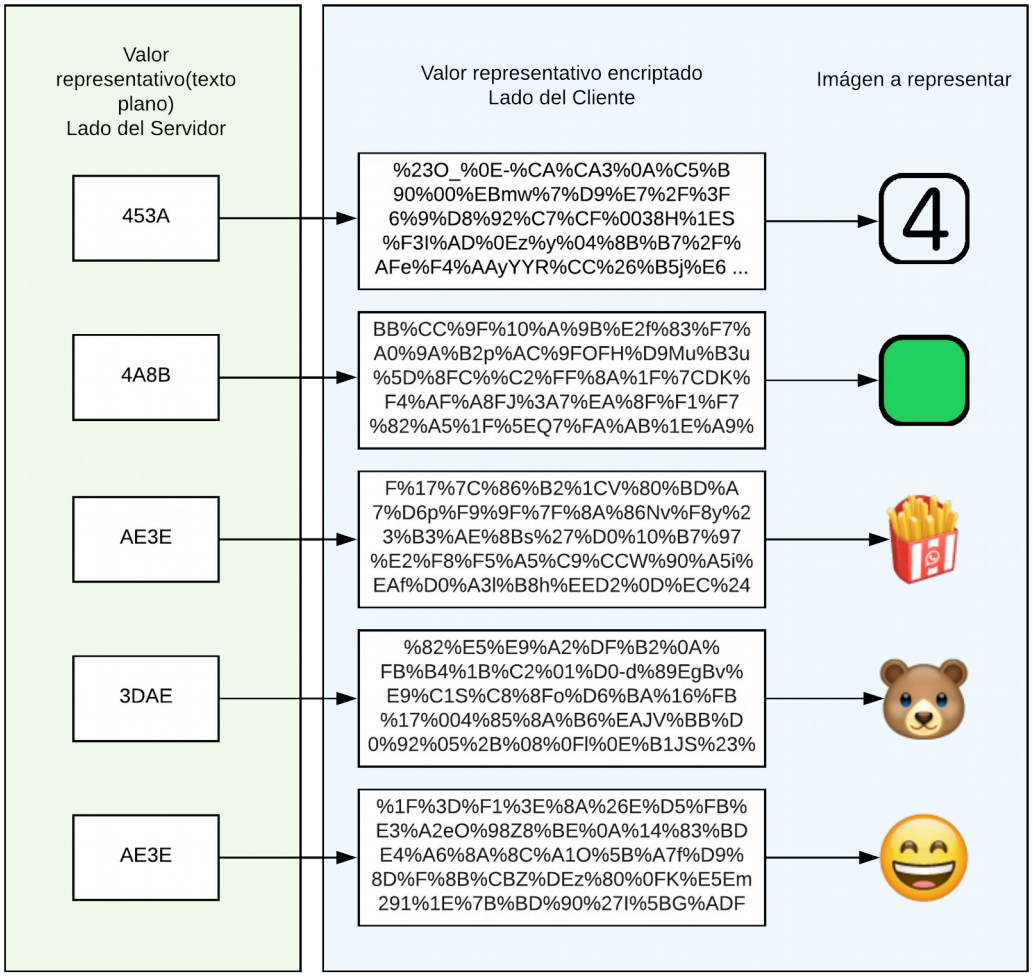


Figura 4: Diagrama valor real – valor encriptado

Finalmente, alguien que se dispusiera a ver el código de la página cargada no tendría del texto escondido tras la encriptación.

Figura 5: resultado de la implementación de la encriptación

4.5.1.2.1. ENCRIPTACIÓN Y DESENCRIPTACIÓN HÍBRIDA

En el ámbito de la criptografía, al hablar de una encriptación hibrida lo podemos considerar como un método de cifrado que emplea varios cifrados uno tras otro para así para el que el texto cifrado sea más difícil de descifrar.

De esta forma este proyecto utiliza un esquema de encriptación híbrido en el cual, a un texto plano pasa por dos procesos de encriptación, primeramente, una encriptación simétrica con una clave, luego una encriptación asimétrica o de clave pública.

4.5.1.2.1.1. ENCRIPTACIÓN SIMÉTRICA:

El cifrado simétrico, también conocido como cifrado convencional o cifrado de una sola clave, fue el único tipo de cifrado en uso antes del desarrollo del cifrado de clave pública en la década de 1970. Sigue siendo, con mucho, el más utilizado de los dos tipos de cifrado [11].

4.5.1.2.1.1.1. MODELO DE ENCRIPTACIÓN SIMÉTRICA:

Texto plano: Este es el mensaje o datos legibles originales que se introducen en el algoritmo como entrada [11].

Algoritmo de cifrado: el algoritmo de cifrado realiza varias sustituciones y transformaciones en el texto plano [11].

Clave secreta: la clave secreta también se ingresa al algoritmo de cifrado. La clave es un valor independiente del texto simple y del algoritmo. El algoritmo producirá una salida diferente dependiendo de la clave específica que se use en ese momento. Las sustituciones y transformaciones exactas realizadas por el algoritmo dependen de la clave [5].

Texto cifrado: Este es el mensaje codificado producido como salida. Depende del texto plano y la clave secreta. Para un mensaje dado, dos claves diferentes producirán dos textos cifrados diferentes. El texto cifrado es un flujo de datos aparentemente aleatorio y, en su forma actual, es ininteligible [11].

Algoritmo de descifrado: este es esencialmente el algoritmo de cifrado ejecutado en sentido inverso. Toma el texto cifrado y la clave secreta y produce el texto plano original [11].

Hay dos requisitos para el uso seguro del cifrado convencional:

Necesitamos un algoritmo de cifrado fuerte, como mínimo, que el algoritmo fuera tal que un oponente que conozca el algoritmo y tenga acceso a uno o más textos cifrados no pueda descifrar el texto cifrado o descifrar la clave. Este requisito generalmente se establece en una forma más fuerte: el oponente no debe poder descifrar el texto cifrado o descubrir la clave, incluso si él o ella está en posesión de varios textos cifrados junto con el texto simple que produjo cada texto cifrado. Luego el remitente y el destinatario deben haber obtenido copias de la clave secreta de manera segura y deben mantener la clave a salvo. Si alguien puede descubrir la clave y conoce el algoritmo, se puede leer toda la comunicación que usa esta clave [11].

4.5.1.2.1.1.2. ENCRIPTACIÓN ASIMÉTRICA

La criptografía de clave pública proporciona una salida radical de todo lo que ha sucedido antes. Por un lado, los algoritmos de clave pública se basan en funciones matemáticas en lugar de en la sustitución y la permutación. Más importante aún, la criptografía de clave pública es asimétrica, involucrando el uso de dos claves separadas, en contraste con el cifrado simétrico, que usa

solo una clave. El uso de dos claves tiene profundas consecuencias en las áreas de confidencialidad, distribución de claves y autenticación [11].

Gran parte de la teoría de los criptosistemas de clave pública se basa en la teoría de los números. Los algoritmos asimétricos se basan en una clave para el cifrado y una clave diferente pero relacionada para el descifrado. Estos algoritmos tienen la siguiente característica importante, resulta computacionalmente imposible determinar la clave de descifrado dado solo el conocimiento del algoritmo criptográfico y la clave de cifrado [11].

4.5.1.2.1.1.3. MODELO DE ENCRIPTACIÓN ASIMÉTRICA

Este modelo es parecido a de la Encriptación, manteniendo un texto plano, un algoritmo de encriptación, un algoritmo de desencriptación y un texto cifrado, con la diferencia de que en el modelo asimétrico se tienen dos claves, denominadas clave pública y privada respectivamente, este es un par de claves que se han seleccionado de modo que, si una se usa para el cifrado, la otra se usa para el descifrado. Las transformaciones exactas realizadas por el algoritmo dependen de la clave pública o privada que se proporciona como entrada [11].

4.5.1.2.1.2. OPENSSL

OpenSSL es un kit de herramientas robusto, de grado comercial y con todas las funciones para los protocolos de Seguridad de la capa de transporte (TLS) y de Capa de sockets seguros (SSL). También es una biblioteca de criptografía de propósito general. OpenSSL tiene licencia del estilo Apache, lo que básicamente significa que es libre de obtener y usar la librería con fines comerciales y no comerciales, sujeto a algunas condiciones de licencia simples.

4.5.1.2.2. BENEFICIOS DE LAS ENCRIPTACIÓN HÍBRIDA

El esquema de cifrado híbrido (simétrico y asimétrico en conjunto) nos da la ventaja de no recaer en la confianza de una clave, sino que en este caso se utilizar tres claves. Además, se podría decir que ambos esquemas mantienen sus propias vulnerabilidades, al usarlas en conjunto lo que sucede es que se permite que cada una apoye a la otra. Finalmente, el beneficio mas atípico es que la encriptación asimétrica hace que el texto cifrado (por ende, el valor representativo del lado del cliente) cambie con cada nueva encriptación realizada, lo que ocasiona que a un atacante le sea imposible realizar un ataque de fuerza bruta asistido por código (una vez individualizado el valor representativo presentado en el lado del cliente).

4.5.2. FRONTEND

HTML5: HyperText Markup Language (HTML) es un lenguaje de programación. A diferencia de otros lenguajes, HTML no está compuesto por comandos o instrucciones sino por un conjunto de etiquetas que organizan y declaran el propósito del contenido del documento. En un sentido estricto, HTML es solo texto escrito en una sintaxis particular que un navegador puede entender e implementar. La idea detrás de la creación de este lenguaje era compartir a través de Internet no solo el texto incluido en el documento sino también su formato. La posibilidad de diferenciar partes importantes del contenido del documento abrió la puerta para la creación de la web tal como la conocemos hoy en día. HTML es el lenguaje que lo hizo posible [12].

JAVASCRIPT: es un lenguaje interpretado que puede ser utilizado para diversos propósitos, pero que había sido considerado hasta ahora como solo un complemento de HTML y CSS. Una de las innovaciones que ayudó a cambiar esta imagen fueron los nuevos motores de procesamiento

incorporados por las recientes versiones de los navegadores más populares. Estos motores fueron desarrollados para acelerar el procesamiento del código Javascript convirtiéndolo en código maquina y así alcanzar velocidades de ejecución similares a las aplicaciones de escritorio. Esta nueva capacidad ayudó al lenguaje a superar limitaciones previas y confirmarlo como la mejor opción de codificación para la web. Javascript necesita un ambiente donde ser ejecutado, pero gracias a los nuevos interpretes y motores de procesamiento como V8 de Google, se ha convertido en un lenguaje más poderoso e independiente. Desde ahora, puede ser ejecutado casi en cualquier parte y sus nuevas características lo han hecho responsable de la revolución de Internet en estos últimos años así como el surgimiento del nuevo mercado de dispositivos móviles [12].

CSS: es un lenguaje que trabaja junto a HTML para otorgar estilos visuales a los elementos del documento, como tamaño, color, fondos, bordes, etc. A pesar de que cada navegador asigna estilos por defecto a cada elemento HTML, esos estilos pueden no estar dentro de la visión del diseñador. En la mayoría de los casos, estos estilos se encuentran alejados de lo que queremos para nuestros sitios web. La mayoría de las veces, desarrolladores y diseñadores necesitan aplicar sus propios estilos para lograr mostrar en pantalla la apariencia y organización que desean [12].

4.5.2.1. API DRAG&DROP

Arrastrar y soltar elementos de un lado a otro es algo que acostumbramos a hacer todo el tiempo en aplicaciones de escritorio, pero anteriormente nunca se esperaba poder hacer el mismo procedimiento en la web. Esto no se debe a que las aplicaciones para la web sean diferentes, sino

más bien a que los desarrolladores no contaban con una tecnología estándar para ofrecer esta herramienta. Desde la introducción del API Drag and Drop insertada por HTML5, finalmente se tuvo la oportunidad de crear aplicaciones web que se comportarán exactamente como aplicaciones de escritorio [12].

En lo que concierne al API Drag&Drop de HTML5 se pueden distinguir dos tipos de elementos:

Elemento Fuente: es aquel elemento que será arrastrado por el usuario. Por defecto sólo las imágenes, enlaces y selecciones son Elementos Fuente o *Draggables* por defecto, en otros casos el elemento que se desea hacer elemento fuente se deberá especificar el atributo draggable="true" [13].

Elemento Objetivo: es aquel elemento en el que un responde a una parte de eventos especiales del api, como es el caso del evento dragEnter, que es activado cuando un elemento que está siendo arrastrado pasa encima de este.

Comportamiento por defecto: si se quiere programar por encima de estos eventos y haciendo uso del API es de tener en cuenta el comportamiento por defecto de estos, ya que por ejemplo elementos como imágenes o enlaces al no especificarse acciones concretas a realizar al dispararse los eventos, estos responderán con acciones no deseadas, ya que dependerán del comportamiento por defecto que les asigne el navegador que está abriendo el sitio

4.5.2.1.1. EVENTOS INVOLUCRADOS:

4.5.2.1.1.1. DISPARADOS POR EL ELEMENTO FUENTE:

dragstart: Este evento es disparado en el momento en que la operación de arrastrar y soltar comienza. Los datos asociados con el elemento fuente son declarados en el sistema en este momento [12].

drag: Este evento es similar al evento mousemove, excepto que es disparado durante una operación de arrastrar y soltar por el elemento fuente [12].

dragend: Cuando la operación de arrastrar es terminada, con éxito o no, este evento es disparado por el elemento fuente [12].

4.5.2.1.1.2. DISPARADOS POR EL ELEMENTO OBJETIVO

dragenter: Este evento es disparado cuando el puntero del ratón ingresa en el área de un posible elemento objetivo durante una operación de arrastre [12].

dragover: Este evento es similar al evento mouseover, excepto que es disparado durante una operación de arrastre por posibles elementos objetivo [12].

drop: Este evento es disparado cuando el elemento fuente es soltado sobre el objetivo [12].

dragleave: Este evento es disparado cuando el puntero del ratón abandona un elemento durante una operación de arrastre. Es usado junto con el evento dragenter para ayudar al usuario a identificar el elemento objetivo [12].

4.5.2.2. ALGORITMO APLICADO

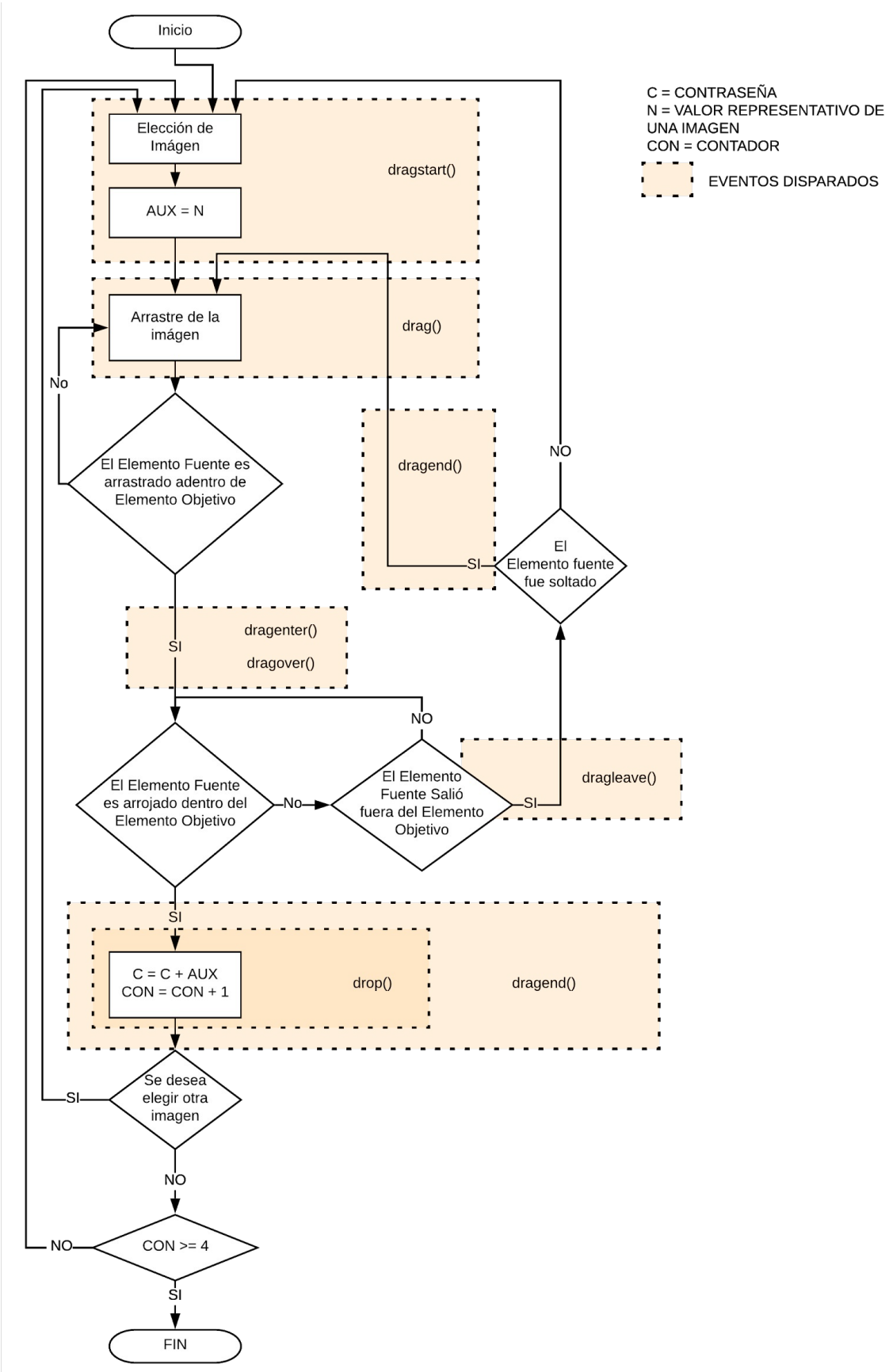


Figura 6: Diagrama del uso del API Drag&Drop en el proyecto

4.5.2.3. DISPOSITIVOS TÁCTILES

Se da el caso especial con aquellos dispositivos con interfaz de pantalla táctil (teléfonos inteligentes, tabletas etc.), ya que estos dispositivos no reconocen los eventos del API de Drag&Drop, ya que estos se disparan con el accionar del mouse, esto representa un gran problema para la idea de concebir un esquema de autenticación de usuarios gráfico utilizando la mencionada API, ya que, hoy en día usuarios ingresan indistintamente a los sitios web, redes sociales, correos electrónicos desde sus computadoras como desde sus dispositivos móviles (con pantallas táctiles). Según la investigación realizada en este trabajo, el 78% de los usuarios ingresó desde dispositivos móviles o tablets, y el 22% restante lo hizo desde una computadora.

A manera de lidiar con el inconveniente se utilizó el polyfill denominado DragDropTouch.js, él mismo traduce eventos touch en eventos estándar de arrastrar y soltar en HTML5. Al agregarse el polyfill a las páginas, las operaciones de arrastrar y soltar deberían funcionar en dispositivos móviles como lo hacen en el escritorio [14].

Diseño adaptativo con Bootstrap:

Teniendo en cuenta la necesidad de que la ventana de logueo pueda ser accedida por medio de dispositivos móviles, es indispensable tener en cuenta un diseño adaptativo, para esos efectos se tiene en cuenta el uso de la librería Bootstrap, de manera que el mismo sitio pueda adaptarse a diferentes configuraciones de pantalla y de dispositivos.

Bootstrap:

Bootstrap es un marco front-end gratuito para un desarrollo web más rápido y sencillo, incluye plantillas de diseño basadas en HTML y CSS para

tipografía, formularios, botones, tablas, navegación, modales, carruseles de imágenes y muchos otros, así como complementos opcionales de JavaScript, Bootstrap también te da la posibilidad de crear fácilmente diseños sensibles orientados a adaptarse a la pantalla donde se despliega [15].

Polyfill: Un polyfill, o polyfiller, es un fragmento de código (o complemento) que proporciona la tecnología que el desarrollador, espera que el navegador proporcione de forma nativa. Poly significa que podría resolverse utilizando cualquier número de técnicas; no se limita a solo hacerlo usando JavaScript, y fill, porque llenaría el agujero en el navegador donde la tecnología debía estar. Tampoco implica que el navegador sea antiguo (porque también se dan casos de utilización de polyfills en navegadores nuevos) [16].

Comportamiento del Polyfill DragDropTouch.js

El polyfill DragDropTouch adjunta escuchas a los eventos táctiles del documento:

En touchstart, verifica si el elemento objetivo tiene el atributo que se puede arrastrar o está contenido en un elemento que sí lo tiene. Si ese es el caso, guarda una referencia al elemento "arrastrar fuente" y evita el manejo predeterminado del evento.

En touchmove, verifica si el touch se ha movido una cierta distancia de umbral desde el origen. Si ese es el caso, levanta el evento dragstart y continúa monitoreando movimientos para disparar dragenter y dragleave.

En touchend, desactiva los eventos de Drag&Drop.

Para evitar interferir con la traducción automática del navegador de algunos eventos táctiles en eventos del mouse, el polyfill realiza algunas tareas adicionales:

Eleva los eventos mousemove, mousedown, mouseup y click cuando el usuario toca un elemento que se puede arrastrar, pero no comienza a arrastrar.

Desactiva el evento dblclick cuando haya un nuevo touchstart justo después de un clic, y desactiva el evento del menú contextual cuando el toque dura un tiempo, pero el usuario no comienza a arrastrar el elemento [14].

4.5.2.4. COMUNICACIÓN CON EL BACKEND

4.5.2.4.1. AJAX

La palabra AJAX es acrónimo de **A**synchronous **J**avaScript **A**nd **X**ML, no es un lenguaje de programación, sino que usa una combinación de: Un objeto llamado XMLHttpRequest integrado en el navegador (para solicitar datos de un servidor web), JavaScript y el DOM HTML (para mostrar o usar los datos), AJAX permite que las páginas web se actualicen de forma asíncrona mediante el intercambio de datos con un servidor web entre bastidores. Esto significa que es posible actualizar partes de una página web, sin volver a cargar toda la página [17].

4.5.2.4.1.1. DOM HTML

Cuando se carga una página web, el navegador crea un modelo de objeto de documento de la página. El DOM de HTML es un modelo de objeto estándar y una interfaz de programación para HTML. Define:

- Los elementos HTML como objetos.
- Las propiedades de todos los elementos HTML.
- Los métodos para acceder a todos los elementos HTML.
- Los eventos para todos los elementos HTML.

En otras palabras: el DOM de HTML es un estándar sobre cómo obtener, cambiar, agregar o eliminar elementos HTML.

Se construye como un árbol de Objetos: con el modelo de objetos, JavaScript obtiene todo el poder que necesita para crear HTML dinámico:

- JavaScript puede cambiar todos los elementos HTML en la página
- JavaScript puede cambiar todos los atributos HTML en la página
- JavaScript puede cambiar todos los estilos CSS en la página
- JavaScript puede eliminar elementos y atributos HTML existentes
- JavaScript puede agregar nuevos elementos y atributos HTML
- JavaScript puede reaccionar a todos los eventos HTML existentes en la página
- JavaScript puede crear nuevos eventos HTML en la página [18].

4.5.2.5. INTERFAZ GRÁFICA EN EL FRONTEND

Aplicando todas las bases teóricas de programación presentadas, se procedió al diseño de una interfaz sencilla pero completa de login, en la cual se le es solicitado al usuario un nombre de usuario o correo electrónico, y por su puesto su contraseña; para los efectos se agregan elementos fuentes (estos serías las imágenes) y un elemento objetivo representado por una caja de bordes punteados hasta donde el usuario, haciendo uso del API Drag&Drop, debe literalmente arrastrando las imágenes en el orden en el que desea que se establezca su contraseña, también se agregaron botones que permiten al usuario visualizar más imágenes como opciones, ya que estas se encuentran agrupadas bajo un criterio de semejanza entre cada una. De igual manera se dispone de un botón que permite al usuario corregir la contraseña en el caso de ser necesario, y a manera de asistir al usuario en el caso de tener dificultades en la utilización del sistema se incluye un botón de ayuda.

Figura 7: Interfaz de logueo gráfica Drag&Drop para Desktops, con imágenes alusivas a números

En la imagen anterior se puede visualizar una captura de pantalla de la interfaz de usuario, en este caso, con opciones de imágenes que representan números. Como se mencionó con anterioridad, el usuario tiene la posibilidad de elegir de otras gamas de imágenes, esto haciendo click en los botones amarillos de los lados.

Como por ejemplo, la siguiente captura muestra el uso de gamas de imágenes que se asemejan a emojis normalmente utilizados por los usuarios.

Figura 8: Interfaz de logueo gráfica Drag&Drop para Desktops, con imágenes alusivas a emoji con emociones

O por ejemplo en lugar de emojis, el usuario podría elegir de entre imágenes que representen colores:

Figura 9: Interfaz de logueo gráfica Drag&Drop para Desktops, con imágenes alusivas colores

Mientras que en dispositivos móviles se mantiene el mismo diseño de interfaz, con la misma gama de imágenes.

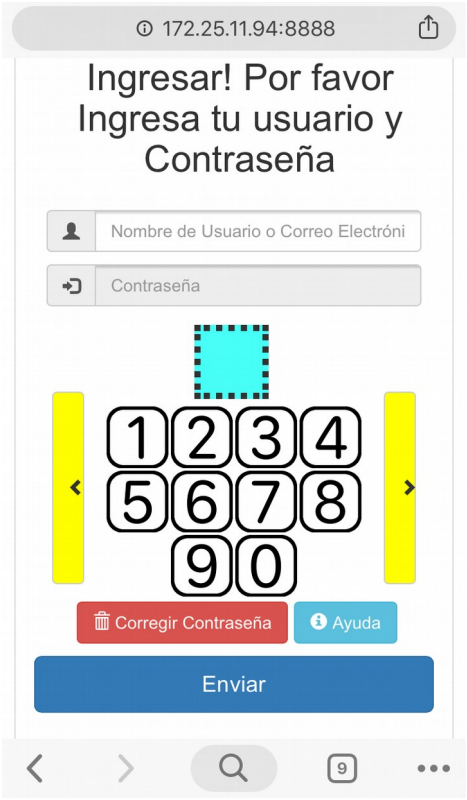


Figura 10: Interfaz de logueo gráfica Drag&Drop para móviles, con imágenes alusivas a números

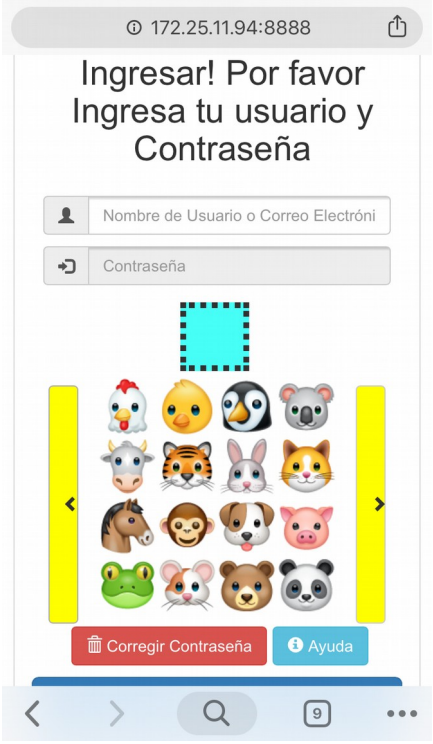


Figura 11: Interfaz de logueo gráfica Drag&Drop para móviles, con imágenes alusivas a animales

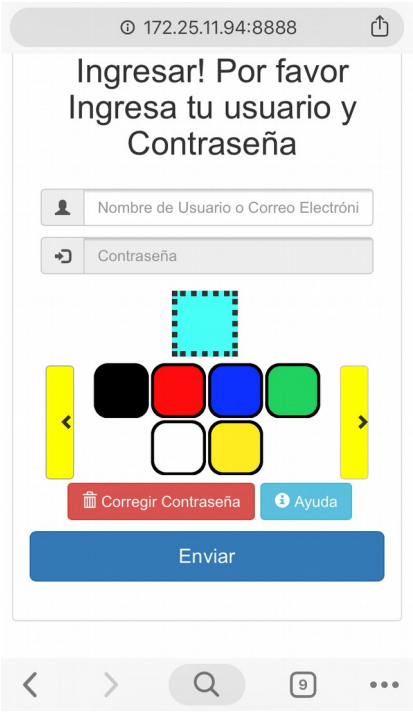


Figura 12: Interfaz de logueo gráfica Drag&Drop para móviles, con imágenes alusivas a colores

4.5.2.6. MANIPULACIÓN DE EVENTOS DRAG&DROP

Suponiendo que el usuario complete el proceso satisfactoriamente los eventos se dispararán y realzarán una operación determinada, la acción de cada evento de forma correcta significará que el usuario ha añadido una imagen como parte de su contraseña.

4.5.2.6.1. ONDRAGSTART()

Este evento es disparado inmediatamente cuando el usuario hace click por encima de una imagen o elemento fuente, y lo mantiene, no se debería confundir con el evento onclick().

Evento Precedente: ninguno

Operaciones realizadas:

Este evento es disparado cuando el usuario hace un click encima de la imagen con la intención de arrastrarla, lo que hace que se reciban los

parámetros enviado por el evento, que son: ev y nu; donde ev es un objeto que manipulará el evento, y nu remite el valor representativo de la imagen en cuestión.

Luego se asigna una imagen de señuelo que reemplazará a la imagen seleccionada, se recalca que se sustituye la imagen, no así el valor representativo de esta, con el fin de que terceras personas no puedan visualizar la imagen que será arrastrada.

Finalmente se asigna el valor de nu a una variable auxiliar, a la espera de que el usuario concrete exitosamente el proceso y se hacen desaparecer las imágenes.

Captura de Pantalla de la interfaz de usuario:

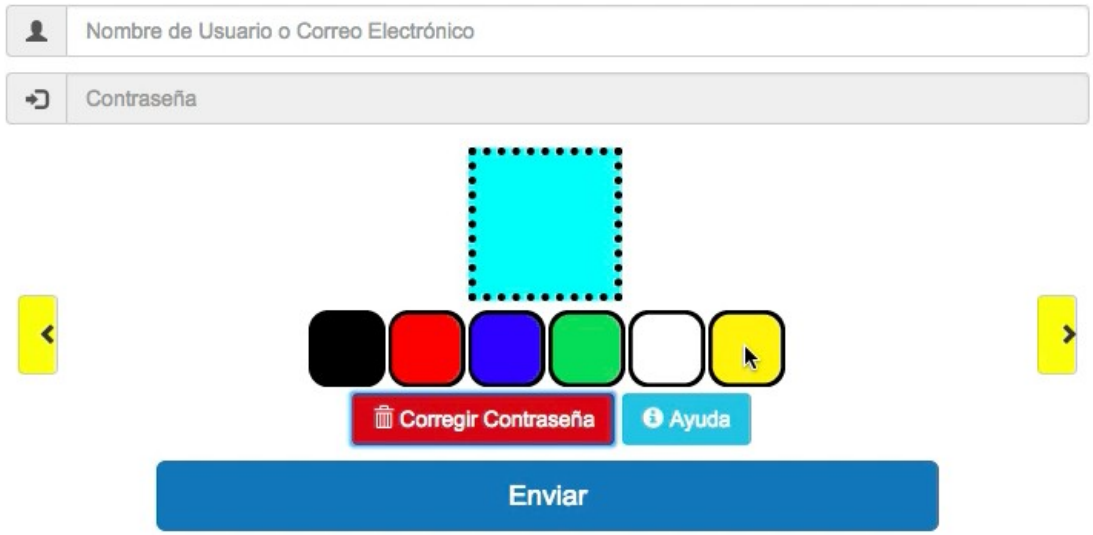


Figura 13: Interfaz de logueo gráfica Drag&Drop durante el evento ondragstart() activado

4.5.2.6.2. ONDRAG()

Evento Precedente: ondragstart()

Operaciones realizadas:

El evento es disparado una vez que el usuario mueva el cursor con la imagen elegida, el evento se mantiene activo siempre y cuando el usuario mantenga el botón del mouse oprimido.

Al estar activo, este evento nos permite destacar el área hasta donde el usuario debe arrastrar la imagen, en este caso lo que se hace es que se colorea en rojo el borde de la caja, esto a manera de darle una idea al usuario de que hacer.

Captura de Pantalla de la interfaz de usuario:

Figura 14: Interfaz de logueo gráfica Drag&Drop durante el evento ondrag() activado

4.5.2.6.3. ONDRAGENTER() Y ONDRAGOVER

Evento Precedente: ondrag()

Operaciones realizadas:

Ondragenter() y Ondragover() actúan en conjunto, y pueden considerarse similares, pero actúan de forma diferente, ondraenter() se activa cada vez que el usuario ingresa con la imagen a la caja objetivo, mientras que

ondragover() se mantiene activo todo el tiempo que el elemento fuente se encuentre dentro de la caja.

Permiten cambiar el color de la caja objetivo, reemplazando el color original por el color verde, dándole al usuario la idea de que arrastró la imagen al lugar correcto.

Captura de Pantalla de la interfaz de usuario:

Figura 15: Interfaz de logueo gráfica Drag&Drop durante el evento ondragenter() y ondragover() activados

4.5.2.6.4. ONDRAGLEAVE()

Evento Precedente: ondragenter()

Operaciones realizadas:

Este evento es disparado cuando el usuario sale con la imagen arrastrada afuera de la caja objetivo sin dejarla caer, lo que nos permite hacer es volver a colorear en rojo el borde de la caja, a modo de indicarle el área correcta donde debe realizarse el 'drop', se usa en conjunto con el evento ondragenter para este fin.

Captura de Pantalla de la interfaz de usuario:

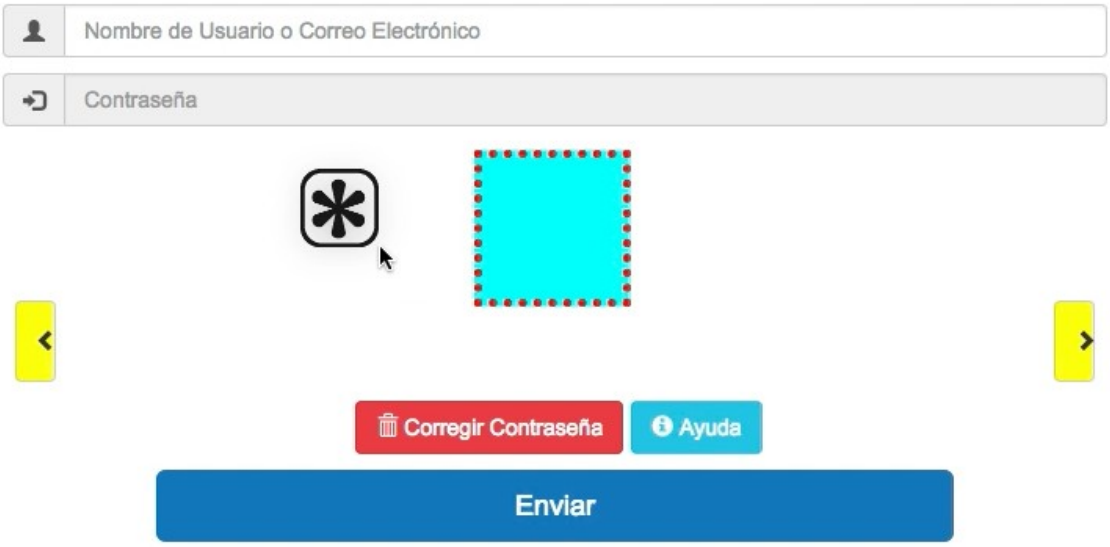


Figura 16: Interfaz de logueo gráfica Drag&Drop durante el evento ondragleavet() activado

4.5.2.6.5. ONDRAGEND()

Evento Precedente: ondrag() o ondrop()

Operaciones realizadas:

Este evento es disparado cuando el usuario suelta la imagen que estaba siendo arrastrada, tanto por soltarla dentro de la caja objetivo como por dentro, no ayuda a devolver la caja objetivo a su aspecto original, con el fin de comenzar el proceso de nuevo, como también vuelve a aparecer la gama de imágenes de la parte inferior.

Captura de Pantalla de la interfaz de usuario:

4.5.2.6.6. ONDROP()

Evento Precedente: ondragenter() y ondragover()

Operaciones realizadas:

Este evento es disparado cuando el usuario suelta la imagen dentro de la caja objetivo, en el caso del proyecto es la pauta de que el proceso de arrastre de una imagen que compone una contraseña se realizó con éxito.

Y se realizan dos operaciones importantes, primeramente, se pasa el valor de la variable auxiliar que en la que se guardó nu (en el evento ondragstart), a un arreglo donde se irán guardando secuencialmente cada valor representativo de las imágenes arrastradas por el usuario, y también se añadirá un asterisco al campo de contraseña de la interfaz de usuario, esto para darle al usuario de que arrastró exitosamente una imagen.

Captura de Pantalla de la interfaz de usuario:

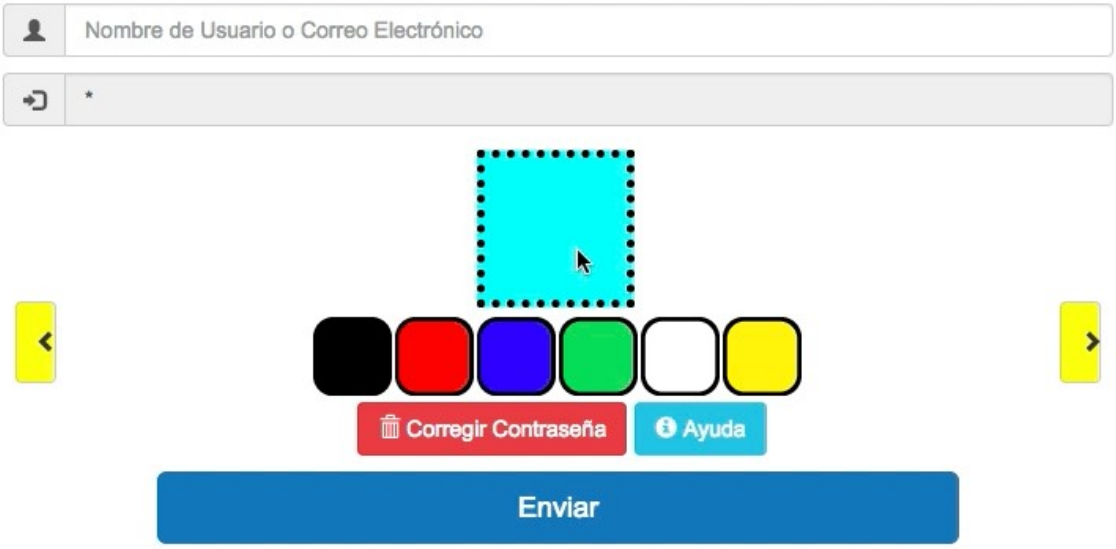


Figura 17: Interfaz de logueo gráfica Drag&Drop durante el evento ondrop() activado

4.5.2.6.7. BOTONES COMPLEMENTARIOS DEL PROCESO

Corregir Contraseña:

Para aquellos casos en el que usuario por un error involuntario arrastre una imagen que no sea de su elección, se añade el botón Corregir Contraseña, ya que este esquema no convencional de logueo no permite la corrección por métodos convencionales (mediante la tecla retroceso por ejemplo).

Este botón hace que el arreglo que almacena los valores de las imágenes en secuencia se vacíe, y al mismo tiempo vaciar de los asteriscos el

campo de contraseña de la interfaz de usuario, dándole la oportunidad al usuario de comenzar de vuelta el proceso en caso de algún inconveniente.

Ayuda:

En el caso de que el usuario no pueda o tenga dificultades en la intuición de como funciona el esquema de autenticación, se añade el botón de Ayuda, este permitirá el despliegue de una pequeña ventana modal con la una explicación del mecanismo a utilizar.

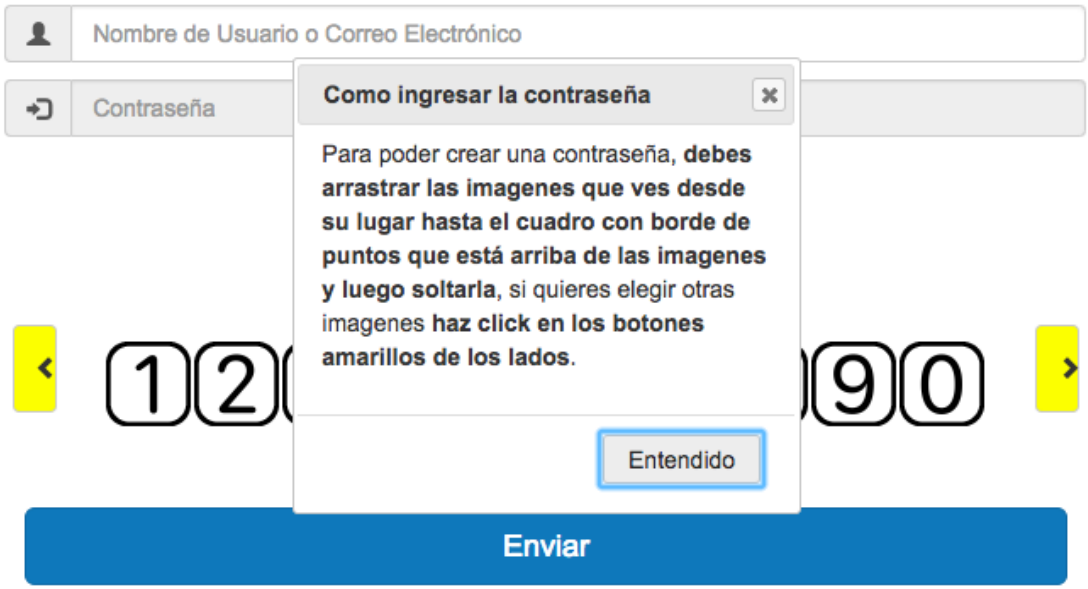


Figura 18: Muestra de mensaje de ayuda al usuario

Direccionales para cambiar de imágenes:

A manera de poder darle al usuario mayor variedad en cuanto a las posibles elecciones de las imágenes componentes de su contraseña se agregaron un total de 126 imágenes, agrupadas según similitudes entre si. Sin embargo, cargar la interfaz de usuario con 126 elementos representaría una ineficiencia y un mal diseño de la interfaz, para la solución de este

inconveniente, se agregaron dos botones a los lados, los cuales se encargan de cambiar el grupo de imágenes una vez que son oprimidos.

4.6. PRUEBA PILOTO DE EXPERIMENTACIÓN

Cumpliendo con los objetivos del proyecto se llevaron a cabo pruebas de experimentación, en donde usuarios verdaderos fueron sometidos al proceso de, primeramente creación de la contraseña gráfica con Drag&Drop y las imágenes, y luego varios procesos autenticación seguidos, esto con el propósito de analizar el comportamiento del usuario en cuanto al nuevo esquema de logueo sugerido, y al mismo tiempo observar al sistema mismo, esperando observar debilidades o puntos que mejorar y adaptar.

De igual manera se buscó comparar el método gráfico con el convencional, fue por eso por lo que se edificaron dos ventanas de logueo, una con un sistema convencional de logueo a base de texto y otras con el sistema gráfico con Drag&Drop.

Para la realización de la mencionada prueba se procedió a la habilitación de un servidor web en donde alojar un simple esquema de registro de usuarios y logueo en ambos sistemas, que luego diera paso a la realización de una encuesta que se tratara sobre los ámbitos de los usuarios consultados para con sus contraseñas.

Se dividió el grupo en dos partes, una parte realizaron el registro y creación de contraseña un el método convencional y la otra parte lo hizo con el método gráfico con Drag&Drop. Se midieron varios tiempos con el fin de tener datos certeros del comportamiento del sistema de autenticación Drag&drop, y poder compararlos con el esquema convencional, entre los que podemos citar: el tiempo de arrastre de una imagen, tiempo de creación de una contraseña,

así como también se registró las veces que los usuarios oprimieron los botones de corregir contraseña y ayuda, de igual manera las veces en las que los usuarios fallaron su contraseña como también las veces que tuvieron éxito.

En base al modelo descrito anteriormente se pueden citar los siguientes resultados:

Tiempo de Creación de una Contraseña:

	Sistema Convencional	Sistema Drag&Drop
Tiempos en General		
Tiempo Máximo	40052	130274
Tiempo Mínimo	745	519
Promedio	17285	25854
Tiempos en Dispositivos Móviles		
Tiempo Máximo	37867	130274
Tiempo Mínimo	745	519
Promedio	16950	27863
Tiempos en Desktops		
Tiempo Máximo	40052	68484
Tiempo Mínimo	3875	2653
Promedio	20085	19710

Tabla 1. Tiempos de creación de contraseñas Drag&Drop y Convencional, en dispositivos móviles y desktops

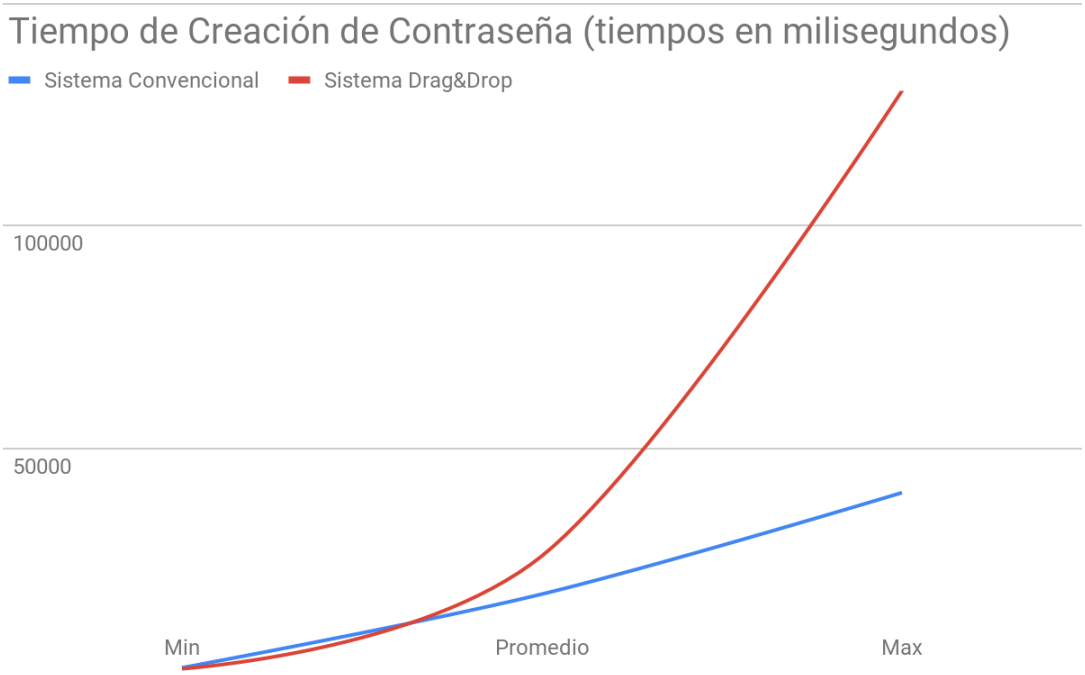


Figura 19: Gráfico de Tiempos de Creación de Contraseñas en registros con contraseñas Drag&Drop y contraseñas Convencionales

Interpretación de resultados:

Gracias a los tiempos captados podemos decir que promedio los usuarios de un grupo tardaron 25 segundos aproximadamente en recordar la contraseña creada con el sistema Drag&Drop, frente a los 17 segundos que llevo al otro grupo recordar la contraseña convencional.

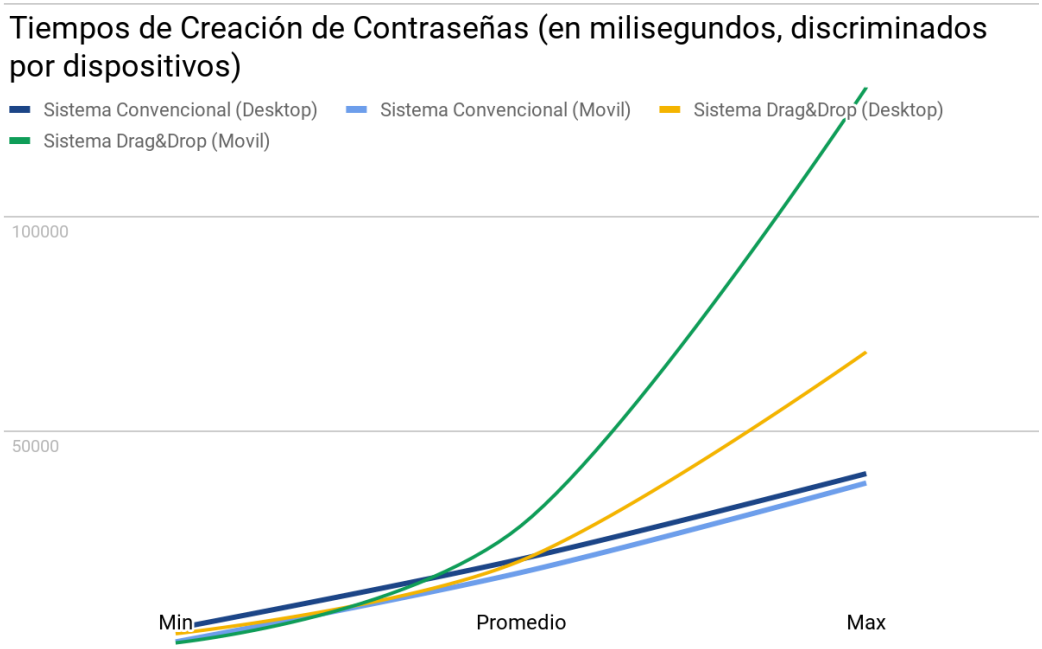


Figura 20: Gráfico de Tiempos de Creación de Contraseñas discriminados por dispositivos utilizados

Arrastre de imágenes:

Cantidad:

Arrastres Exitosos en Dispositivos Móviles	1372
Arrastres Exitosos en Dispositivos Desktop	380
Total	1752

Tabla 2. Cantidad de arrastres exitosos de imágenes en dispositivos móviles y desktops

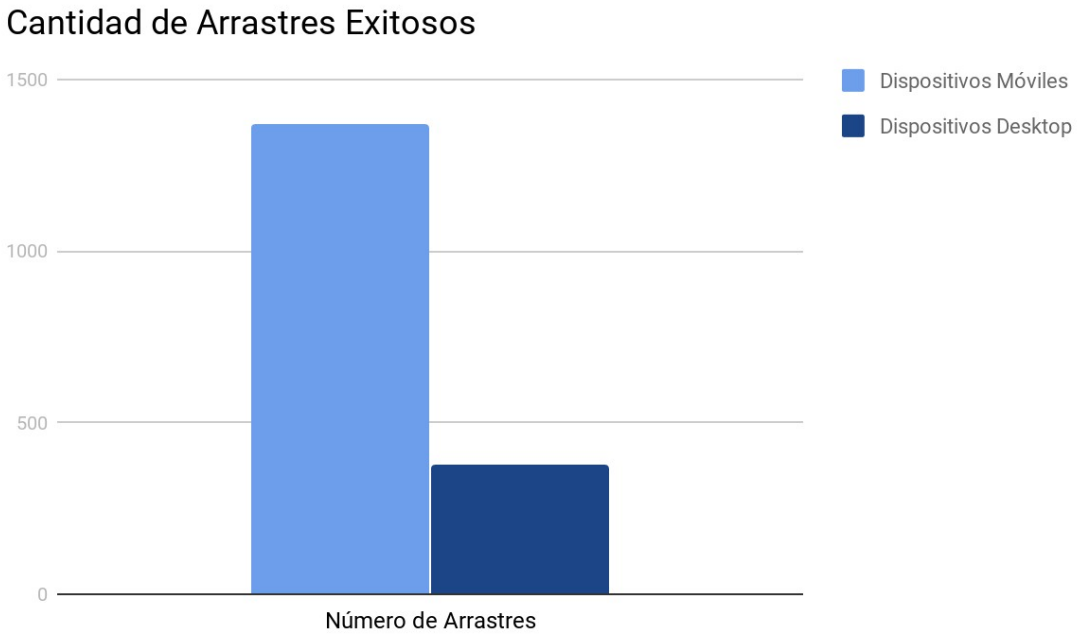


Figura 21: Gráfico de cantidad de arrastres exitosos de imágenes con el sistema Drag&Drop en Dispositivos Móviles y Desktops

Interpretación de resultados:

Estos números nos dicen el número de arrastres desde dispositivos móviles es superior en por tres veces al número de arrastres realizados desde desktops con mouses.

Tiempos de Arrastre de una imagen:

Tiempos en General	
Tiempo Máximo	6733
Tiempo Mínimo	109
Promedio	798
Tiempos en Dispositivos Móviles	
Tiempo Máximo	6681
Tiempo Mínimo	109
Promedio	811
Tiempos en Desktops	
Tiempo Máximo	6733
Tiempo Mínimo	177
Promedio	753

Tabla 3. Tiempos de arrastres exitosos de imágenes en dispositivos móviles y desktops

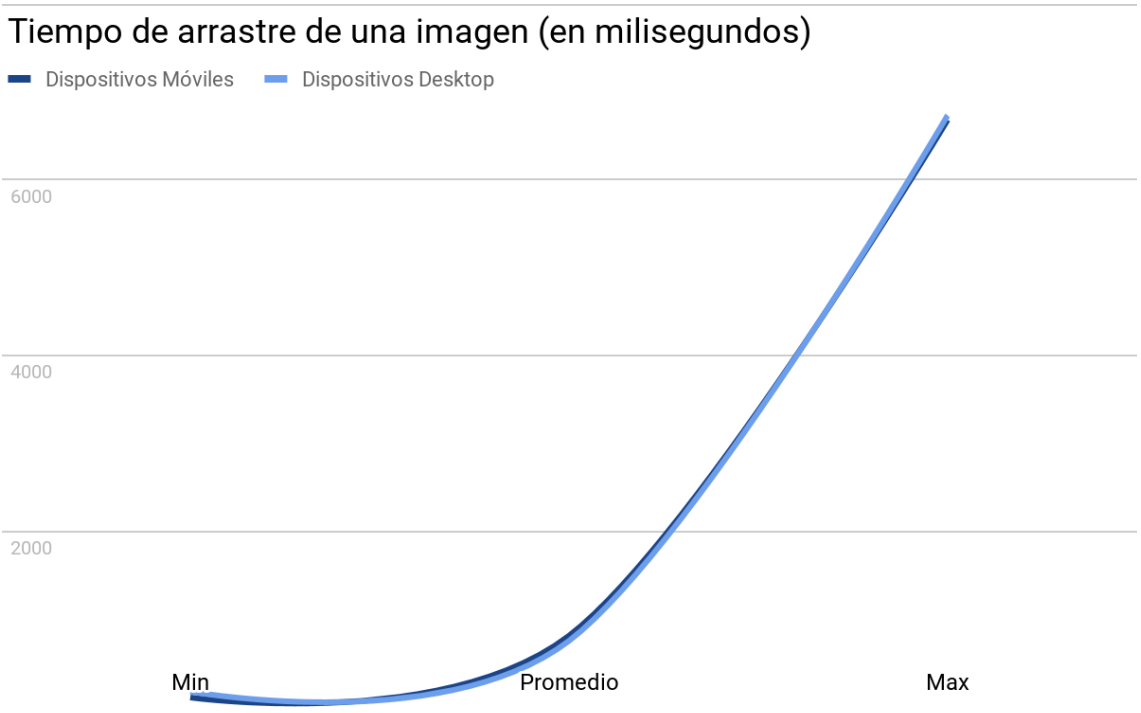


Figura 22: Gráfico de tiempo de arrastres exitosos de imágenes con el sistema Drag&Drop en Dispositivos Móviles y Desktops

Interpretación de resultados:

Mediante los tiempos captados durante el proceso de arrastre en dispositivos móviles como en desktop, podemos decir que la diferencia entre una plataforma y otra es minúsculo. Por ende la usabilidad es la misma en ambos tipos de dispositivos.

Presión de Botones de Ayuda y Corregir Contraseña:

Botón Oprimido	Cantidad de Veces
Corregir Contraseña	135
Ayuda	19
Total	154

Tabla 4. Cantidad de veces oprimidas de botones de Ayuda y Corregir Contraseña

Ingresos Exitosos y Fallidos:

	Sistema Convencional	Sistema Drag&Drop
Porcentaje de Intentos Exitosos	63%	76%
Porcentaje de Intentos Fallidos	37%	24%

Tabla 5. Porcentaje logeos exitosos y fallidos en el Sistema de Contraseña Drag&Drop y Convencional

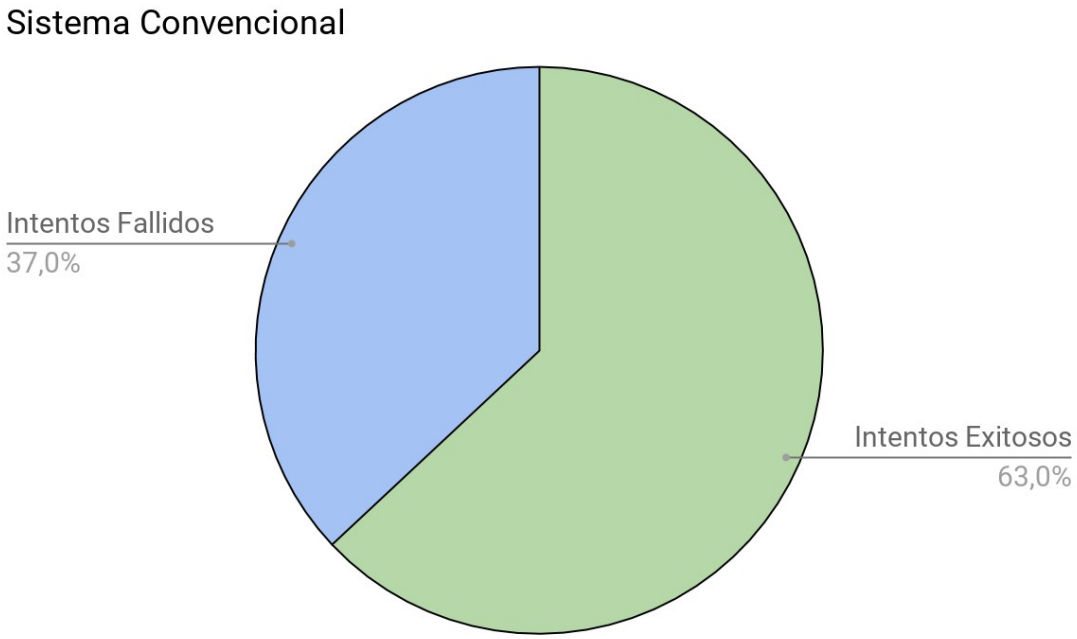


Figura 23: Gráfico de porcentaje de logeos fallidos y exitosos con un sistema convencional de contraseñas

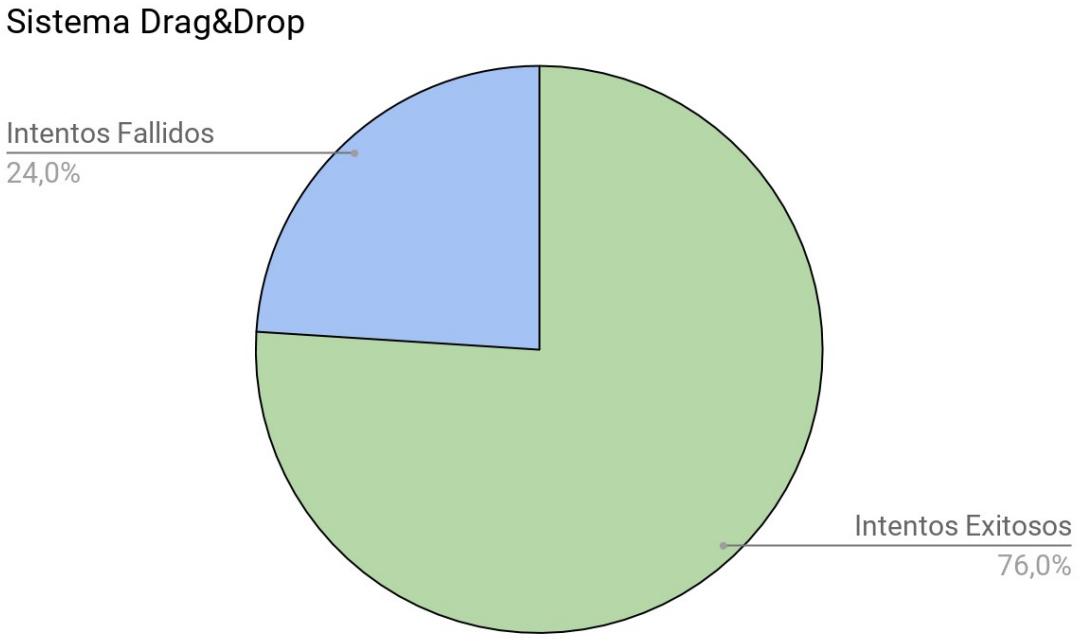


Figura 24: Gráfico de porcentaje de logeos fallidos y exitosos con el sistema Drag&Drop e Imágenes

Interpretación de resultados:

Esta podría ser la medición comparativa más importante de la prueba, nos demuestra que con el sistema gráfico de autenticación con Drag&Drop los usuarios tendieron a fallar menos que con las contraseñas convencionales, por 13 puntos para ser exactos.

4.7. ANÁLISIS DE CARGA DE IMPLEMENTACIÓN DE SISTEMA DE AUTENTICACIÓN CON DRAG&DROP

Al hablar del desarrollo de cualquier software es prácticamente inevitable hacerlo sin tener en cuenta el análisis del rendimiento de este, y en el caso particular del método de autenticación gráfico con Drag&Drop se pueden destacar dos procesos que podrían implicar una carga para el sistema en comparación con otros métodos de autenticación convencional.

En primer lugar se tiene el proceso de encriptación del valor representativo de cada imagen en el back-end, el cual como se mencionó anteriormente es encriptado dos veces (simétrica y asimétricamente) para luego ser codificado para su paso al lado del cliente, este proceso de encriptación y codificación de aproximadamente 120 texto plano en un lapso de 20 segundo podría representar una carga poco común para un servidor cualquiera.

Posterior a la encriptación en el lado del servidor, se tiene otro lapso de posible carga considerable, y esta vez ya presenta una carga en el lado del cliente, y una carga para el dispositivo en el que se esté realizando el proceso de autenticación, esta consistiría en la solicitud al servidor y descarga de cada imagen, lo cual en condiciones de red poco favorables podría traer inconvenientes con los tiempos de carga de un grupo cualquiera de imágenes.

4.7.1. LADO DEL SERVIDOR:

Antes de realizar cualquier análisis de rendimiento es conveniente describir el elemento a ser analizado, en el este caso el servidor donde es alojado el sistema de autenticación, el mismo es un Servidor Privado Virtual, proveído por vultr.com, con las siguientes características:

- CPU: 1 vCore
- Memoria RAM: 1024 MB
- Capacidad de Almacenamiento: 25 GB SSD
- Sistema Operativo: Ubuntu 16.04 x64

Para el correspondiente análisis de la carga del sistema en el servidor se utilizó el Software Utilitario para servidores denominado Netdata, con el cual se colecta información relevante del desempeño del servidor

4.7.1.1. NETDATA:

Netdata actúa en tiempo real, monitoreando el rendimiento y el estado de los sistemas y aplicaciones. Se basa en un potente agente de supervisión que es instalado en todos los sistemas y contenedores. Netdata proporciona información incomparable, en tiempo real, de todo lo que sucede en los sistemas que se están ejecutando (incluidos servidores web, bases de datos, aplicaciones) mediante el uso de paneles web altamente interactivos. Puede ejecutarse de forma autónoma, sin componentes de terceros, o puede integrarse a las cadenas de herramientas de monitoreo existentes (Prometheus, Graphite, OpenTSDB, Kafka, Grafana, etc.). Netdata es rápido y eficiente, diseñado para ejecutarse permanentemente en todos los sistemas (servidores físicos y virtuales, contenedores, dispositivos IoT), sin interrumpir su función principal. Es un software gratuito de código abierto y actualmente se ejecuta en Linux, FreeBSD y MacOS [19].

Para la realización del análisis se mantuvo al servidor primeramente sin ninguna actividad, con el software de monitoreo Netdata activo se procedió a ingresar a la ventana de logueo con el método de Drag&Drop, para luego poder observar en el monitor los cambios ocurridos en el servidor cuando un usuario recorría las imágenes disponibles para ser parte de su contraseña, este acción es la única que merece la atención ya que al cambiar de un grupo de imágenes a otro, se realiza una nueva solicitud al servidor, por lo que este responde con las imágenes solicitadas y más importante es el hecho de que el servidor realiza la encriptación híbrida al texto plano representativo de cada imagen.

De la correspondiente observación se obtuvo las siguiente observaciones y deducciones.

Utilización de CPU de los servicios de Systemd (100% = 1 núcleo) (services.cpu)

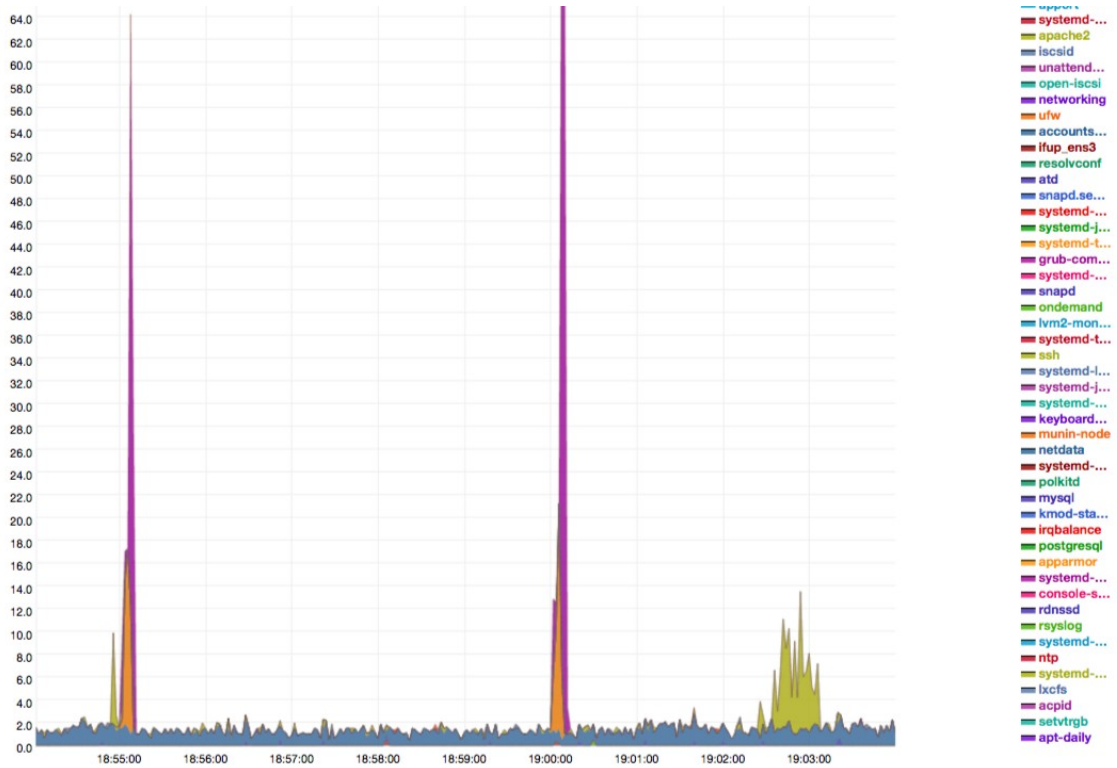


Figura 25: Gráfico de utilización del procesador durante un proceso de uso de contraseña Drag&Drop

La actividad de interés correspondiente al servidor web es la marcada con el color verde, entre los puntos 19:02:00 y 19:03:10, alcanzando un pico máximo del 14% de uso del CPU, valor aceptable, teniendo en cuenta la capacidad del servidor, y que un usuario en ese momento hizo que el sistema encriptara (simétrica y asimétricamente) más de 120 textos planos de una longitud de 4 caracteres cada uno.

Memoria RAM

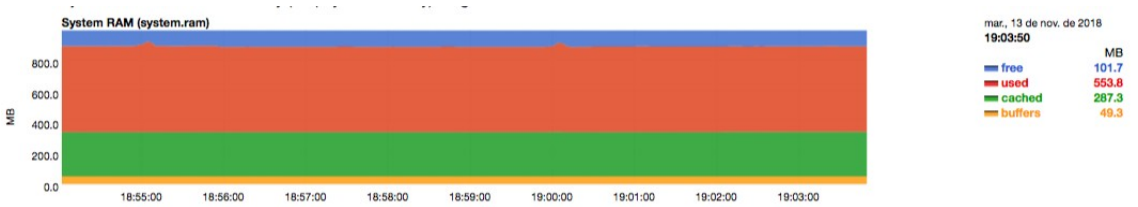


Figura 26: Gráfico de utilización de la Memoria RAM durante un proceso de uso de contraseña Drag&Drop

En el caso de la memoria RAM esta se mantiene prácticamente invariable durante la interacción con el usuario.

Escritura/Lectura del Disco

Figura 27: Gráfico de Lectura/Escritura del Disco durante un proceso de uso de contraseña Drag&Drop

En el caso de la interacción con el disco al momento de que el usuario este interactuando con la interfaz, esta es casi nula al igual que la memoria RAM.

Uso de la Red

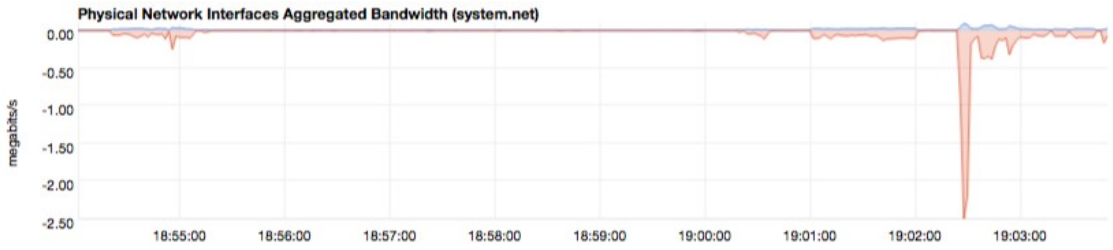


Figura 28: Gráfico de uso de la red durante un proceso de uso de contraseña Drag&Drop

El pico rojo visualizado corresponde al momento de la interacción, este gráfico nos da a entender que más que solo la carga de la encriptación, el sistema tiene una carga poco común al momento de enviar el grupo de imágenes, lo cual es de considerar cuidadosamente, más si se tienen muchos usuarios simultáneamente.

Los datos observados dan una idea del impacto que tiene el proceso de encriptación utilizado y el envío de varias imágenes al mismo tiempo para el servidor en el que se implemente, por más que las cifras parecen ínfimas, es de tener en cuenta que al comparar el de los mismos parámetros en un sistema de autenticación convencional la diferencia será notable, como se podrá ver a continuación.

Utilización de CPU de los servicios de Systemd (100% = 1 núcleo) (services.cpu), en un sistema de logueo convencional (en el mismo servidor, bajo las mismas condiciones de red).

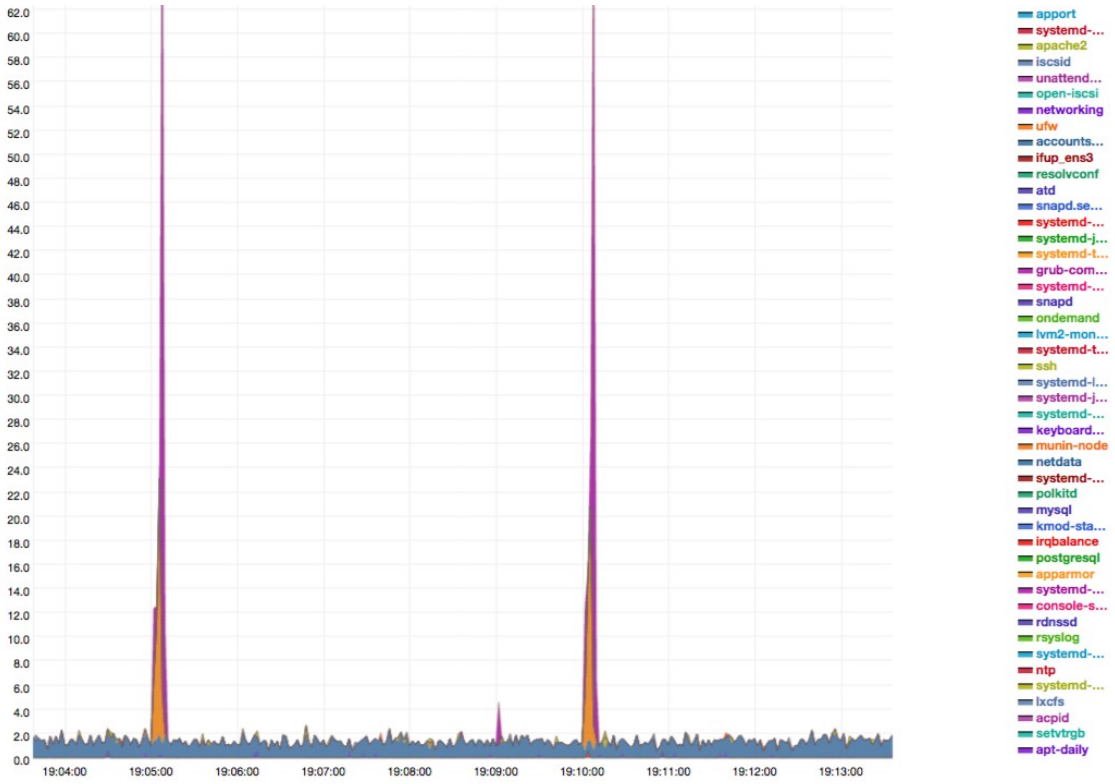


Figura 29: Gráfico de uso del procesador durante un proceso de uso de contraseña convencional

Memoria RAM, en un sistema de logueo convencional (en el mismo servidor, bajo las mismas condiciones de red).

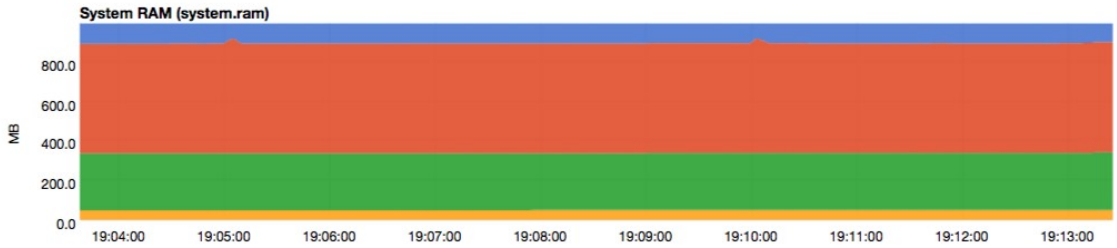


Figura 30: Gráfico de uso de la memoria RAM durante un proceso de uso de contraseña convencional

Escritura/Lectura del Disco, en un sistema de logueo convencional (en el mismo servidor, bajo las mismas condiciones de red).

Figura 31: Gráfico de Lectura/Escritura del disco durante un proceso de uso de contraseña convencional

Uso de la Red, en un sistema de logueo convencional (en el mismo servidor, bajo las mismas condiciones de red).

Figura 32: Gráfico uso de la red durante un proceso de uso de contraseña convencional

Para esta observación se procedió de forma similar a la anterior, teniendo el servidor inactivo, un usuario accedió a una ventana de logueo convencional, esta interacción se da entre los puntos 19:11:00 y 19:13:00 y como se puede observar en los gráficos, las cifras son despreciables en comparación con el sistema de Drag&Drop e imágenes.

Al terminar el análisis en el backend se puede concluir que la carga en el servidor puede ser considerable, comparándola con sistemas convencionales, de igual manera puede representar una sobrecarga para el servidor si la cantidad de usuarios excede las capacidades del equipamiento.

4.7.2. LADO DEL CLIENTE:

4.7.2.1. CHROME DEVTOOLS:

Chrome DevTools es un conjunto de herramientas de creación web, análisis y depuración integrado con el navegador web Google Chrome.

Parámetros iniciales del estado de la red:

A manera de realizar un adecuado análisis a los tiempos de carga del sitio en el lado del cliente es conveniente definir las condiciones de la red donde se realizó este análisis, para eso definimos los siguientes:

- Dirección del Servidor que aloja el código a analizar: http://207.246.114.46/
- Latencia Promedio: 290,6 ms

```
sh-3.2# ping 207.246.114.46
PING 207.246.114.46 (207.246.114.46): 56 data bytes
64 bytes from 207.246.114.46: icmp_seq=0 ttl=50 time=296.120 ms
64 bytes from 207.246.114.46: icmp_seq=1 ttl=50 time=268.965 ms
64 bytes from 207.246.114.46: icmp_seq=2 ttl=50 time=262.976 ms
64 bytes from 207.246.114.46: icmp_seq=3 ttl=50 time=357.375 ms
64 bytes from 207.246.114.46: icmp_seq=4 ttl=50 time=376.299 ms
64 bytes from 207.246.114.46: icmp_seq=5 ttl=50 time=292.617 ms
64 bytes from 207.246.114.46: icmp_seq=6 ttl=50 time=316.070 ms
64 bytes from 207.246.114.46: icmp_seq=7 ttl=50 time=263.307 ms
64 bytes from 207.246.114.46: icmp_seq=8 ttl=50 time=360.639 ms
64 bytes from 207.246.114.46: icmp_seq=9 ttl=50 time=379.936 ms
64 bytes from 207.246.114.46: icmp_seq=10 ttl=50 time=259.018 ms
```

Figura 33: Latencia de la red al momento de realizar el análisis

Para comenzar a analizar el comportamiento del esquema de autenticación gráfico con Drag&Drop se debe recordar lo siguiente: un usuario puede crear su contraseña con imágenes, este dispone de un total de 216 imágenes como opciones, sin embargo las mismas no aparecen al mismo tiempo en la misma interfaz, para que el usuario pueda elegir de entre las diferentes opciones disponibles debe hacer click o tocar los botones amarillos a los lados del grupo de imágenes ya disponible, esto le ayuda a desplazarse de entre las opciones disponibles.

También es de considerar que las imágenes se encuentran agrupadas de acuerdo con semejanzas cognitivas entre si, es decir, las imágenes que representen animales conformarán un grupo, las imágenes que representen comida serán otro, y así sucesivamente, el último detalle a considerar es que cada vez que el usuario oprima los botones amarillos para pasar al siguiente grupo de imágenes, esto desembocará en una nueva solicitud al servidor.

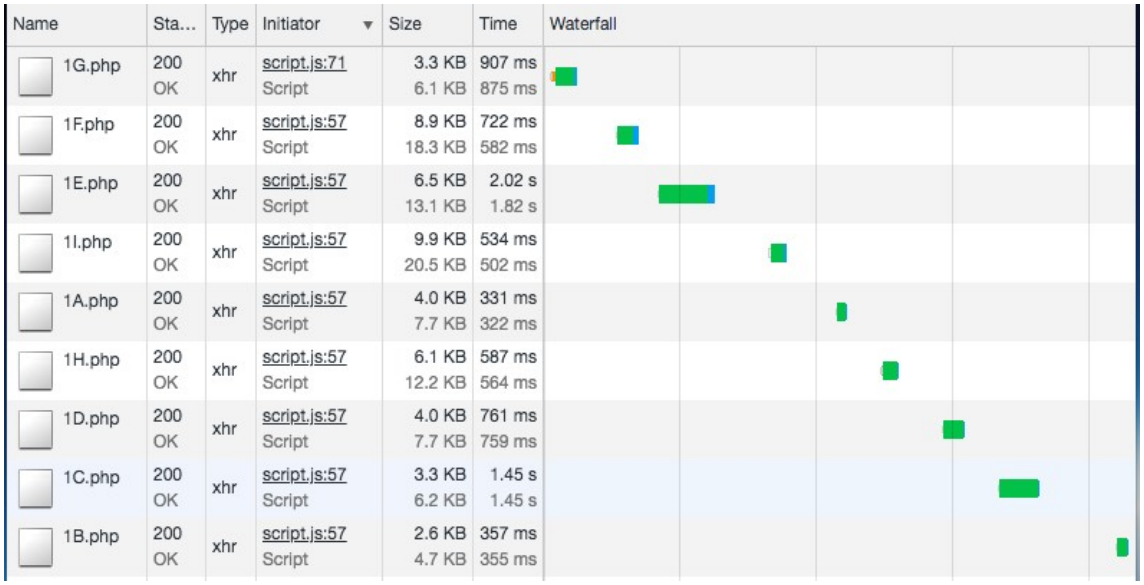
Considerando lo mencionado se podrá entender mejor el siguiente gráfico que muestra los tiempos de carga de cada grupo de imágenes mientras que un usuario se desplaza por ellos.

Figura 34: Tiempos de espera y carga de grupos de imágenes durante una interacción con la ventana de logueo Drag&Drop

Este gráfico nos indica que el recorrido tras todos los grupos de imágenes tarda un poco menos de 20 segundos, también en promedio una

imagen tarda 500 milisegundos en cargarse, y que pueden haber en promedio 5 imágenes cargándose en paralelo, lo cual permite por ejemplo la carga de 26 imágenes en 1,36 segundos.

El siguiente gráfico muestra cuánto tiempo espera el cliente para comenzar a recibir el contenido de cada grupo de imágenes, el tiempo de espera representado en verde y el tiempo de descarga en azul, el tiempo de espera se podría considerar el tiempo desde que el usuario solicita el siguiente grupo de imágenes hasta que estas comienzan a cargarse, este es el lapso de tiempo en el que el servidor encripta los valores representativos de cada imagen, y como es de esperarse, aquellos grupo con un mayor número de imágenes tardan mas en comenzar la carga del contenido ya que es mayor el número de valores a encriptar, tardando así hasta 1,82 segundos en comenzar la carga de un grupo numeroso.



Name	Sta...	Type	Initiator	Size	Time	Waterfall
1G.php	200 OK	xhr	script.js:71 Script	3.3 KB 6.1 KB	907 ms 875 ms	
1F.php	200 OK	xhr	script.js:57 Script	8.9 KB 18.3 KB	722 ms 582 ms	
1E.php	200 OK	xhr	script.js:57 Script	6.5 KB 13.1 KB	2.02 s 1.82 s	
1I.php	200 OK	xhr	script.js:57 Script	9.9 KB 20.5 KB	534 ms 502 ms	
1A.php	200 OK	xhr	script.js:57 Script	4.0 KB 7.7 KB	331 ms 322 ms	
1H.php	200 OK	xhr	script.js:57 Script	6.1 KB 12.2 KB	587 ms 564 ms	
1D.php	200 OK	xhr	script.js:57 Script	4.0 KB 7.7 KB	761 ms 759 ms	
1C.php	200 OK	xhr	script.js:57 Script	3.3 KB 6.2 KB	1.45 s 1.45 s	
1B.php	200 OK	xhr	script.js:57 Script	2.6 KB 4.7 KB	357 ms 355 ms	

Figura 35: Tiempos de espera y carga simplificado de grupos de imágenes durante una interacción con la ventana de logueo Drag&Drop

Esto da una idea de que el tener que desplazarse entre cada grupo de imágenes y a la vez esperar que estas se carguen, podría representar cierto tiempo que el usuario no este dispuesto a esperar, comparando estos tiempos

con el proceso de autenticación normal (a base de texto) el tiempo tomado por el sistema gráfico es considerablemente alto.

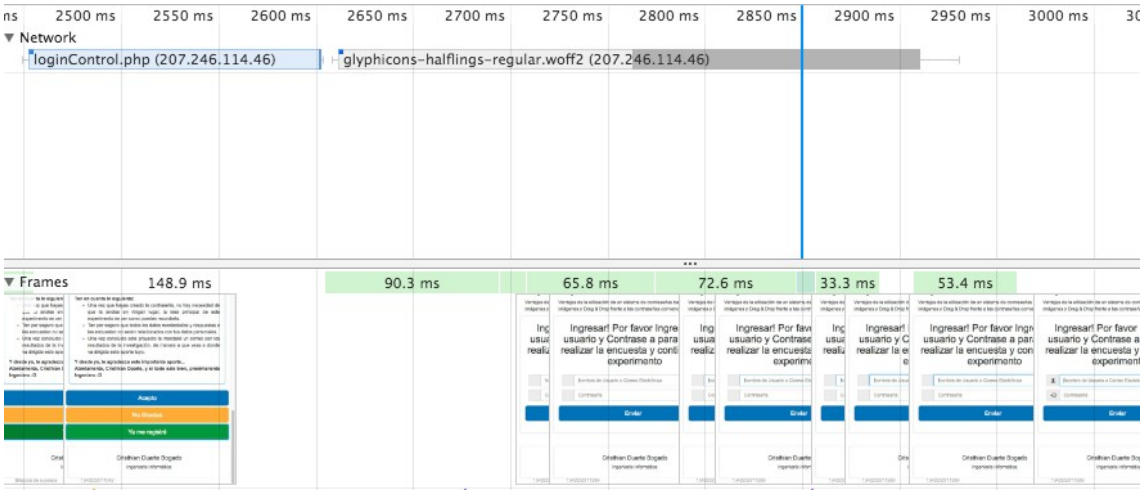


Figura 36: Tiempos de espera y carga simplificado de grupos de imágenes durante una interacción con una ventana de logueo convencional

La imagen anterior muestra el tiempo de carga de una interfaz de logueo convencional, compuesta por un campo de texto para el nombre de usuario y otro campo tipo password para la contraseña del usuario, lo cual es meramente código HTML, sin ningún otro elemento adicional.

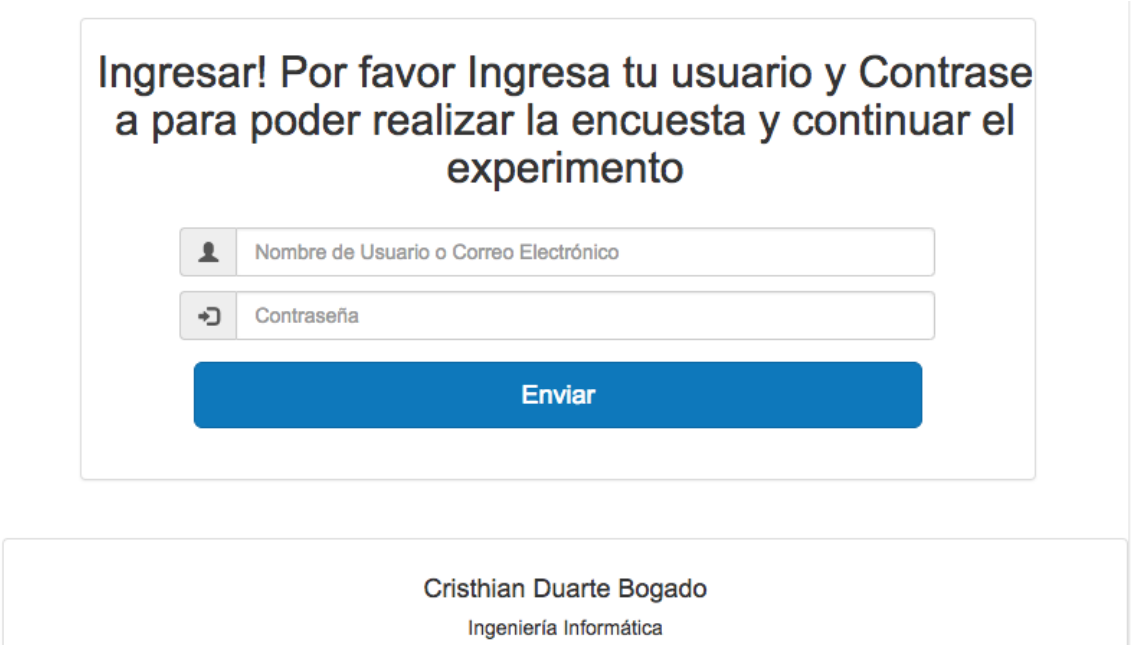


Figura 37: Interfaz de logueo convencional

Según el gráfico observado esta ventana es cargada a la interfaz del cliente en no más de 350 milisegundos, notablemente mucho más rápido que toda la experiencia con el método gráfico con Drag&Drop, este aspecto del análisis de carga es de gran importancia a la hora de deducir la efectividad de un método frente a otro y realizar una comparación costo/beneficio.

4.8. ESQUEMAS DE USO EFECTIVO DE LAS CLAVES PUBLICO/PRIVADA.

El uso de la encriptación asimétrica o de clave pública le brinda varias ventajas de seguridad a la estructura del método de autenticación ya mencionadas anteriormente, sin embargo para dotar al sistema de más mecanismos de seguridad, se recomienda adoptar configuraciones o políticas al sitio donde se implementará, como las que se detallarán más adelante.

4.8.1. CAMBIO PERIÓDICO DEL PAR DE CLAVES.

La adopción de políticas o configuraciones de cambio periódico y automático del par de claves, tanto la clave pública como la clave privada,

utilizadas para la encriptación asimétrica, podría dotar al esquema de fortaleza ante cierto tipo de ataque de robo de contraseña.

Esto no representaría ningún riesgo para que el sistema pueda cumplir con su objetivo, ya que como se ha visto en la descripción del esquema de encriptación utilizado, donde la encriptación híbrida utilizada en primera instancia al momento de cargar los valores representativos de cada imagen no tienen incidencia en el valor final guardado en la base de datos, ya que solo sirve para ocultar el valor real de cada imagen, por ende no afecta la comparación del valor en la base de datos y el valor ingresado por el usuario, al momento de querer este autenticarse.

El único recaudo a tener en cuenta para la adopción de esta política es el de no realizar el cambio del par de claves entre la carga de las imágenes y el proceso de entrada de la contraseña por parte del usuario, ya que de realizar esto, habrá una incongruencia al momento de desencriptar los valores de las imágenes elegidas por el usuario.

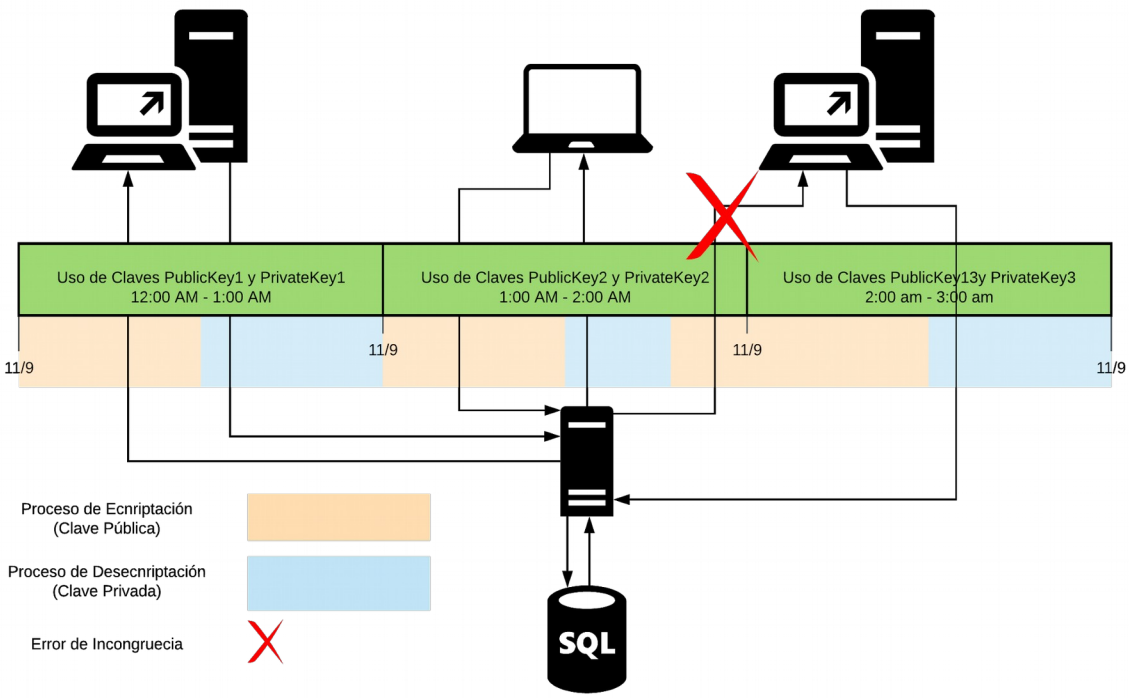


Figura 38: Esquema de cambio periódico de claves público/privada

4.8.2. ESTABLECIMIENTO DE VARIOS SERVIDORES WEB CON CLAVES DIFERENTES ENTRE SÍ.

Una variante de la política descrita anteriormente, vendría ser la configuración de varios servidores web dando servicio en paralelo, cada uno con un par de claves diferente al de los otros, pero ejecutando la misma interfaz y realizando consultas a la misma base de datos.

A modo de hacer más segura esta configuración se podría combinar con la anterior, es decir, configurar cambios periódicos a cada par de clave de cada servidor, tomando la precaución de sacar de servicio a aquel servidor al que las claves se le están cambiando, a modo de prevenir incongruencias a la hora de la desencriptación.

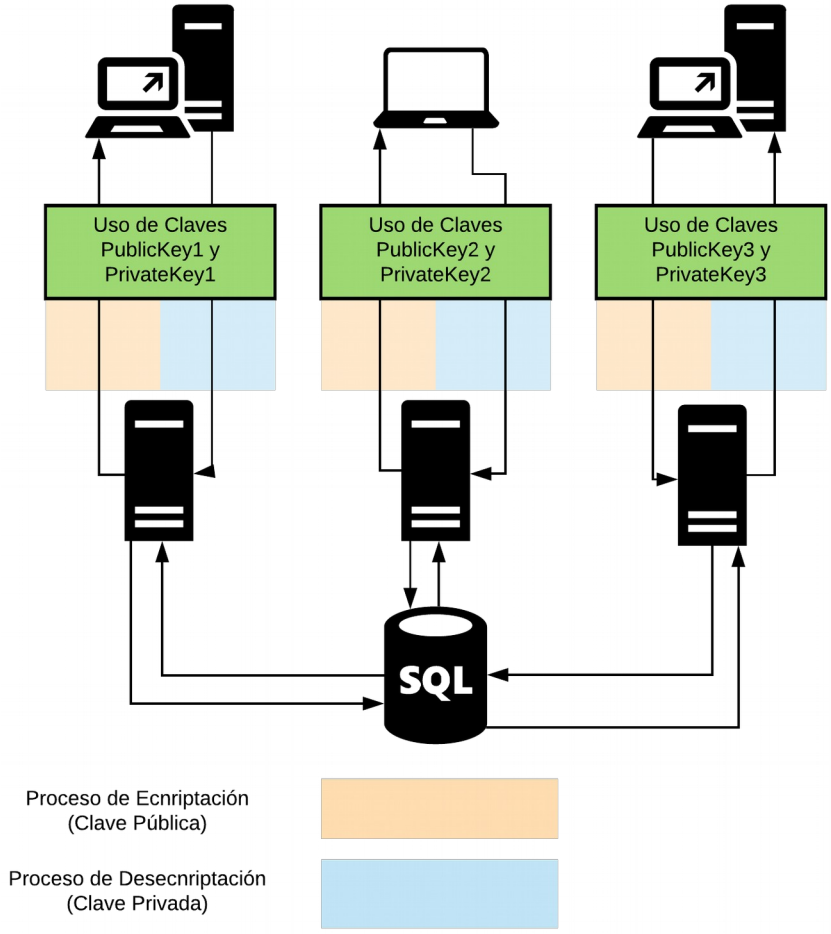


Figura 39: Esquema de configuración de servidores web en paralelo, con claves público/privada distintos entre si

4.8.3. ESTABLECIMIENTO DE PAR DE CLAVES ÚNICOS PARA SOLICITUD DE CLIENTE.

De todas las configuraciones propuesta, se podría considerar esta como la más sofisticada y segura, consistiría en establecer un par de claves pública y privada únicos por cada solicitud del cliente realizada al servidor, con este ya no se tiene que tener la misma precaución mencionada anteriormente sobre el cambio de las claves en el momento incorrecto, ya que de esta manera, el par de claves se mantiene fijo durante un proceso de logueo, y cambia ante alguna nueva solicitud de carga completa de la página web en cuestión.

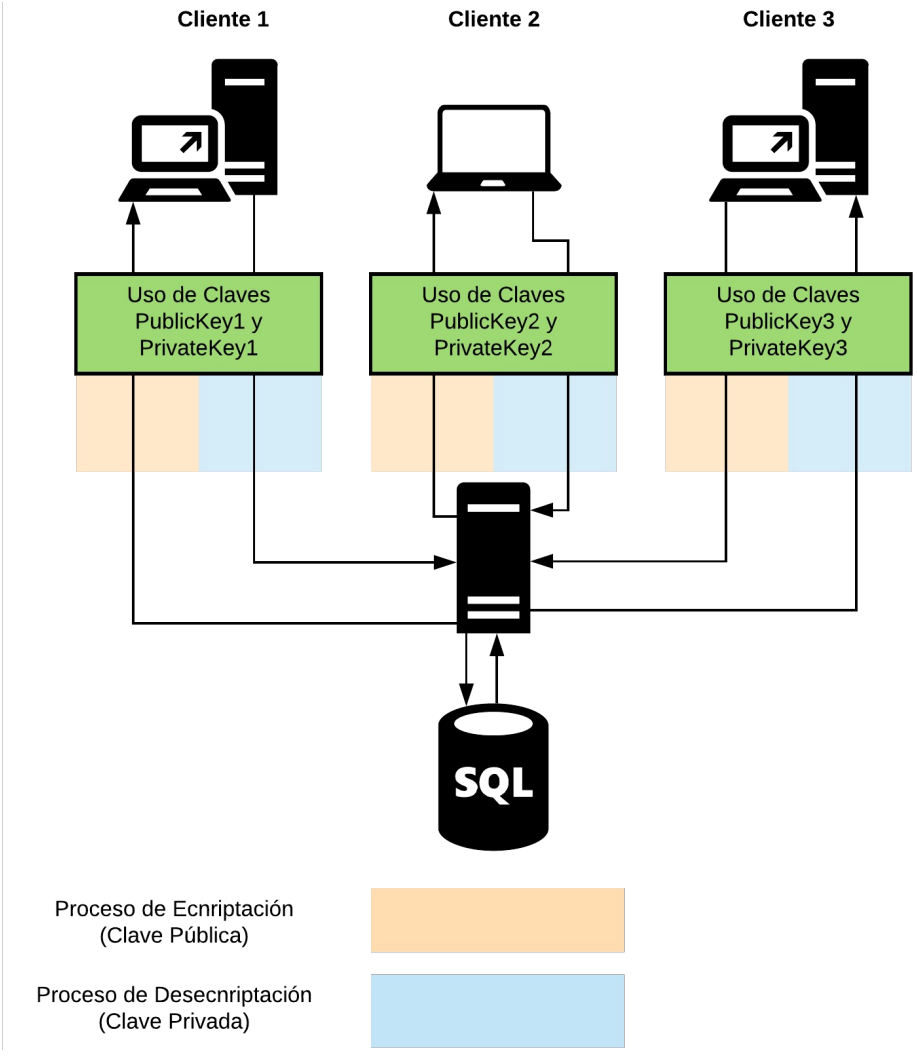


Figura 40: Esquema de establecimiento de claves público/privado únicos para cada conexión

4.9. ANALISIS TECNICO-TEORICO DE SEGURIDAD FRENTE A ATAQUES DE ROBO DE CONTRASEÑA.

Fuerza Bruta: Este tipo de ataque para el robo de una contraseña consiste simplemente en intentar todas las posibles combinaciones posibles hasta dar con la combinación correcta que corresponda a la contraseña del usuario.

Fuerza Bruta Asistida por Código: Este método es parecido al anterior, con la diferencia de que en lugar de que una persona esté intentando varias combinaciones de contraseña, una pieza de código es la que realiza las pruebas con todas las combinaciones posibles hasta dar con la indicada.

En el caso de que el sistema de autenticación Gráfico quiera ser sometido a un ataque de fuerza bruta asistido por código, el atacante debería (en el caso de que haya identificado la forma de utilizar los eventos de Drag&Drop para completar el proceso de logueo) captar el valor representativo de cada imagen, luego intentar cada combinación posible hasta que el servidor dé con una respuesta favorable.

Sin embargo un ataque de este tipo resultaría infructuoso, en primer lugar, debido a que cada valor representativo en el lado del cliente es encriptado con un cifrado híbrido (donde se incluye el cifrado asimétrico), y es esta funcionalidad la que hace que el valor representativo de cada imagen cambie con cada solicitud al servidor, por ende, captar cada valor para luego usarlo en un ataque de fuerza bruta sería una práctica frustrante, e innecesaria si no se conoce las claves con las que se encriptaron los valores.

Phishing: El phishing es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o

datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndolos a un sitio web falso [20].

MITM: Un ataque de hombre en el medio interfieren tres elementos, la víctima, la entidad con la que la víctima está tratando de comunicarse y el "hombre en el medio", que está interceptando las comunicaciones de la víctima (interceptando información confidencial, como nombres de usuario, contraseñas o números de tarjetas de crédito). Crítico para el escenario es que la víctima no es consciente del hombre en el medio [21].

Analizando la posibilidad de robo de la contraseña gráfica propuesta mediante un ataque de phishing o MITM, los cuales técnicamente tratarían de interceptar la comunicación Cliente - Servidor, en el caso del Phishing mediante un sitio web falso, asumiendo que en el phishing el atacante haya conseguido replicar el uso del Drag&Drop para el ingreso de la contraseña, y que en el MITM haya identificado el lugar donde se almacena el arreglo de los valores de la contraseña, ambos se toparía con un gran inconveniente en el caso de que las claves público-privada hayan sido cambiadas desde que el atacante capturo la información, ya que si el atacante tratara de utilizar la información robada esta no será aceptada por el servidor ya que fue cifrada con un par de claves ya descontinuadas.

Keyloggers: Los keyloggers realizan un seguimiento y registran cada tecla que se pulsa en una computadora, a menudo sin el permiso ni el conocimiento del usuario. Un keylogger puede estar basado en hardware o software, y se puede usar como herramienta lícita de control de TI, tanto profesional como personal. Sin embargo, los keyloggers también se pueden utilizar con fines delictivos. Por

regla general, los keyloggers son un spyware malicioso que se usa para capturar información confidencial, como contraseñas o información financiera que posteriormente se envía a terceros para su explotación con fines delictivos {Citation}.

Esta podría considerar como la fortaleza más evidente al ser esta, una propuesta de autenticación gráfica y no depender del teclado del usuario, dicho de otra manera, debido a la forma de uso del API de Drag&Drop para el ingreso de la contraseña, esto ayuda a exclusión del teclado como medio de ingreso de alguna clave importante, por ende cualquier software malicioso que esté captando las teclas oprimidas no podrá captar una contraseña ingresada con este medio gráfico.

Criptoanálisis: Normalmente, el objetivo de atacar un sistema de encriptación es recuperar la clave en uso en lugar de simplemente recuperar el texto plano de un solo texto cifrado. Los ataques criptoanalíticos se basan en la naturaleza del algoritmo y, quizás, algún conocimiento de las características generales del texto simple o incluso algunos ejemplos de pares de texto simple y texto cifrado. Este tipo de ataque explota las características del algoritmo para intentar deducir un texto simple específico o para deducir la clave que se está utilizando [11].

Un ataque de criptoanálisis en el escenario presentado por el método de autenticación gráfico buscaría saber el valor (en texto plano) representativo de cada imagen, o saber las claves involucradas, desafortunadamente para el atacante, hay un proceso de encriptación híbrido de por medio, dicho de otro modo, el texto plano (cuyo valor es el que representa una imagen) es primeramente encriptado de forma simétrica con una clave binaria, luego es

encriptado de forma asimétrica con una clave pública, esto provoca que el atacante en cuestión tenga que deducir las tres claves involucradas, sin embargo, en el caso de lograrlo, aun se estaría topando con inconvenientes ante un eventual cambio de claves.

Habiendo conocido los mecanismos de ataque de algunos métodos de robo de contraseñas es de notar las numerosas ventajas de sistema de autenticación basado en Drag&Drop e imágenes, como por ejemplo su fortaleza frente ataques de keyloggers, al ser un esquema gráfico y no habiendo nada que se ingrese por teclado o la fortaleza otorgada por el sistema de encriptación utilizado, dificultando ataques de fuerza bruta asistida por código, phishing o hombre en el medio.

A continuación se muestra un resumen en forma de tabla con las formas de ataque mencionadas anteriormente mencionadas asociadas a los mecanismos involucrados en el proceso de autenticación con Drag&Drop e imágenes, y como estos dan al sistema una forma de protección.

Mecanismo de seguridad implementado Forma de Ataque	Uso de Imágenes y del API Drag&Drop	Sistema de Encriptación	Cambio de Claves
Fuerza Bruta Asistida por código		Protegido	
Keylogger	Protegido	Protegido	
Phishing			Protegido
MITM			Protegido
Cripto análisis			Protegido

Tabla 6. Resumen de Protección ante diversas formas de robo de contraseña y Mecanismos implementados para la protección

4.10. OTROS BENEFICIOS PARA LA SEGURIDAD

4.10.1. CAPTCHAS

Un CAPTCHA (test de Turing público y automático para distinguir a los ordenadores de los humanos, del inglés "Completely Automated Public Turing test to tell Computers and Humans Apart") es un tipo de medida de seguridad conocido como autenticación pregunta-respuesta. Un CAPTCHA te ayuda a protegerte del spam y del descifrado de contraseñas pidiéndote que completes una simple prueba que demuestre que eres humano y no un ordenador que intenta acceder a una cuenta protegida con contraseña.

La prueba de un CAPTCHA consta de dos partes simples: una secuencia de letras o de números generada aleatoriamente que aparece como una imagen distorsionada y un cuadro de texto. Para superar la prueba y probar que eres un ser humano, simplemente tienes que escribir los caracteres que veas en la imagen del cuadro de texto. Los CAPTCHA funcionan porque los ordenadores pueden crear imágenes distorsionadas y procesar una respuesta, pero no pueden leer o solucionar un problema del modo que lo hace un humano para superar la prueba.

4.10.2. SISTEMA DE AUTENTICACION CON DRAG&DROP COMO PRUEBA DE SER HUMANO.

Ya que el esquema de autenticación gráfico propuesto establece que para que una contraseña pueda ser ingresada correctamente el usuario en cuestión de debe arrastrar y soltar una imagen hasta un lugar determinado, esto significaría oprimir el botón del mouse, moverlo hasta la zona definida y soltar el botón, o en el caso de pantallas táctiles mover el dedo por la pantalla hasta el lugar indicado, esto más que nada daría al sistema general la

veracidad de quien esté tratando de entrar es, en esencia un humano, y no una máquina o robot tratando de acceder de forma mecánica.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIÓN

En el presente trabajo se expuso el estado del arte en cuanto al desarrollo de mecanismos de autenticación gráfica, para luego en base a lo aprendido se pudiera desarrollar una nueva propuesta que añadiera un eslabón mas a la cadena de desarrollo de esta alternativa a las contraseñas convencionales.

Se constató que la forma de autenticación mas utilizado es aquel a base de texto, que en este trabajo se considera como el método convencional, luego es seguido por métodos que exigen ciertas características a las contraseñas creadas por el usuario (las cuales hacen que todo el esquema sea mas seguro), por ultimo se encontraron sistemas contraseñas a base de teclados numéricos virtuales en sitios de bancas web.

Lo que continuó con el desarrollo de una propuesta de autenticación a base de imágenes en secuencia como elementos componentes y como secreto compartido con el usuario como prueba de su identidad, el uso del API de Drag&Drop como medio para constituirla en reemplazo del teclado, y de por medio un esquema de encriptación que permitiera no rebelar el valor certero de cada imagen al momento de presentar la interfaz al cliente.

Al realizarse una prueba piloto de la implementación del mecanismo desarrollado, se obtuvieron varios resultados en base a lo experimentado se puede concluir que, el sistema de autenticación con Drag&Drop e Imágenes es en gran medida mucho mas seguro que otros esquemas convencionales, y una gran alternativa como método de logueo seguro para entidades bancarias y otras entidades que precisen de mecanismos de seguridad sofisticados.

Sin embargo, la prueba piloto también dio a entender que a muchos usuarios les podrías llegar a dificultar adaptarse a este nuevo método, de igual manera el análisis y monitorización realizados evidenciaron una carga los dispositivos en los que se implementa, esta es considerable comparándola con lo convencional.

Finalmente, ante cada posible implementación de este esquema, se asegura un alto nivel de seguridad, y ante un buen análisis de costo-beneficio ante cada situación, ambiente, usuarios y recursos, podría representar un gran y beneficioso cambio para el entorno mismo.

RECOMENDACIONES

A aquellas empresas, instituciones o personas que implementen este proyecto se les recomienda realizar pruebas piloto antes de la implementación, y hacer un énfasis en la forma de respuesta que da el servidor usado ante la carga generada por el uso de este método de autenticación.

A los compañeros que deseen tomar este trabajo ampliarlo y profundizarlo, se les recomienda enfatizar en un diseño mas eficaz y ligero para ambos lados, es decir el lado del servidor y el del cliente, una opción podría ser el diseño de imágenes mas ligeras y fáciles de cagar, o la implementación de un algoritmo de encriptación mas liviano.

A la Facultad de Ciencias y Tecnología, que promueva la cultura de innovación entre los alumnos, animándolos a crear nuevos y revolucionarios sistemas, herramientas o dispositivos.

BIBLIOGRAFÍA

[1] R. Biddle, S. Chiasson, y P. C. Van Oorschot, «Graphical passwords: Learning from the first twelve years», *ACM Comput. Surv.*, vol. 44, n.º 4, pp. 1-41, ago. 2012.

[2] A. De Angeli, L. Coventry, G. Johnson, y K. Renaud, «Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems», *Int. J. Hum.-Comput. Stud.*, vol. 63, n.º 1-2, pp. 128-152, jul. 2005.

[3] Department of Computer Science and Engineering, Amity School of Engineering and Technology, Noida, Uttar Pradesh, India y K. Chanda, «Password Security: An Analysis of Password Strengths and Vulnerabilities», *Int. J. Comput. Netw. Inf. Secur.*, vol. 8, n.º 7, pp. 23-30, jul. 2016.

[4] C. J. D. Bogado, *A proposal for a more secure and user-friendly authentication method using HTML5 API Drag&Drop and images: cris-Duarte/Graphical-Password-with-Drag-Drop*. 2018.

[5] R. Hernández Sampieri, C. Fernández Collado, P. Baptista Lucio, S. Méndez Valencia, y C. P. Mendoza Torres, *Metodología de la investigación*. México, D.F.: McGraw-Hill Education, 2014.

[6] M. Tamayo y Tamayo, *El proceso de la investigación científica*. México, D.F.: Editorial Limusa, 2015.

[7] A. Lázaro, J. Asensi, y Pedagogía hoy. Estudios, *Manual de orientación escolar y tutoria*. Madrid: Narcea, 1989.

[8] «Qué es SCRUM», *Proyectos Ágiles*, 04-ago-2008. .

[9] K. E. Kendall y J. E. Kendall, *Análisis y diseño de sistemas*. México: Prentice Hall Hispanoamericana, 1997.

[10] «PHP: ¿Qué es PHP? - Manual». [En línea]. Disponible en:

http://php.net/manual/es/intro-whatis.php. [Accedido: 01-nov-2018].

[11] W. Stallings, *Cryptography and network security: principles and practice*, Seventh edition. Boston: Pearson, 2014.

[12] J. D. Gauchat, *HTML5 para masterminds*. 2012.

[13] «draggable», *Documentación web de MDN*. [En línea]. Disponible en: https://developer.mozilla.org/es/docs/Web/HTML/Atributos_Globales/draggable. [Accedido: 03-nov-2018].

[14] B. Castilho, *Polyfill that enables HTML5 drag drop support on mobile (touch) devices.: Bernardo-Castilho/dragdroptouch*. 2018.

[15] «Bootstrap 4 Get Started». [En línea]. Disponible en: https://www.w3schools.com/bootstrap4/bootstrap_get_started.asp. [Accedido: 06-nov-2018].

[16] «What is a Polyfill?» [En línea]. Disponible en: https://remysharp.com/2010/10/08/what-is-a-polyfill. [Accedido: 05-nov-2018].

[17] «AJAX Introduction». [En línea]. Disponible en: https://www.w3schools.com/xml/ajax_intro.asp. [Accedido: 03-nov-2018].

[18] «JavaScript HTML DOM». [En línea]. Disponible en: https://www.w3schools.com/js/js_htmldom.asp. [Accedido: 05-nov-2018].

[19] *Get control of your servers. Simple. Effective. Awesome! https://my-netdata.io/: netdata/netdata*. netdata, 2018.

[20] «¿Qué es el phishing y cómo evitarlo?» [En línea]. Disponible en: https://www.avast.com/es-es/c-phishing. [Accedido: 11-nov-2018].

[21] «What is a man-in-the-middle attack?» [En línea]. Disponible en: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html. [Accedido: 11-nov-2018].

APÉNDICES

Encuesta:

La encuesta era el objeto al acceder tras el registro y el primer logueo en la Prueba Piloto de Experimentación, y el propósito de esta era determinar si los usuarios consultados mantenían malos hábitos en el uso de sus contraseñas, hay igual de captar su opinión en lo que se refería al sistema de autenticación gráfico de Drag&Drop.

Preguntas:

- ¿En qué ámbito utiliza las contraseñas?
- ¿Está consciente de la importancia que tienen las contraseñas y su adecuado uso?
- Actualmente ¿Cuantas cuentas en redes sociales (Facebook, Instagram, Twitter) o cuentas de correo electrónico tienes activas?
- ¿Alguna vez haz utilizado la misma contraseña para todos los servicios?
- ¿Con qué frecuencia olvidas una contraseña en internet?
- ¿Alguna vez creaste una contraseña a base de información personal? Ya sea nro de cédula, nro de teléfono, fecha de cumpleaños, nombre de familiares o mascotas
- ¿Alguna vez creaste una contraseña a base de patrones numéricos, alfabéticos u otros? Patrones como estos, por ejemplo: 12345678, abcde, abc123, qwerty123, o similares.
- ¿Tiendes a hacer que el navegador guarde tu contraseña?
- ¿Tiendes a guardar tu contraseña en una libreta, agenda o algún otro medio físico?

- Normalmente sitios como Amazon, Ebay y otros hacen que sus usuarios creen contraseñas más seguras según los siguientes requerimientos: Por lo menos 8 caracteres, una mayúscula, una minúscula, un número y un símbolo. Teniendo esto en cuenta, ¿Podrías tú recordar una contraseña como esta t0Esun4#3
- ¿Qué opinas del sistema de contraseñas propuesto?
- ¿Crees que con este método podrás recordar más fácilmente una contraseña?

Respuestas:

- **¿En qué ámbito utiliza las contraseñas?**

Redes Sociales	Correos Electrónicos	Home Banking	Sistemas de Información	Amazon / Ebay	Otros	Tota l
49	43	10	21	15	10	148

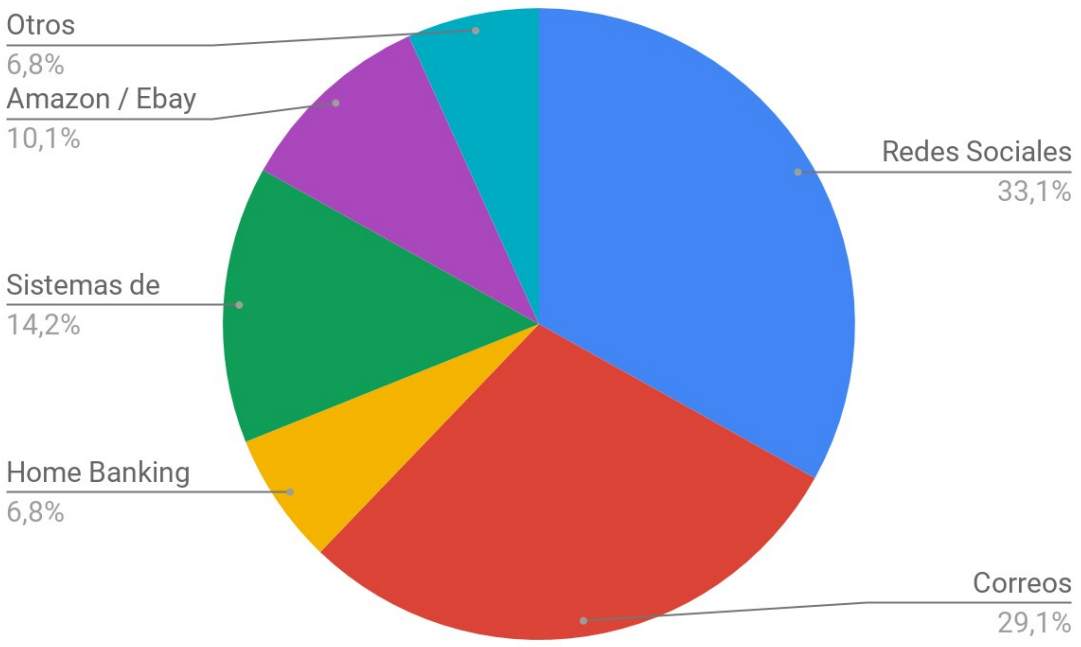


Figura 41: Gráfico, ámbito de uso de las contraseñas

Interpretación de resultado:

Con el resultado obtenido en esta pregunta podemos inferir que hay un bajo número de usuarios que estén sometidos a procesos de autenticación rigurosos o sofisticados, como es el caso de sitios de e-commerce y home banking. Por otro lado, se deduce que usuarios realizan procesos de autenticación seguidamente, ya que la mayoría de ellos poseen cuentas de correo electrónico y/o redes sociales, que son de uso muy frecuente.

- **¿Está consciente de la importancia que tienen las contraseñas y su adecuado uso?**

Si	No	Total
35	19	54

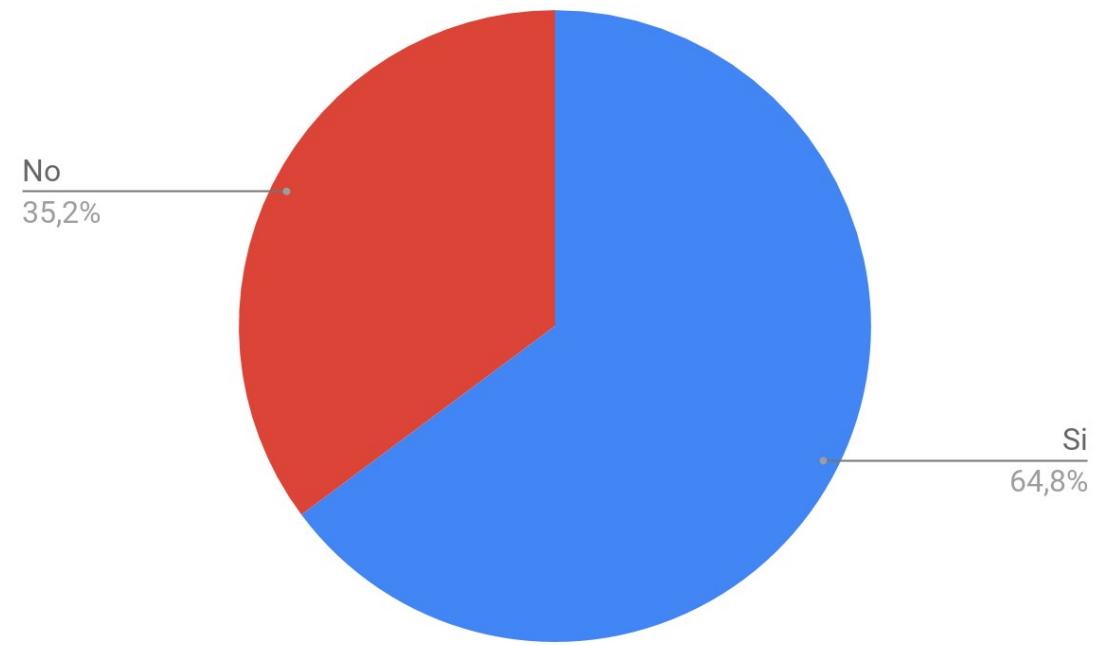


Figura 42: Gráfico, conciencia sobre la importancia y el buen uso de las contraseñas por parte los usuarios

Interpretación de resultado:

De igual manera se observa que los usuarios consultados están conscientes de la importancia de mantener un buen hábito en el uso de las contraseñas.

- **Actualmente ¿Cuantas cuentas en redes sociales (Facebook, Instagram, Twitter) o cuentas de correo electrónico tienes activas?**

Mínimo	Promedio	Máximo
1	5	20

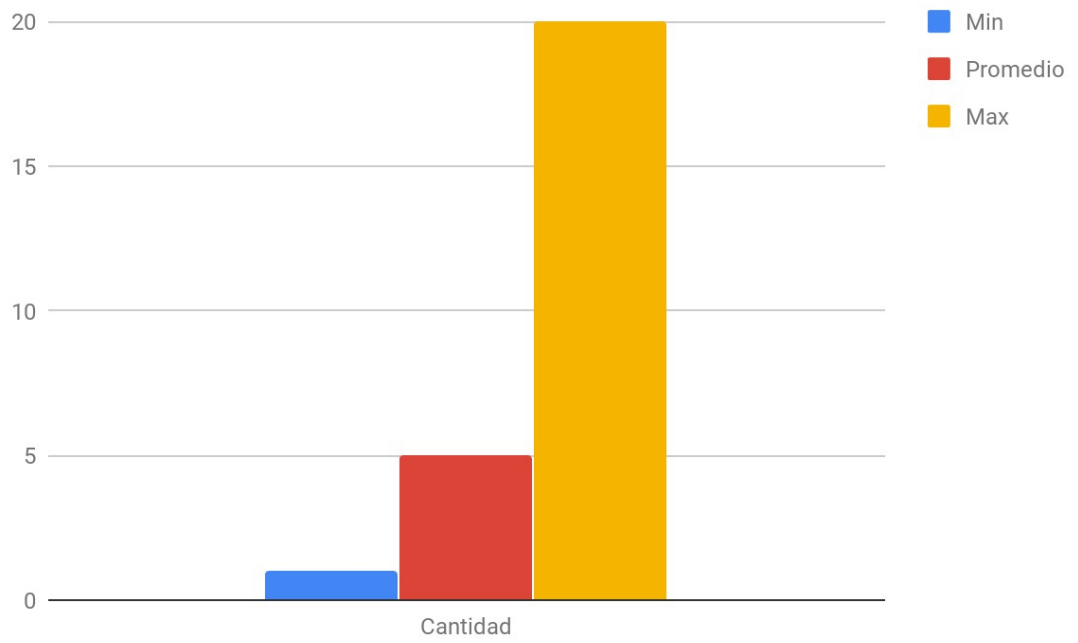


Figura 43: Gráfico, cantidad de cuentas de usuario

Interpretación de resultado:

Al consultarle a los usuarios sobre el número de cuentas de usuario que cuenta (y por ende el número de contraseñas que se le es obligado a recordar), se descubrió que en promedio un usuario mantiene y usa normalmente 5 cuentas, y por ende se infiere que, el usuario promedio debería recordar por lo menos 5 contraseñas distintas.

- **¿Alguna vez haz utilizado la misma contraseña para todos los servicios?**

Si	No	Total

40	12	52

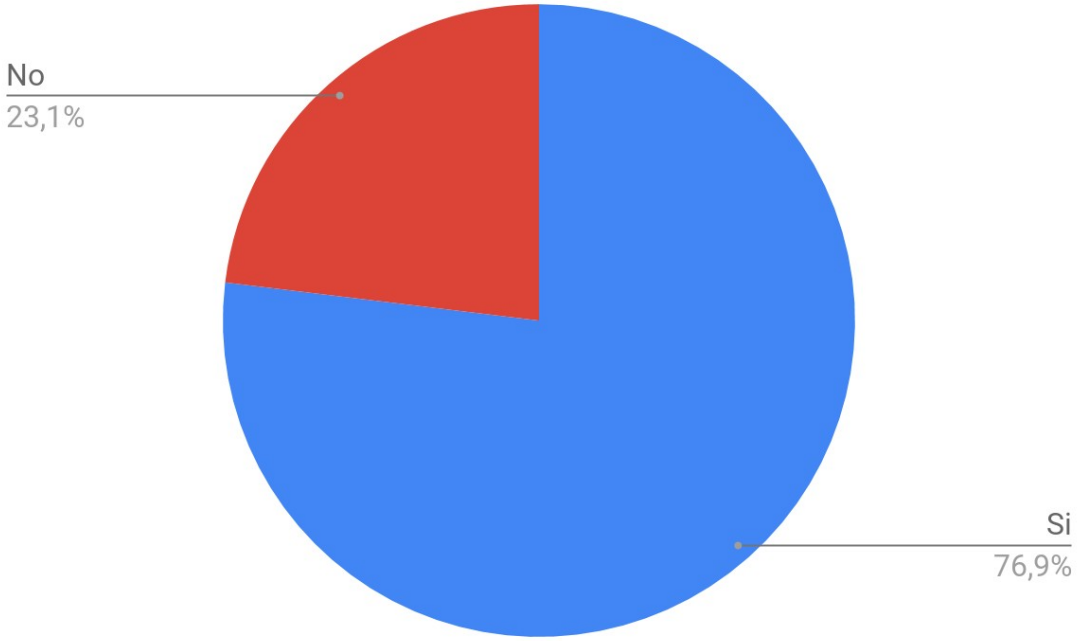


Figura 44: Gráfico, utilización de una contraseña para todas las cuentas de usuario

Interpretación de resultado:

Con el resultado arrojado por esta pregunta, queda demostrado la existencia del mal e inseguro hábito de los usuarios de mantener una sola contraseña para todas las cuentas de usuario que utiliza. Realizando el cruce de información con la pregunta anterior se puede decir que hay una cierta cantidad de usuarios que en promedio mantienen la misma contraseña para 5 cuentas en lineas.

- **¿Con qué frecuencia olvidas una contraseña en internet?**

Nunca	Raramente	Ocasionalmente	A menudo	Muy a menudo	Total
5	20	17	9	1	52

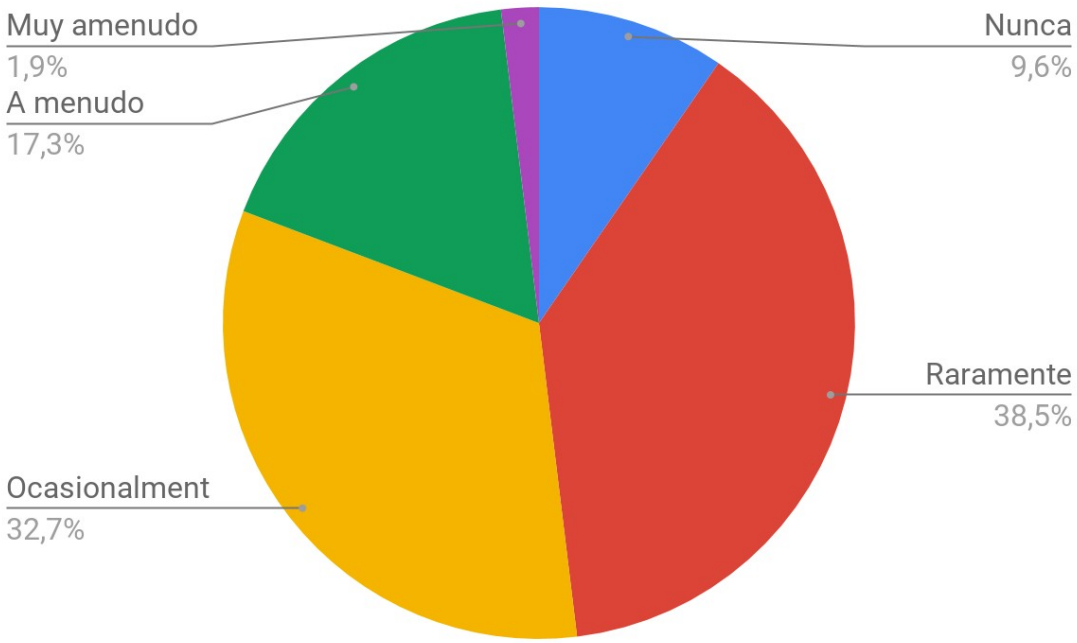


Figura 45: Gráfico, frecuencia de olvido de contraseñas

Las respuestas a esta pregunta se mantuvieron en un rango medio, es decir que las personas consultadas dijeron que ocasionalmente o raramente olvidaban sus contraseñas.

- **¿Alguna vez creaste una contraseña a base de información personal? Ya sea nro de cédula, nro de teléfono, fecha de cumpleaños, nombre de familiares o mascotas.**

Si	No	total
43	9	52

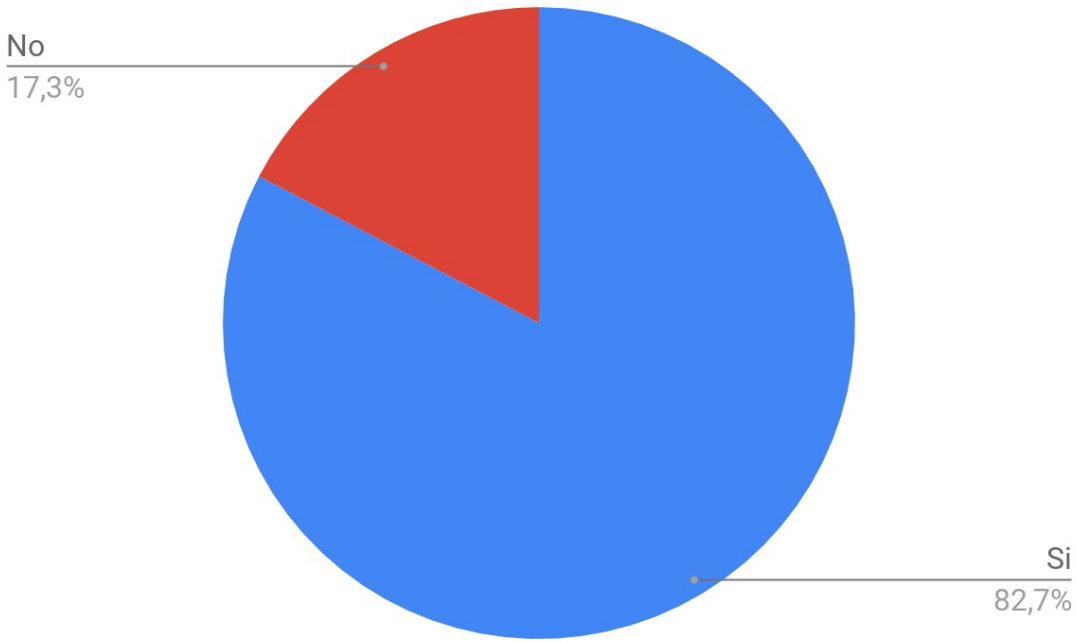


Figura 46: Gráfico, porcentaje creación de contraseñas a base de información personal

Las respuestas a esta pregunta es otra demostración de los malo hábitos de los usuarios en el manejo y uso de las contraseñas, ya que, al conformar sus contraseñas con información personal, esta es fácilmente deducible por personas cercanas a la persona, o por alguien que realice averiguaciones básicas del mismo usuario.

- **¿Alguna vez creaste una contraseña a base de patrones numéricos, alfabéticos u otros? Patrones como estos, por ejemplo: 12345678, abcde, abc123, qwerty123, o similares.**

Si	No	total
28	24	52

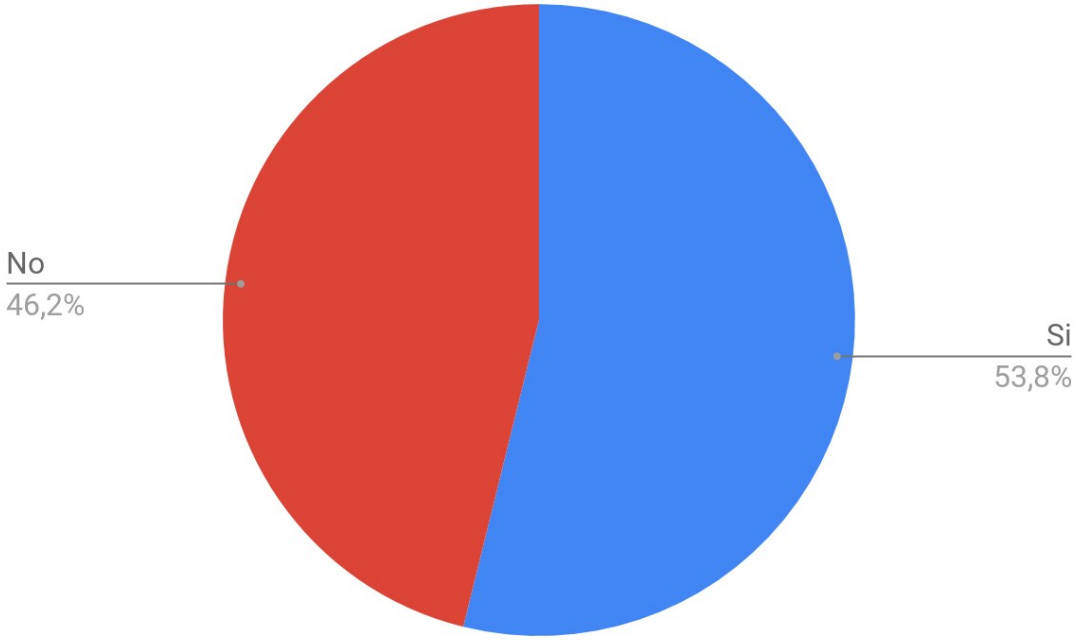


Figura 47: Gráfico, porcentaje creación de contraseñas a base de patrones alfanuméricos

Interpretación de resultado:

Esta pregunta nos da a entender que un poco de más de la mitad de los encuestados usa como contraseñas patrones numéricos o alfabéticos, con la idea de poder recordarla fácilmente, este hábito también representa una vulnerabilidad que muchos atacantes pueden utilizar para hacerse con la contraseña del usuario.

- **¿Tiendes a hacer que el navegador guarde tu contraseña?**

Si	No	total
16	36	52

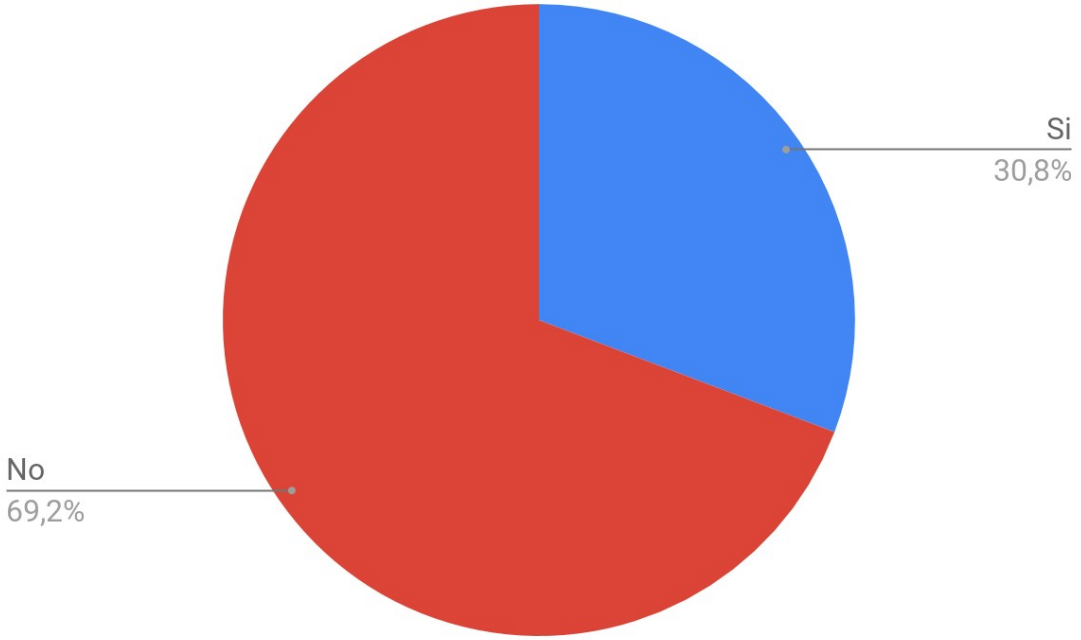


Figura 48: Gráfico, porcentaje creación de contraseñas a base de información personal

Interpretación de resultado:

Las respuestas a esta pregunta nos dan a entender que muchos usuarios prefieren recuperar sus contraseñas por medios propios (tal vez recordarlas) antes que hacer que el navegador desde que se accede guarde y recuerde posteriormente la contraseña en un posterior acceso. Esto significa que la mayoría consultada tiene el buen hábito de no guardar las contraseñas en el dispositivo utilizado.

- **¿Tiendes a guardar tu contraseña en una libreta, agenda o algún otro medio físico?**

Si	No	total
13	39	52

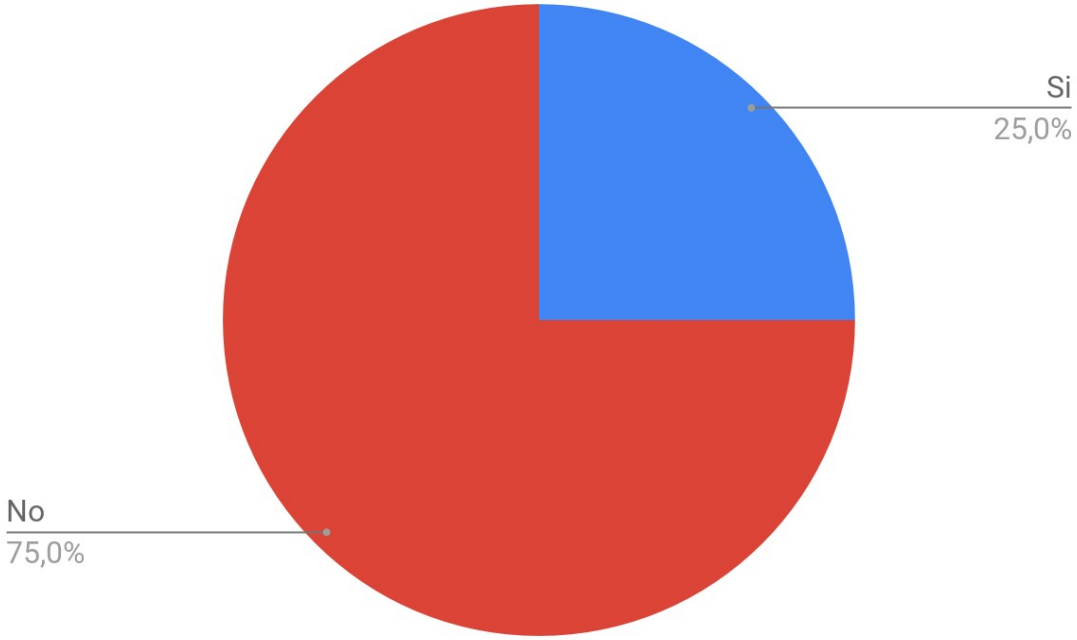


Figura 49: Gráfico, porcentaje usuarios que guardan sus contraseñas en medios físicos

Interpretación de resultado:

De igual manera este resultado nos da a entender que muchos usuarios también toman buenas decisiones en cuanto al uso de sus contraseñas, como el de no mantener todas sus contraseñas anotadas en el mismo medio físico, que al perderla representaría un riesgo grave.

- **Normalmente sitios como Amazon, Ebay y otros hacen que sus usuarios creen contraseñas más seguras según los siguientes requerimientos: Por lo menos 8 caracteres, una mayúscula, una minúscula, un número y un símbolo. Teniendo esto en cuenta, ¿Podrías tú recordar una contraseña como esta t0Esun4#3.**

Definitivamente si	Probablemente si	No estoy seguro	Probablemente no	Definitivamente no	Total
4	15	16	13	4	52

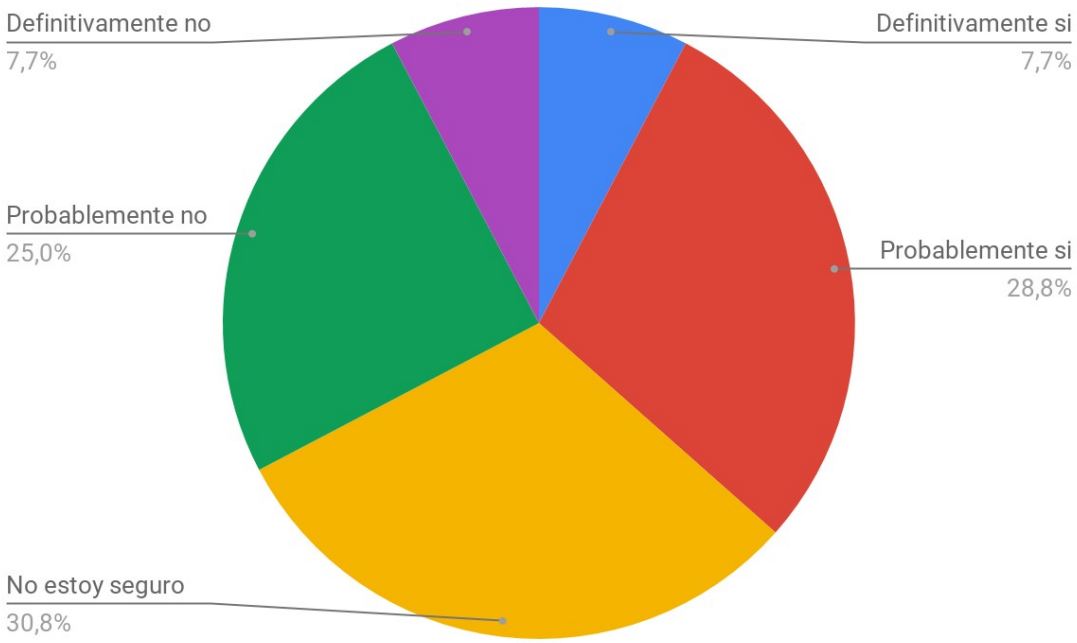


Figura 50: Gráfico, porcentaje de probabilidad de recordación de una contraseña con exigencias de seguridad

Interpretación de resultado:

El propósito de esta pregunta era el de dar una idea de lo propenso que se vería el usuario ante la necesidad de recordar una contraseña con varias exigencias como las de sitios de e-commerce, como se resultado se tuvo que muchos usuarios creen que no les será posible recordar una contraseña como la exigida.

- **¿Crees que con este método podrás recordar más fácilmente una contraseña?**

Definitivamente si?	Probablemente si?	No estoy seguro	Probablemente no	Definitivamente no	Total
12	29	8	3	0	52

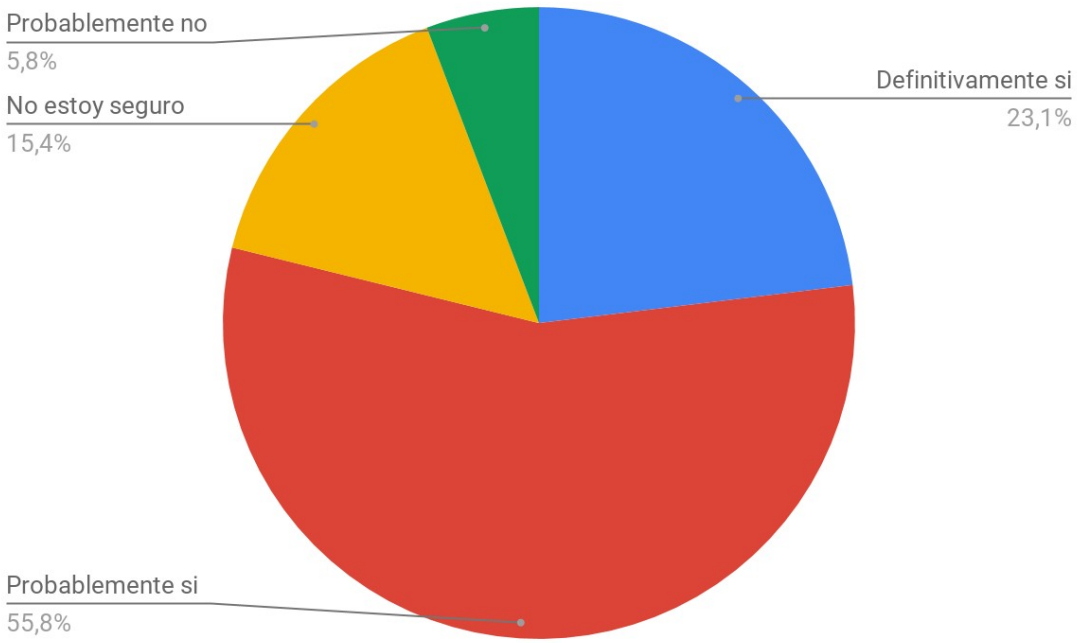


Figura 51: Gráfico, porcentaje de probabilidad de recordación de la contraseña a base de Drag&Drop e Imágenes

Interpretación de resultado:

Esta encuesta también busco saber que tan propenso el usuario se veía así mismo tratando de recordar la contraseña gráfica con Drag&Drop. Como resultado se tuvo que un más de la mitad de los consultados se vio capaz de recordar la contraseña creada con el sistema propuesto.

- **¿Qué opinas del sistema de contraseñas propuesto?**

Por último, se buscó saber la opinión que le merecía el esquema de logueo con Drag&Drop al usuario consultado. En los resultados se puede destacar que la gran mayoría de los consultados considera al Sistema de Autenticación Gráfico Propuesto como muy novedoso e innovador.

De igual manera hubo un número de usuarios que opinaron que por ser un concepto nuevo, les sería algo complicado y difícil poder acostumbrarse al uso del método propuesto y por ende poder recordarla.

ANEXOS

Figura 52: Sistema de autenticación gráfico basado en el dibujo de un patrón solo conocido por el usuario

Figura 53: Sistema de autenticación gráfico basado la marcación de puntos en una imagen

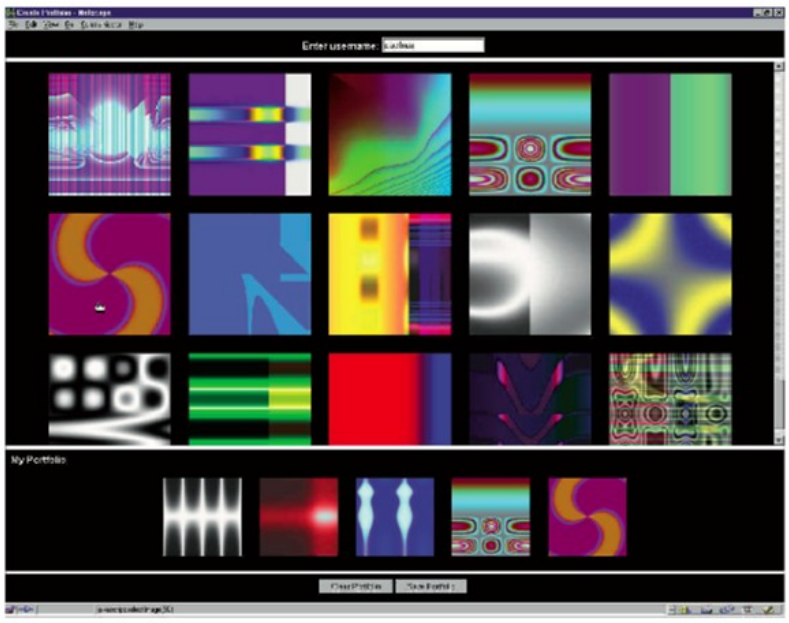


Figura 54: Sistema de autenticación gráfico basado en la elección (por cliqueo) de imágenes en secuencia

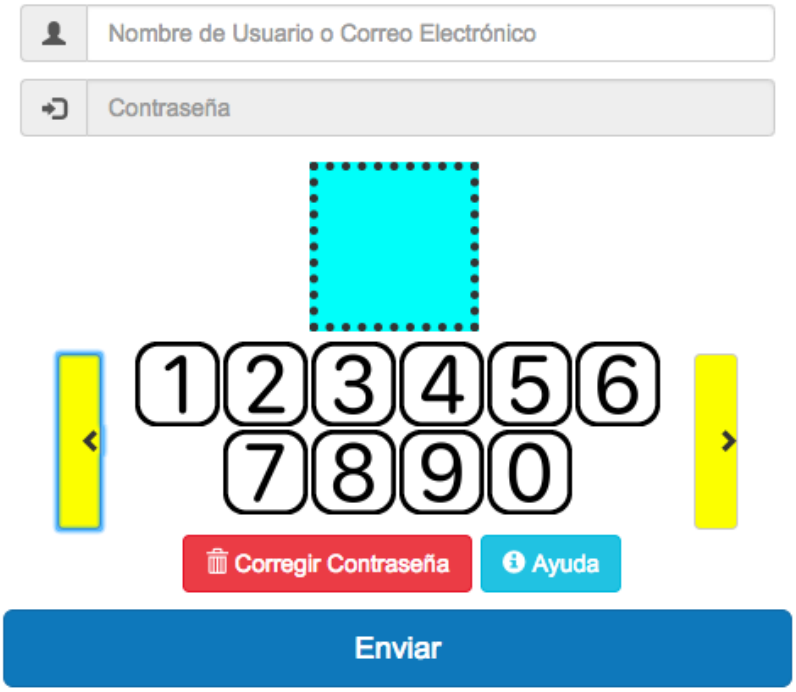


Figura 55: Sistema de autenticación gráfica propuesto

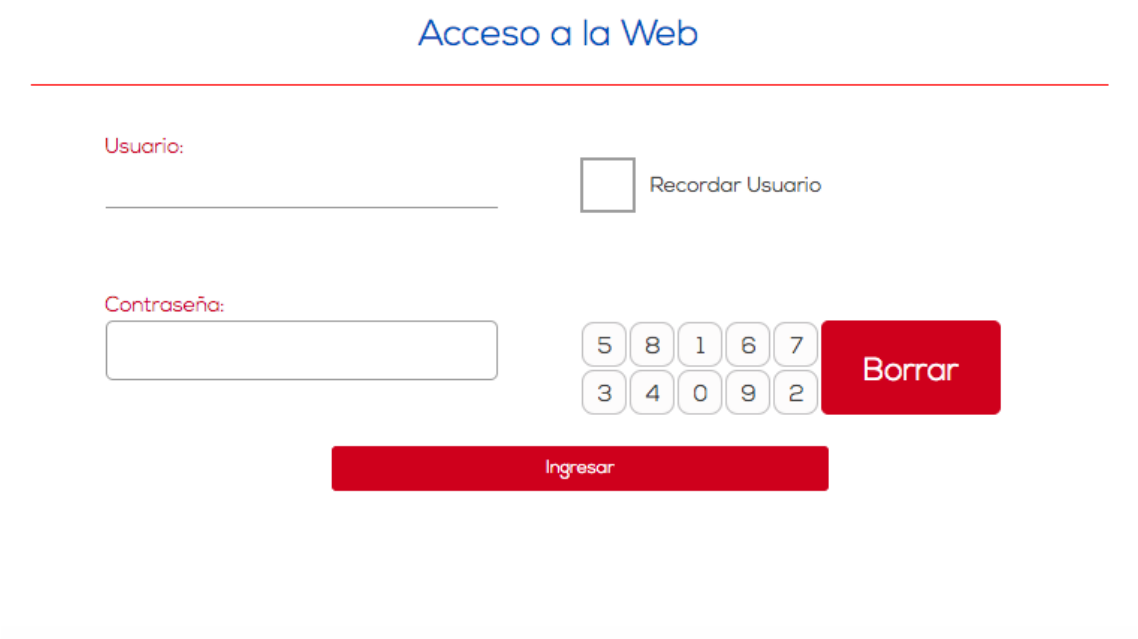


Figura 56: Sistema de autenticación seguro, con un teclado virtual, utilizados en bancas web

GLOSARIO

A

Ajax: La palabra AJAX es acrónimo de **A**synchronous **J**avaScript **A**nd **X**ML, no es un lenguaje de programación, sino que usa una combinación de: Un objeto llamado XMLHttpRequest integrado en el navegador (para solicitar datos de un servidor web), JavaScript y el DOM HTML (para mostrar o usar los datos), AJAX permite que las páginas web se actualicen de forma asíncrona mediante el intercambio de datos con un servidor web entre bastidores. Esto significa que es posible actualizar partes de una página web, sin volver a cargar toda la página

Alfanumérico: Que está formado por letras y números conjuntamente: teclado alfanumérico; cada artículo del almacén queda identificado por una clave alfanumérica.

Análisis: Examen detallado de una cosa para conocer sus características o cualidades, o su estado, y extraer conclusiones, que se realiza separando o considerando por separado las partes que la constituyen: análisis de los derechos y las libertades; análisis diacrónico de la lengua; del análisis se desprende que ambos modelos metafóricos constituyen, en sí mismos, incertidumbre frente a razonamientos que no presentan ninguna salida lógica.

Android: es un sistema operativo basado en el núcleo Linux. Fue diseñado principalmente para dispositivos móviles con pantalla táctil, como teléfonos inteligentes, tabletas y también para relojes inteligentes, televisores y automóviles.

API: La interfaz de programación de aplicaciones, conocida también por la sigla API del inglés application programming interface, es un conjunto de subrutinas,

funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

Apple: es una empresa estadounidense que diseña y produce equipos electrónicos, software y servicios en línea.

Archivo: Conjunto lógico de información o de datos que se designa con un nombre y se configura como una unidad autónoma completa para el sistema o el usuario.

Asimétrica: La asimetría es una propiedad de determinados cuerpos, dibujos, funciones matemáticas y otros tipos de elementos en los que, al aplicarles una regla de transformación efectiva, se observan cambios respecto al elemento original.

Autenticación: Procedimiento informático que permite asegurar que un usuario de un sitio web u otro servicio similar es auténtico o quien dice ser.

Autoría: Cualidad o condición de autor, especialmente de una obra literaria, científica o artística: los derechos de autoría.

B

Backend: relacionado con o que denota la parte de un sistema informático o aplicación a la que el usuario no accede directamente, generalmente es responsable de almacenar y manipular datos.

Biometría: estudio para el reconocimiento inequívoco de personas basado en uno o más rasgos conductuales o físicos intrínsecos.

Bootstrap: es una biblioteca multiplataforma o conjunto de herramientas de código abierto para diseño de sitios y aplicaciones web.

C

Captcha: son las siglas de Completely Automated Public Turing test to tell Computers and Humans Apart (prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos). Este test es controlado por una máquina, en lugar de por un humano como en la prueba de Turing.

Caracteres: es una secuencia ordenada (de longitud arbitraria, aunque finita) de elementos que pertenecen a un cierto lenguaje formal o alfabeto análogas a una fórmula o a una oración.

Ciberseguridad: es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.

Cifrar: Escribir un mensaje en clave mediante un sistema de signos formado por números, letras, símbolos, etc.

Codificación: método que permite convertir un carácter de un lenguaje natural (como el de un alfabeto o silabario) en un símbolo de otro sistema de representación, como un número o una secuencia de pulsos eléctricos en un sistema electrónico.

Contraseñas: o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.

Criptografía: arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

CSS: (siglas en inglés de Cascading Style Sheets), en español "Hojas de estilo en cascada", es un lenguaje de diseño gráfico para definir y crear la

presentación de un documento estructurado escrito en un lenguaje de marcado.

D

Descifrar: Descubrir el significado de un mensaje escrito en clave o en código desconocido.

Desencriptación: es un conjunto de técnicas de análisis de códigos que permite conocer e interpretar toda o parte de la información expresada mediante un código desconocido (es decir, un código cuyas reglas de codificación convencionales son desconocidas).

DOM: es un modelo de objeto estándar y una interfaz de programación para HTML.

Drag&Drop: Traducido sería “Arrastrar y Soltar”, en las interfaces gráficas de usuario, arrastrar y soltar es un gesto del dispositivo señalador en el que el usuario selecciona un objeto virtual al "agarrarlo" y arrastrarlo a una ubicación diferente o a otro objeto virtual.

Draggable: es un atributo global enumerado, que indica si el elemento puede ser arrastrado, usando el HTML Drag and Drop API.

Droppable: Un componente en el que el usuario puede arrastrar otros elementos, como también atributo que lo indica.

E

E-commerce: El comercio electrónico, también conocido como e-commerce o bien comercio por Internet o comercio en línea, consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como redes sociales y otras páginas web.

Emojis: es un término japonés para los ideogramas o caracteres usados en mensajes electrónicos y sitios web. El término es una palabra compuesta que significa lo siguiente: imagen + adaptada al español como “emoyi”.

Encriptación: En criptografía, es un procedimiento que utiliza un algoritmo de cifrado con cierta clave para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta del algoritmo.

Escalable: A un sistema cuyo rendimiento es mejorado después de haberle añadido más capacidad hardware/software, proporcionalmente a la capacidad añadida, se dice que pasa a ser un sistema escalable.

F

Frontend: en relación o que denota la parte de un sistema informático o aplicación con la que el usuario interactúa directamente.

H

Hash: es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

Híbrida: Que es producto de la combinación de elementos de distinta naturaleza.

HTML: es un lenguaje de programación que se utiliza para el desarrollo de páginas de Internet. Se trata de las siglas que corresponden a HyperText Markup Language, es decir, “Lenguaje de Marcas de Hipertexto”.

I

IOS: es un sistema operativo móvil de la multinacional Apple Inc. Originalmente desarrollado para el iPhone, después se ha usado en dispositivos como el iPod touch y el iPad.

Internet: es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP.

J

Javascript: es un lenguaje de programación interpretado, dialecto del estándar ECMAScript. Se define como orientado a objetos, basado en prototipos, imperativo, débilmente tipado y dinámico.

K

Keyloggers: Los keyloggers realizan un seguimiento y registran cada tecla que se pulsa en una computadora, a menudo sin el permiso ni el conocimiento del usuario.

L

Licencia: Una licencia de software es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribución) y el licenciatario (usuario consumidor, profesional o empresa) del programa informático, para utilizarlo cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas, es decir, es un conjunto de permisos que un desarrollador le puede otorgar a un usuario en los que tiene la posibilidad de distribuir, usar o modificar el producto bajo una licencia determinada.

Logueo: es el proceso mediante el cual un usuario accede a sus distintas cuentas informáticas, este tipo de proceso suele ir acompañado primero de un previo registro y segundo por el ingreso de un nickname o ID de usuario y una contraseña o password.

M

Malware: El término se utiliza para hablar de todo tipo de amenazas informáticas o software hostil.

MITM: Un ataque de hombre en el medio interfieren tres elementos, la víctima, la entidad con la que la víctima está tratando de comunicarse y el "hombre en el medio", que está interceptando las comunicaciones de la víctima.

Móvil: es un dispositivo inalámbrico electrónico que permite tener acceso a la red de telefonía celular o móvil.

N

Netdata: es un software utilitario que permite monitorizar en tiempo real, el rendimiento y el estado de los sistemas y aplicaciones en un servidor.

O

Openssl: es un kit de herramientas robusto, de grado comercial y con todas las funciones para los protocolos de Seguridad de la capa de transporte (TLS) y de Capa de sockets seguros (SSL).

P

Phishing: es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias.

PHP: es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML.

PIN: es un número de identificación personal utilizado en ciertos sistemas, como el teléfono móvil o el cajero automático, para identificarse y obtener acceso al sistema. El PIN es un tipo de contraseña. Sólo la persona

beneficiaria del servicio conoce el PIN que le da acceso al mismo; esa es su finalidad.

Polyfill: es un fragmento de código (o complemento) que proporciona la tecnología que el desarrollador, espera que el navegador proporcione de forma nativa.

Prototipo: primer ejemplar que se fabrica de una figura, un invento u otra cosa, y que sirve de modelo para fabricar otras iguales, o molde original con el que se fabrica.

R

Reconocimiento: es la acción de distinguir a una cosa, entre las demás como consecuencia de sus características y rasgos.

S

Scrum: es un proceso en el que se aplican de manera regular un conjunto de buenas prácticas para trabajar colaborativamente, en equipo, y obtener el mejor resultado posible de un proyecto.

Simétrica: es un rasgo característico de sistemas, ecuaciones o entidades abstractas, relacionada con su invariancia bajo ciertas transformaciones, movimientos o intercambios.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Susceptibles: indica la probabilidad que algo suceda, está vinculado a aquello capaz de ser modificado o de recibir impresión por algo o alguien.

T

Tablet: también denominada tableta en muchos lugares es una computadora portátil de mayor tamaño que un teléfono inteligente.

Touch: es una pantalla que mediante un toque directo sobre su superficie permite la entrada de datos y órdenes al dispositivo, y a su vez muestra los resultados introducidos previamente.

Tokens: Un token de seguridad es un aparato electrónico que se le da a un usuario autorizado de un servicio.

U

Usabilidad: Cualidad de la página web o del programa informático que son sencillos de usar porque facilitan la lectura de los textos, descargan rápidamente la información y presentan funciones y menús sencillos, por lo que el usuario encuentra satisfechas sus consultas y cómodo su uso.

Usuario: persona que utiliza una computadora o sistema informático.

W

Web: conjunto de información que se encuentra en una dirección determinada de internet.