ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

CREACIÓN DE UN PROTOTIPO DE SISTEMA DE ONE-TIME PASSWORD (OTP) PARA UN SISTEMA DE AUTENTICACIÓN DE DOS FACTORES.

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO/A EN CIENCIAS DE LA COMPUTACIÓN

IMPLEMENTACIÓN DE UN PROTOTIPO DE SISTEMA GENERADOR OTP BASADO EN HOTP Y ENVIO POR CORREO ELECTRONICO.

HILTON BLADIMIR PILLAJO ANAGUANO

hilton.pillajo@epn.edu.ec

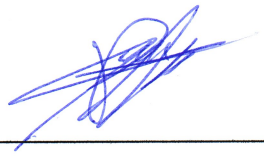
DIRECTOR: PHD. SANG GUUN YOO

sang.yoo@epn.edu.ec

QUITO, febrero 2023

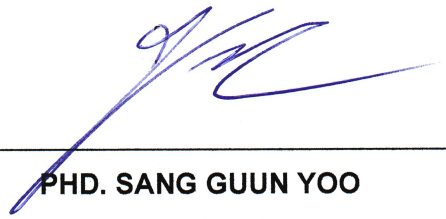
CERTIFICACIONES

Yo, Hilton Bladimir Pillajo Anaguano declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.



Hilton Bladimir Pillajo Anaguano

Certifico que el presente trabajo de integración curricular fue desarrollado por Hilton Bladimir Pillajo Anaguano, bajo mi supervisión.



PHD. SANG GUUN YOO

DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

HILTON BLADIMIR PILLAJO ANAGUANO

PHD. SANG GUUN YOO

LUIS ERNESTO ALMEIDA ZAMBRANO

BRAYAN ALEXIS FERNÁNDEZ GONZA

DALIANA ZAMBRANO PEREDA

ANTHONY ISRAEL ALMACHI CHASI

DEDICATORIA

El desarrollo del presente trabajo va dedicado a mi familia Milton Pillajo, Gloria Anaguano, Susana Anaguano, Alex Anaguano, por todo el apoyo que me han brindado en mi vida y que nunca permitieron que me rinda y siga luchando por buscar este sueño que he tenido desde niño.

A mis hermanos Marlon Pillajo y Milene Pillajo, que me acompañaban en los trasnoches de mi vida universitaria, apoyándome y alentándome a ser una mejor versión de mí.

A mis tíos, primos y amigos que me supieron dar un buen concejo o simplemente preguntar cómo te va en la universidad, hacerme sentir que puedo lograrlo y saber que cuento con su apoyo.

Bladimir Pillajo

AGRADECIMIENTO

El agradecimiento es totalmente hacia Dios quien me ha dado el don y talento para estudiar, quien ha sido mi refugio en los momentos más difíciles de mi vida, siempre cuido y protegió a mi familia, además de permitirme estudiar en la mejor Universidad de Ecuador, la Escuela Politécnica Nacional.

Agradezco a mi abuelita y mis padres, por el apoyo incondicional que me dan, por su amor, por sus concejos para salir siempre adelante y ayudarme a cumplir mis metas.

A mis tíos, primos y amigos, les agradezco que se preocupaban por mi cada semestre, que me alentaban y creían en mí.

A la Escuela Politécnica Nacional por brindarme la oportunidad de cursar mi carrera en la Facultad de Ingeniería en Sistemas, donde viví y compartí grandes momentos de mi vida, a cada uno de los docentes que compartieron sus experiencias y conocimientos para mi desempeño profesional.

Bladimir Pillajo

ÍNDICE DE CONTENIDO

RESUMEN

Con el desarrollo y avance tecnológico que se tiene anualmente en el campo de la informática es cada vez más común que las personas mediante sus teléfonos móviles inteligentes o computadores personales ingresen a páginas web y se registren en alguna página de su agrado, sin tener en cuenta la seguridad de su información personal, ya que pueden ser víctimas de los ciberdelincuentes y estos a su vez tener el acceso a su información, lo que como usuarios nos exponemos, teniendo mayor riesgo de suplantación de nuestra identidad.

Este trabajo maneja los conceptos de seguridad informática, de esta manera al tener claro estos conceptos se asociará de claramente al tema principal de este trabajo, el cual es la creación de un prototipo de un doble factor de autenticación utilizando contraseñas de un solo uso como una solución para evitar el acceso no deseado por ciberdelincuentes y la suplantación de identidad.

Para el desarrollo de este trabajo se enfoca en generar, enviar, verificar que la contraseña generada por un generador de contraseñas de un solo uso HMAC-Based One-Time Password (HOTP), esta contraseña se enviará mediante correo electrónico al usuario registrado y el sistema validará que contraseña generada es la correcta, permitiendo al usuario su autenticación y sea quien dice ser, así el sistema permite el acceso a la web desarrollada.

Este prototipo de sistema de doble factor de autenticación mediante correo electrónico utilizará la contraseña del usuario y un código de verificación enviado al correo electrónico como factores de autenticación. El sistema ayudará a aumentar la seguridad de la cuenta del usuario y garantizará que solo el usuario registrado tenga acceso, cabe mencionar que el prototipo se lo realizará de manera local.

PALABRAS CLAVE: Seguridad Informática, HOTP, doble factor de autenticación, contraseñas de un solo uso, encriptación.

ABSTRACT

With the development and technological advances that occur annually in the field of information technology, it is increasingly common for people through their smart mobile phones or personal computers to enter web pages and register on a page of their liking, without taking into account the security of your personal information, since they can be victims of cybercriminals and these in turn have access to your information, which as users we expose ourselves, having a greater risk of impersonation of our identity.

This work handles the concepts of computer security, in this way, by being clear about these concepts, it will be clearly associated with the main theme of this work, which is the creation of a prototype of a double authentication factor using one-time passwords as a solution to prevent unwanted access by cybercriminals and identity theft.

For the development of this work, it focuses on generating, sending, verifying that the password generated by a one-time password generator HMAC-Based One-Time Password (HOTP), this password will be sent by email to the registered user and the The system will validate that the generated password is correct, allowing the user to authenticate and be who they say they are, thus the system allows access to the developed website.

This prototype two-factor email authentication system will use the user's password and a verification code sent to the email as authentication factors. The system will help increase the security of the user's account and guarantee that only the registered user has access, it is worth mentioning that the prototype will be made locally.

KEYWORDS: Computer Security, HOTP, double authentication factor, one-time passwords, encryption.

1. DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

Sin duda alguna, el hoy se vive en un mundo tecnológico y la seguridad en la informática se ha considerado de gran importancia en áreas tecnológicas como: Internet de las cosas (IoT) [1], redes [2], desarrollo de software [3], etc. Cada área tecnológica genera información que se la debe proteger de manera que sea segura y eficaz [4]

Y una manera de proteger la información de un sistema informático es mediante un proceso de autenticación, el cual establece la confianza entre el usuario y el dispositivo, con el objetivo de comprobar que el usuario sea quien dice ser [5], [6]. Desde el nacimiento del Internet, el método de autenticación común fue: un identificador de nombre de usuario combinado con una contraseña [7]. En la actualidad con el avance de la Internet, los usuarios están expuestos al robo de las credenciales personales y se ha convertido en un problema importante de seguridad [8]

Ante esta situación, se ha popularizado la autenticación basada en un doble factor de autenticación (2FA), ya que genera un nivel más elevado de seguridad [9].

El NIST [10] define tres factores básicos en una autenticación estándar:

“Algo que el usuario sabe”, como puede ser una contraseña.

“Algo que el usuario tiene”, como puede ser una clave criptográfica o un identificador.

“Algo que el usuario es”, como puede ser una huella dactilar, el iris u otro dato biométrico.

La ventaja de usar varios factores es que la seguridad es mantenida en caso de que uno de ellos se vea comprometido [9]. Muchos sistemas como aplicaciones de banca en línea, plataformas de registros de asistencias, área de la salud, IoT hacen uso del 2FA y estos programas utilizan algoritmos de contraseñas de un solo uso One-Time Password (OTP).

El OTP es considerado una de las formas más simples y populares de implementar una capa extra de seguridad en el 2FA [11], ya que esta solución genera una secuencia de contraseñas basadas en factores como: nombre, hora y semilla, además tienen las características de ser impredecibles e irreversibles y son fundamentales para la seguridad de los sistemas que los emplean [11].

Este trabajo consiste en realizar un prototipo de sistema de doble autenticación de manera local, mediante un generador de contraseñas OTP que pueda ser utilizado una sola vez y esta contraseña se lo enviará al usuario mediante un correo electrónico. De esta manera si un intruso conoce la contraseña que se generó, no podrá acceder al contenido o

información, ya que esta clave no volverá a ser válida debido a que será una contraseña de un solo uso (OTP).

1.1 Objetivo general

Crear un prototipo de un sistema de autenticación de dos factores One-Time Password.

1.2 Objetivos específicos

1. Entender el estado del arte para conocer sobre el sistema de autenticación de dos factores.
2. Crear un prototipo de un sistema de doble factor de autenticación.
3. Verificar el funcionamiento correcto del prototipo creado.

1.3 Alcance

El alcance del proyecto consiste en seis etapas: (1) Estudio de la literatura, (2) Análisis del protocolo OTP, (3) Análisis y diseño del prototipo, (4) Desarrollo del prototipo, (5) Desarrollo de las pruebas del prototipo y (6) Documentación.

En las etapas del 2 al 5 se utilizará la Metodología de prototipo, ya que permite el desarrollo del plan de trabajo de forma progresiva hasta alcanzar el objetivo esperado.

El proyecto empieza con la fase del Estudio de la literatura, en donde se plantea una revisión de los protocolos de OTP que existen y que soluciones proponen.

En la segunda fase, se realizará el Análisis del protocolo de OTP a usar, junto con el método de entrega.

En la tercera fase, se realizará el Análisis y diseño del prototipo. Se definirá y se realizará el diseño de un Mockup de alto nivel. Además, se seleccionarán lenguajes de programación, entornos de desarrollo, entre otros, para diseñar la arquitectura a implementar en la creación del prototipo.

En la cuarta fase, se realizará el Desarrollo del prototipo. Se iniciará con la creación de las interfaces de usuario basados en el mockup de alto nivel desarrollado en la fase anterior.

En la quinta fase, se llevará a cabo el Desarrollo de las pruebas del prototipo.

Por último, en la sexta fase se realizará el desarrollo de la Documentación, que incluye resultados y conclusiones.

1.4 Marco teórico

En la era digital en la cual se vive, todo dispositivo electrónico inteligente puede almacenar información, por tal motivo es necesario utilizar contraseñas de inicio de sesión robustas y brindar una seguridad extra con una única contraseña [4], es decir, utilizar factores de autenticación que permitan demostrar que es el mismo usuario y no puedan acceder sin autorización a la información, sistema informático o aplicación.

Además, en esta sección se desarrollan los conceptos sobre seguridad informática, autenticación, identificación, autorización, 2FA, One-Time Password (OTP), HMAC-Based One-Time Password Protocol (HOTP), criptografía y método de entrega.

Seguridad Informática

El concepto de seguridad informática se encontraba anteriormente más relacionado con la confianza, mientras hoy en día se relaciona con la responsabilidad de proteger [12]

Este cambio data en la década de los 70s, donde las empresas se centraban en garantizar el buen uso de la información, teniendo inconvenientes en su momento por la poca información de riesgos, falta de copias de seguridad o medidas físicas inexistentes [13]

En la década de los 80s, con la aparición de los virus se vieron vulnerables los ordenadores, llevando a cabo la comercialización de antivirus y así brindar seguridad a los ordenadores [4]

En la década de los 90s, empiezan los ataques por internet y la preocupación por brindar seguridad, protección de la red.

En los años 2000, empiezan los ataques corporativos y la preocupación de brindar protección a los datos.

A partir del 2010 hasta la actualidad (2023), se toma conciencia de brindar seguridad a dispositivos móviles, ordenadores, servidores, redes y evitar la pérdida de información corporativa y personal [13]

Mediante esta reseña histórica, la seguridad informática se encarga de proteger redes, ordenadores, datos con medidas de seguridad adecuadas, además de ir evolucionando con el paso del tiempo.

Identificación

Es el momento en el cual el usuario se da a conocer dentro de un sistema, este proceso se lo utiliza para distinguir a un usuario de otro en un sistema o aplicación que se esté ejecutando [14]. El termino identificación se confunde con autenticación, pero la diferencia es cuando el sistema valida al usuario quien realmente es, ahí es cuando se está identificando.

Un usuario se puede identificar con un nombre, huellas digitales, ADN, tarjetas, números de cuenta, etc. y estos métodos de identificación no son únicos lo que conlleva a que pueden ser falsificados, por eso no se debe de considerar como confiable solo a la afirmación de una identidad [15]

Autenticación

El concepto de autenticación está relacionado con la seguridad informática, ya que es un acto a proceso de confirmar que un usuario es quien dice ser, que valida como legitima la identidad del usuario [16]. En la actualidad como usuarios nos autenticamos muchas veces en un día, con la tarjeta de crédito al pagar e ingresar el código el PIN (Personal Identification Number) nos estamos autenticando [17].

El proceso de autenticación es:

- El usuario solicita acceso al sistema.
- El sistema o aplicación solicita al usuario que se autentique.
- El usuario ingresa las credenciales que le identifican y permiten verificar la autenticidad de la identificación.
- El sistema valida las credenciales según sus reglas y permitirá el acceso o no al usuario.

Autorización

La autorización es el paso siguiente de la identificación y autenticación, es decir es la validación que determina lo que el usuario puede hacer, permitiendo o bloqueando el acceso a un recurso.

Figura 1. Identificación, Autenticación y Autorización.

En la Figura 1, se observa la secuencia de los sucesos que suceden cuando el usuario se autentica para tener acceso a un recurso [16].

Doble Factor de Autenticación (2FA)

Con la autenticación mediante el nombre del usuario y contraseña es lo más común en sistemas o aplicaciones en la actualidad, pero esta manera de autenticarse tiene una gran brecha de seguridad, sea por contraseñas no lo suficientemente robustas, contraseñas repetidas, suplantación de identidad, ataques de ingeniería social, software que comprueba millones de combinaciones en segundos se han buscado nuevas formas en que los usuarios se autentiquen de forma rápida y segura [4].

Y una solución es el doble factor de autenticación o autenticación de dos factores que se ha convertido en un estándar de seguridad en la internet [18] y genera un nivel elevado de seguridad [19].

El doble factor de autenticación verifica la identidad del usuario combinando dos de los tres factores universales de autenticación [20], los cuales son [10]:

“Algo que el usuario sabe”, como puede ser una contraseña.

“Algo que el usuario tiene”, como puede ser una clave criptográfica o un identificador.

“Algo que el usuario es”, como puede ser una huella dactilar, el iris u otro dato biométrico.

One Time Password (OTP)

El primer OTP fue propuesto por Leslie Lamport [21] a principio de los 80s y es conocido como un sistema de autenticación S/KEY [22]. Su objetivo de implementación radicó en lograr el proceso de autenticación en computadoras de uso público que no fueran de confianza [23].

El OTP es considerado una forma simple de implementar una capa extra de seguridad en el doble factor de autenticación. Esta solución genera una secuencia de contraseñas

basada en factores como nombre, hora y tiene la característica de ser impredecible e irreversible [11]. El OTP es una alternativa más segura en un proceso de autenticación de multifactor, si un atacante llegase a obtener esta contraseña, el atacante no podrá utilizar y hacer un segundo intento, quedando el usuario protegido si sus credenciales estuviesen comprometidas.

HMAC-Based One-Time Password Protocol (HOTP)

HOTP es un algoritmo de contraseña de un solo y fue creado en 2005, este algoritmo genera valores basados en códigos de autenticación de mensajes hash (HMAC), que es un código de autenticación de mensajes (MAC) basado en funciones hash criptográficas (por ejemplo, MD5, SHA-1, etc.) [24]

HMAC se utiliza para crear el valor HOTP. El algoritmo HOTP funciona en base a un valor de contador creciente (C) y una clave simétrica estática (K) conocida solo por el token y el servicio de validación [25].

Las funciones de hashing criptográfico tienen la particularidad de devolver una única salida [26]. Por lo tanto, cada vez que se aplica hash a la misma entrada, se debe devolver la misma salida hash. Además, las funciones hash también se conocen como funciones "unidireccionales" porque con cada entrada diferente se obtiene una salida única, pero teniendo solo la salida hash no es posible obtener la entrada. A pesar de la longitud de la entrada, las funciones hash suelen generar resultados hash de longitud fija, que suelen oscilar entre 128 y 256 bits [25].

2. METODOLOGÍA

Este trabajo se encuentra orientado a desarrollar un prototipo de un sistema de doble autenticación y la metodología a utilizar va a ser la de prototipo, ya que esta metodología está relacionada con una mejora continua y cada proceso iterativo está enfocado en diseñar, implementar, medir y ajustarse a un plan de trabajo[27].

Esta metodología se la aplica las siguientes etapas:

- Definir los requerimientos.
- Definir las herramientas a utilizar.
- Diseñar el prototipo.
- Testear el prototipo.
- Análisis de resultados.

Es necesario indicar que nuestro proyecto consiste únicamente en la creación de un prototipo de un sistema de One-Time Password (OTP) para un sistema de autenticación de dos factores y no en un sistema que será implementado en un ambiente real.

Se seleccionarán tres protocolos de OTP, los cuales serán implementados por Luis Ernesto Almeida Zambrano, Brayan Alexis Fernández Gonza y Hilton Bladimir Pillajo Anaguano, respectivamente. Mientras que cada uno del resto de los estudiantes Daliana Zambrano Pereda y Anthony Israel Almachi Chasi, se encargará del desarrollo de un prototipo de aplicación móvil (uno cada uno), donde se ingresarán los códigos OTP generados con la finalidad de realizar el proceso de autenticación.

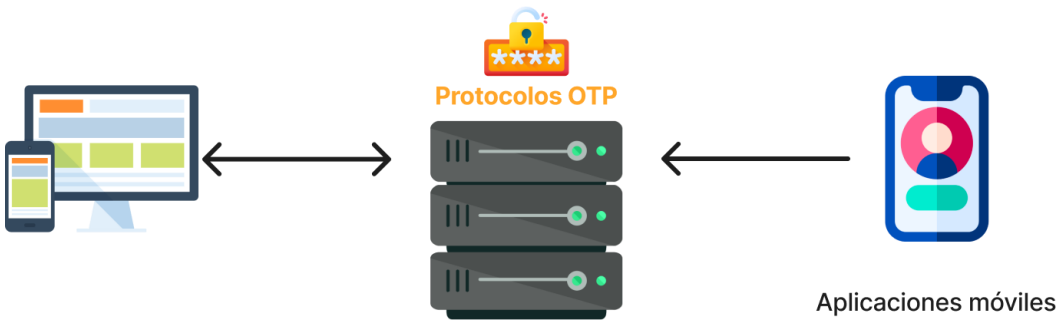


Figura 2. Arquitectura preliminar del prototipo a ser desarrollada

Con el sistema total a desarrollar el presente trabajo se basa en desarrollar un algoritmo de generación de contraseñas de un solo uso HOTP, además de un método de entrega

(correo electrónico) de la contraseña generada, también contar con las interfaces gráficas para el usuario final y con la parte desarrollada de cada estudiante se va realizar un solo prototipo.

2.1 Requerimientos

Los requerimientos para el desarrollo del trabajo se muestran en la Figura 3, se va realizar mediante la implementación de una página web de autenticación (Login), donde el usuario ingresa sus credenciales y se lo solicitará que ingrese el código único el cual se va a generar y se enviará al correo del usuario, permitiéndole el ingreso.

Para esto se va a utilizar NodeJS, Posgresql, ExpressJS y Python.

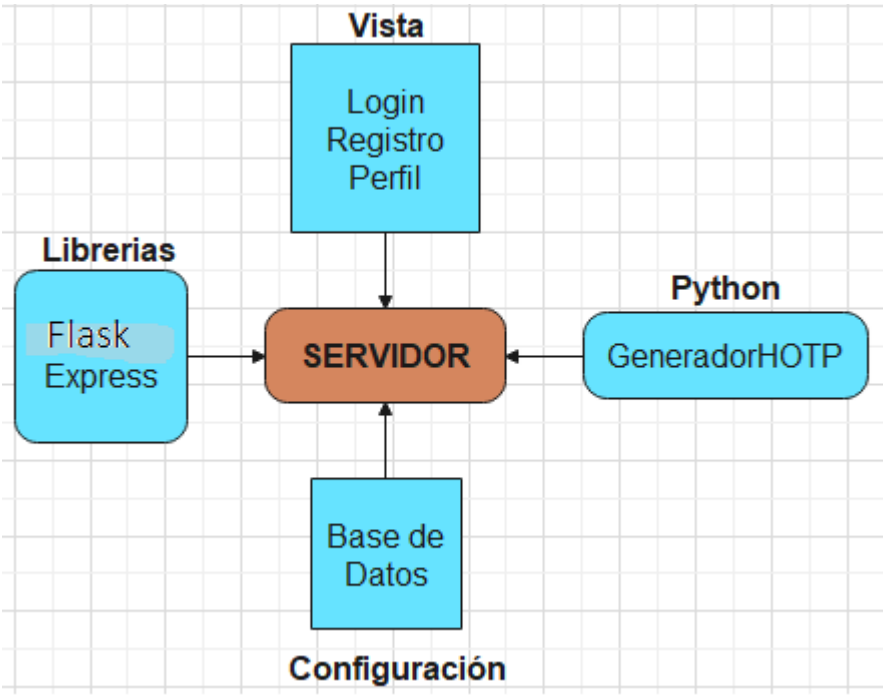


Figura 3. Esquema del Servidor

Autenticación de un solo factor

La autenticación de un usuario se realiza mediante la verificación de la contraseña y de esta manera aseguramos que el usuario es quien dice ser y a este proceso lo llamamos autenticación de un solo factor.

Y al hablar de contraseñas y según la Real Academia Española, una contraseña es una seña secreta que nos permite el acceso a algo [28]. Y como usuarios tenemos el defecto de tener contraseñas muy fáciles de recordar, lo que facilita al ciberdelincuente adivinar o utilizando un software descifrar una contraseña. Y ya que la contraseña es nuestra manera de autenticarnos debemos crear contraseñas mucho más seguras, es decir, realizando

combinaciones de caracteres alfanuméricos y símbolos especiales. Hay que tener muy en cuenta que nuestra contraseña es algo privado y que nadie puede saber o adivinar.

A continuación, en la Figura 4 se muestra las 5 contraseñas más comunes del año 2022 y el tiempo que toma descifrarlo [29]

RANGO	CONTRASEÑA	TIEMPO PARA DESCIFRARLA	RECUENTO
1	**password**	< 1 Segundo	4.929.113
2	**123456**	< 1 Segundo	1.523.537
3	**123456789**	< 1 Segundo	413.056
4	**guest**	10 Segundos	376.417
5	**qwerty**	< 1 Segundo	309.679

Figura 4. Contraseñas comunes 2022

Si se desea investigar un poco podemos dirigirnos a la referencia [32] y buscar en el listado de contraseñas comunes y tal vez nos encontremos con nuestra contraseña.

Como usuario debemos de tener en cuenta que nuestra contraseña es la única barrera que tenemos entre el ciberdelincuente para proteger ese algo, por tal motivo este trabajo se enfoca en brindar una mayor seguridad con un segundo factor de autenticación.

Autenticación de dos factores

La solución del 2FA surge a partir que los ciberdelincuentes pueden autenticarse con gran facilidad impostando la identidad del usuario, por tal motivo expertos en seguridad informática crearon una capa adicional de seguridad y el requiriendo extra por parte del usuario para verificar su identidad será su correo electrónico.

Para la realización de este trabajo la información extra que se va a requerir por parte del usuario es el correo electrónico. Algo importante por mencionar es que el uso de contraseñas en el mundo no es algo nuevo ya que se presenta de forma cotidiana y un claro ejemplo es el uso de la tarjeta para obtener dinero de un cajero automático, el usuario ingresa su contraseña y el cajero automático lo valida, permitiéndole al usuario tomar su dinero.

En pocas palabras la finalidad del 2FA es asegurar que el usuario conoce su contraseña para ingresar a un sitio y que además se verifique quien dice ser mediante esa información extra.

OTP

OTP es conocido como contraseña de un solo uso, esto quiere decir que una contraseña será válida para un solo uso, en nuestro caso para un solo inicio de sesión, al incorporar un OTP a un sistema de autenticación de dos factores creamos una capa extra de seguridad informática.

En OTP la seguridad se basa en no poder revertir la función hash y esa función criptográfica es el SHA1, cabe mencionar que el generador y el validador de códigos OTPs tienen que usar el mismo algoritmo para poder interoperar entre ellos.

HOTP

Es un algoritmo de generación de contraseñas de un solo uso utilizando un mecanismo criptográfico HMAC, este algoritmo nació para dar solución a los sistemas de autenticación de un solo factor.

Y para generar este algoritmo se tomó en cuenta los siguientes requerimientos [30]:

- Generar una clave secreta compartida: esta es una cadena de caracteres que se comparte entre el servidor y el cliente. Es utilizada para generar los códigos HOTP.
- Calcular el código HOTP: esto se hace mediante el uso de una función hash HMAC y un contador que se incrementa cada vez que se solicita un nuevo código HOTP.
- Verificar el código HOTP: el código HOTP se proporciona al servidor, que luego utiliza la clave secreta compartida y el contador para calcular el código HOTP esperado y compararlo con el código proporcionado y si coinciden, se autentica la solicitud.

En la Figura 5 se muestra el proceso de generación de contraseñas de un solo uso HOTP.

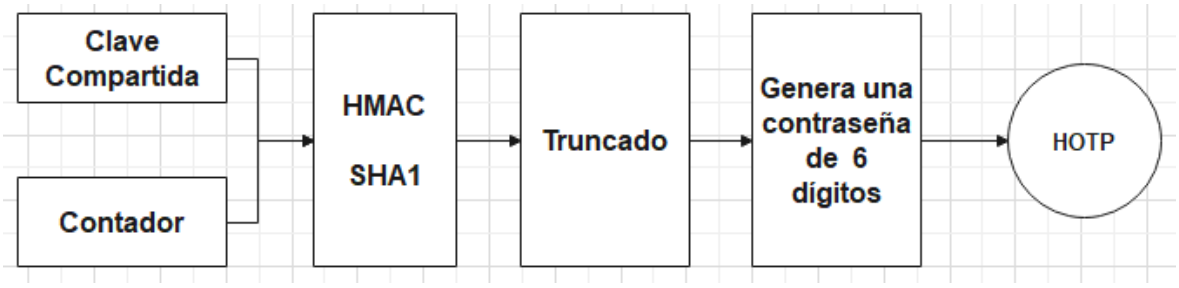


Figura 5. Proceso de Generación de contraseña

El algoritmo de generación de códigos HOTP de un solo uso fue desarrollado en el lenguaje de programación Python, este lenguaje posee una sintaxis legible del código [31].

- Este algoritmo genera contraseñas de un solo uso de 6 dígitos.
- Estos códigos generados son almacenados en la base de datos de Posgresql.

En la Figura 6, se muestra el código desarrollado en Python del generador y el verificador, la función generar HOTP recibe como parámetros la clave y el número del contador, mientras que para el verificador recibe los parámetros de la clave, número del contador y la contraseña generada.

El generador convierte al valor del contador en un valor hexadecimal que en conjunto con la clave se le aplica criptografía (HMAC, SHA1), para posteriormente realizar el trucado.

```
5   def generador_hotp(key, counter):
6     # Convertir la clave y el contador a bytes
7     key = base64.b32decode(key)
8     counter = int(counter).to_bytes(8, byteorder='big')
9
10    # Calcular el código HMAC
11    hmac_value = hmac.new(key, counter, hashlib.sha1).digest()
12
13    # Extraer el último dígito del valor HMAC
14    offset = hmac_value[-1] & 0xf
15
16    # Extraer los 4 dígitos a partir del offset
17    code = ((hmac_value[offset] & 0x7f) << 24 |
18            (hmac_value[offset + 1] & 0xff) << 16 |
19            (hmac_value[offset + 2] & 0xff) << 8 |
20            (hmac_value[offset + 3] & 0xff)) % 1000000
21
22    # Devolver el código como una cadena de 6 dígitos
23    return f'{code:06d}'
24
25  def verificador_hotp(key, counter, code):
26    # Calcular el código HOTP esperado
27    expected_code = generador_hotp(key, counter)
28
29    # Comparar el código esperado con el código proporcionado
30    return expected_code == code
```

Figura 6. Generador y Verificador HOTP

La función del verificador de contraseñas se encarga de verificar si el valor generado coincide con el valor enviado al usuario, si el valor es el correcto se válida la contraseña y el contador aumenta su valor, caso contrario el valor no se valida, ni aumenta el contador.

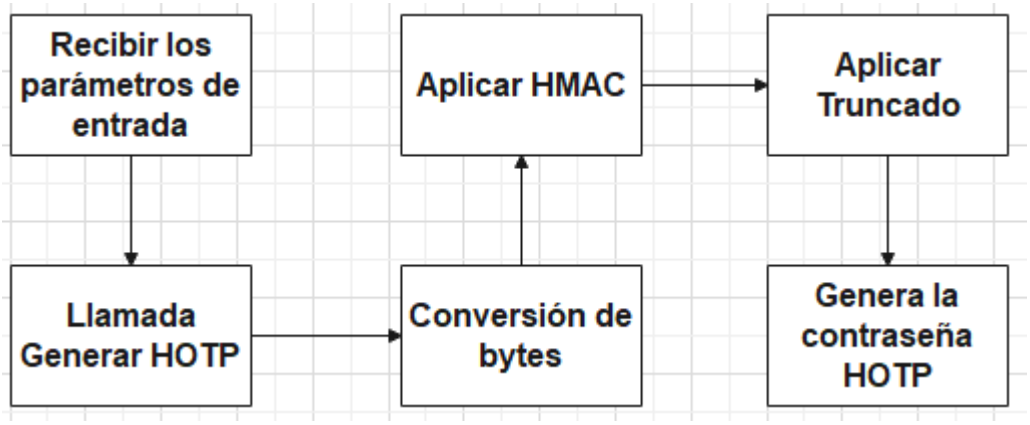


Figura 7. Diagrama de flujo del Generador HOTP

Método de entrega

El usuario tiene una única forma de recibir la contraseña de un solo uso generada por el HOTP y es mediante correo electrónico, por lo que es rápido, fácil y económico de usar.

2.2 Análisis de las Herramientas y Diseño

Dentro de esta sección se va a definir el stack tecnológico con el cual se va a diseñar el prototipo del sistema de doble factor de autenticación, las cuales son:

NodeJS

Usando el entorno de ejecución multiplataforma de NodeJS de código abierto [32], NodeJS nos permite proporcionar un entorno de ejecución del lado del servidor como se muestra en la Figura 3, el esquema proporciona una visualización de las distintas partes del trabajo como las librerías, las vistas, las configuraciones y Python. NodeJs facilita la creación de programas y páginas web mediante aplicaciones como Visual Studio Code, esta aplicación se encuentra instalado y se utilizará en mi ordenador.

Librería

La librería para usar es Express, ya que es un framework web de Node de gran popularidad para desarrollo web [33]

- Express maneja una integración de motores de renderización de vistas.

- Permite establecer ajustes para conectar y usar el puerto.
- Maneja peticiones con diferentes caminos URL.

PosgreSQL

Se hace uso de la base de datos PosgreSQL para almacenar los datos que se proporcionen en la aplicación web y se hizo uso de esta base de datos SQL ya que es de código abierto. Posgresql almacena los datos, permitiendo la integración de los datos a la aplicación.

Para este trabajo se optado por usar un modelo de datos de dos tablas.

La primera tabla va a almacenar el correo electrónico, contraseña, número de celular y la clave. Esta clave es la concatenación del usuario convertido a base64.

Tabla 1. Tabla de Datos (Usuarios)

Atributo	Tipo
Usuario (correo electrónico)	String
Contraseña	String
Número de celular	String
Clave	String

En la segunda tabla se va a almacenar la clave, el OTP generado, valido, es decir si el OTP generado ha sido usado o no.

Tabla 2. Tabla de Datos (contraseñas)

Atributo	Tipo
Clave	String
OTP Generado	String
Valido	Boolean

Python

Se hace uso del lenguaje de programación Python, para desarrollar el código de generación de contraseñas de un solo uso OTP. Este lenguaje es multiparadigma por lo que soporta orientación a objetos, programación funcional e imperativa, además de ser de código abierto.

Figma

Es una herramienta de generación de prototipos y un editor de gráficos [34], con esta herramienta se facilita diseñar las interfaces gráficas del prototipo web que se muestran en las Figura 8, Figura 9 y Figura 10. Figma es un programa de software colaborativo y licenciado, pero tiene una versión de prueba gratuita con limitaciones.

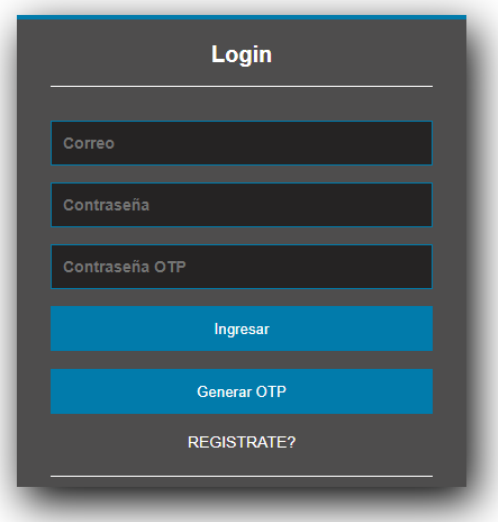


Figura 8. Figma Login

Figura 9. Figma Registro

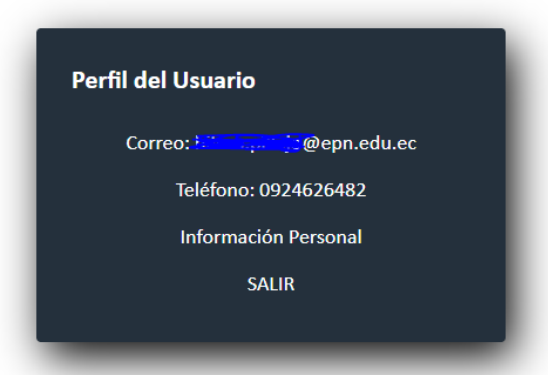


Figura 10. Figma Perfil

2.3 Diseño del prototipo

En esta sección se va a desarrollar las interfaces gráficas de la aplicación web con las que el usuario va a interactuar, y esas interfaces son:

Login

Esta interfaz gráfica va a permitir al usuario poder realizar su autenticación mediante su correo electrónico, contraseña y la contraseña generada por el OTP, esta contraseña generada se lo enviara al correo electrónico del usuario para identificar quien dice ser, con este proceso se aplica el doble factor de autenticación.

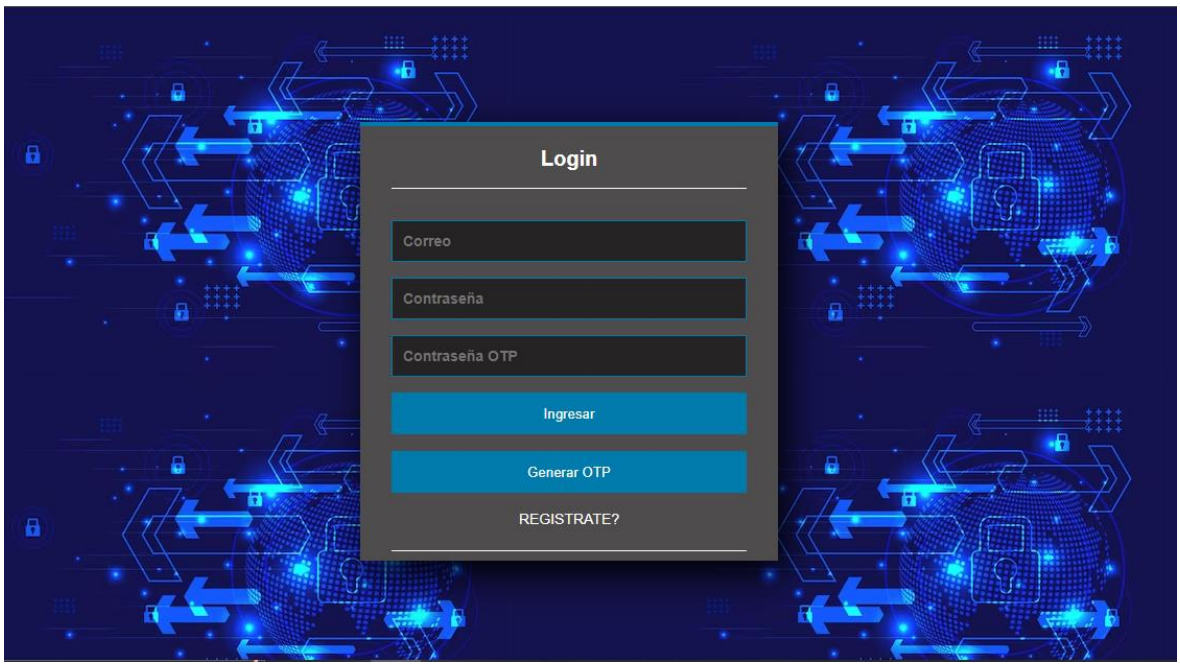


Figura 11. Interfaz Gráfica Login

Registro

Esta interfaz gráfica va a permitir al usuario poder realizar su registro en la aplicación web tomando la información solicitada y posteriormente guardada en la base de datos NoSQL dando un clic en enviar.

Figura 12. Interfaz Gráfica Registro

Perfil

Esta interfaz gráfica va a permitir al usuario poder visualizar información que se encuentre en su perfil, cabe mencionar que esta interfaz gráfica no tiene ninguna finalidad en específica. Y al pulsar el botón de salir, el usuario habrá finalizado su cesión.

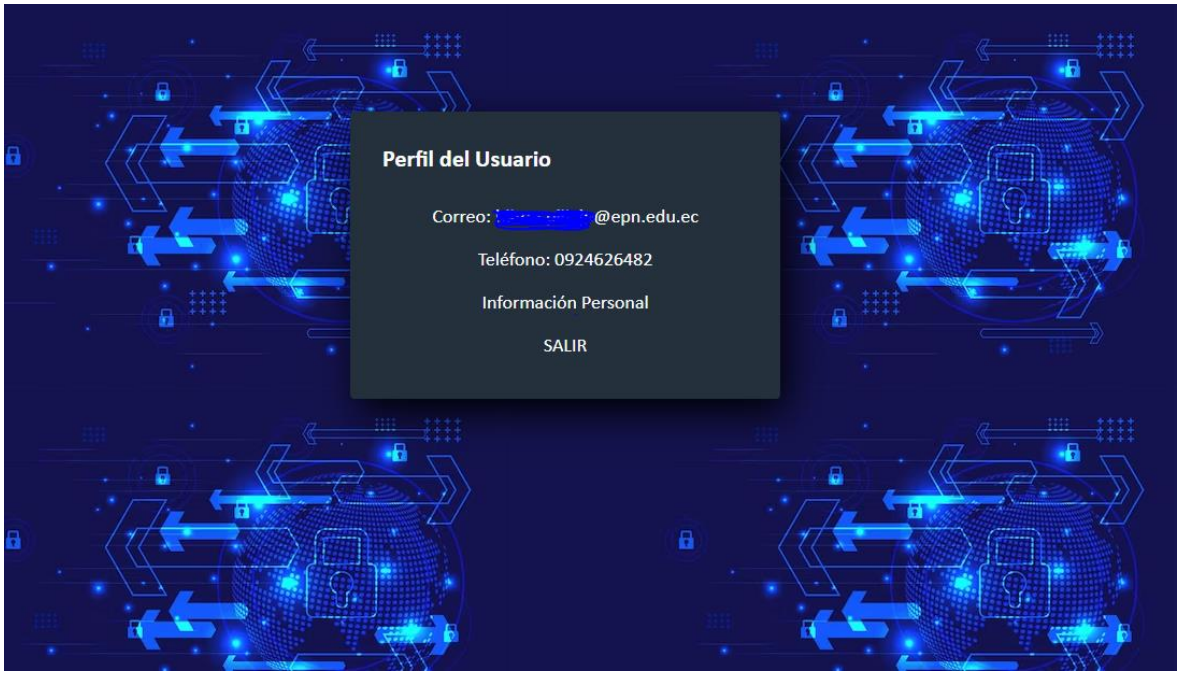


Figura 13. Interfaz Gráfica Perfil

Rutas

Al usar la librería Express el prototipo dispone de rutas que permiten realizar una navegación por sus interfaces.

Login, esta ruta muestra la interfaz gráfica del Login que previamente fue ya descrita y permite peticiones GET como POST.

Registro, esta ruta muestra la interfaz gráfica de Registro que previamente fue ya descrita y permite peticiones GET como POST.

Perfil, esta ruta muestra la interfaz gráfica del Perfil del usuario que previamente fue ya descrita.

Generador OTP, esta ruta permite la generación de un nuevo código y se activa cuando el usuario pulsa el botón “Generar OTP”. Dentro del sistema hace un llamado al script de Python, genera la contraseña de uso único y lo envía mediante correo electrónico al usuario.

Salir, esta ruta realiza el cierre de cesión del usuario.

Figura 14. Arquitectura del Prototipo 2FA

2.4 Testeo del Prototipo

El prototipo creado de doble factor de autenticación es un sistema mucho más robusto y seguro que el sistema de autenticación de un solo factor, aunque se debe mencionar que mientras un sistema tenga múltiples factores de autenticación, el sistema será mucho más seguro, pero tener múltiples factores de autenticación no es viable y genera incomodidad al usuario, ya que al autenticarse el usuario es posible que se demore mucho tiempo.

Y en base al tiempo es lo que se va a realizar el testeo del prototipo en el cual se va a simular la generación de un código HOTP: generar un código OTP y medir el tiempo que se tarda en milisegundos.

Posteriormente se va a medir el tiempo de envío que tarda el sistema en enviar por correo electrónico. Se suma los tiempos de generación y envío para obtener el tiempo total que se tarda en recibir el código OTP. Se procede a repetir el proceso varias veces y tomar el promedio de los tiempos para obtener una mejor estimación del rendimiento del sistema.

Es importante asegurarse de que el tiempo de generación y envío del código HOTP sea lo suficientemente rápido para que los usuarios no experimenten demoras significativas en el proceso de autenticación. La prueba de tiempo de generación y envío del código HOTP por correo electrónico es una de las pruebas importantes para garantizar el rendimiento óptimo del sistema de autenticación de doble factor.

Pruebas de Usabilidad

Para realizar el estudio de usabilidad del prototipo se ha utilizado el Sistema de Escalas de Usabilidad (SUS), pidiéndole al usuario que navegue por el prototipo 2FA para explorar sus funciones y características. Para que posteriormente el usuario llene una encuesta con las 10 preguntas de SUS, esta encuesta se lo realizo con 10 usuarios que oscilan entre los 15 y 50 años. La encuesta se lo realizó en Google forms, obteniendo los siguientes resultados por cada pregunta:

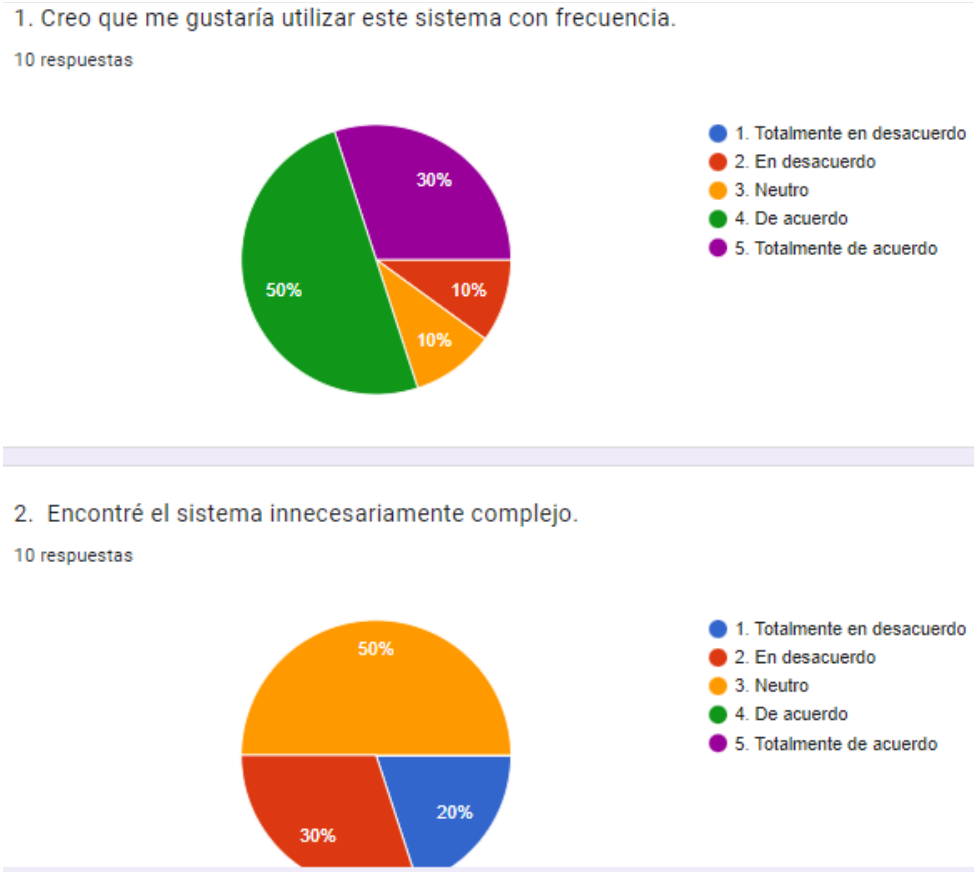
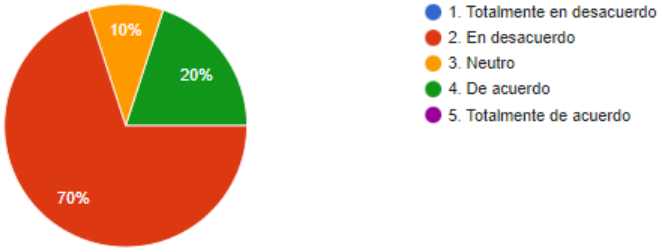


Figura 15. Pregunta 1 y 2 SUS

3. Pensé que el sistema era fácil de usar.

10 respuestas



4. Creo que necesitaría el apoyo de un técnico para poder utilizar este sistema

10 respuestas

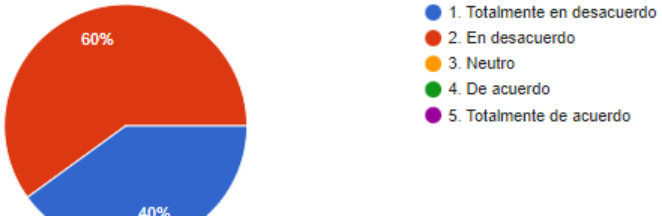
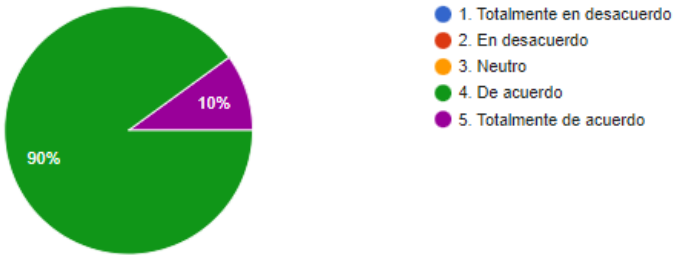


Figura 16. Pregunta 3 y 4 SUS

5. Encontré que las diversas funciones de este sistema estaban bien integradas

10 respuestas



6. Pensé que había demasiada inconsistencia en este sistema

10 respuestas

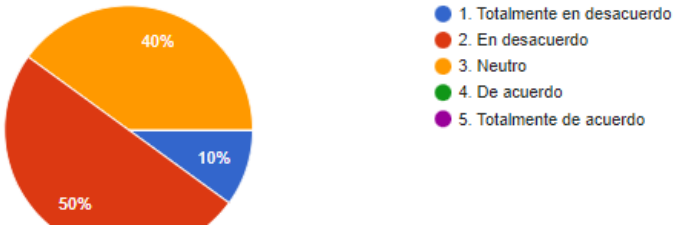


Figura 17. Pregunta 5 y 6 SUS

Figura 18. Pregunta 7 y 8 SUS

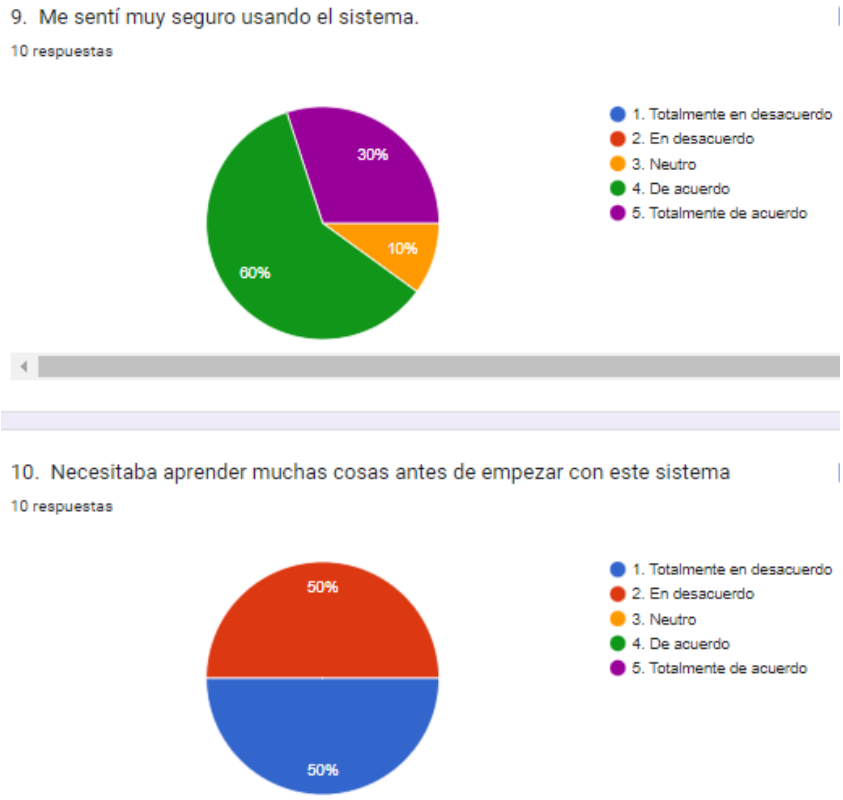


Figura 19. Pregunta 9 y 10 SUS

En base a los porcentajes de cada pregunta se va a obtener un promedio como se muestra en la Tabla 3, con el cual se realizarán los respectivos cálculos y se obtendrá un porcentaje sobre 100. Y el promedio de cada pregunta lo obtengo de la siguiente manera:

Ejemplo Pregunta 1: 50% →4, 30% →5, 10% → 2 y 10% → 3. Como en total son 10 respuestas. (4+4+4+4+4+5+5+5+2+3) / 10 = 4 → promedio pregunta 1

Tabla 3. Valor numérico

# de Pregunta	Promedio
1	4
2	2,3
3	2,5
4	1,6
5	4,1
6	2,3
7	4,4
8	1,9
9	4,2
10	1,5

Y para realizar el cálculo del porcentaje de SUS nos referenciamos a [35], y obtenemos el siguiente resultado:

Respuestas preguntas impares: (4 + 2,5 + 4,1 + 4,4 + 4,2) = 19,2 – 5 = 14,2

Respuestas preguntas pares: (2,3 + 1,6 + 2,3 + 1,9 + 1,5) = 25 – 9,6 = 15,4

Cálculo del SUS: (14,2 + 15,4) * 2,5 = 74

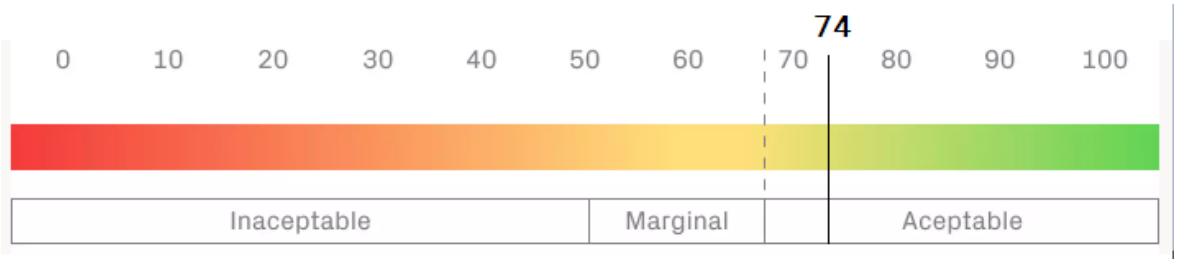


Figura 20. Representación de resultados SUS

Con el porcentaje obtenido del cálculo de SUS, podemos interpretar que el estudio del prototipo de 2FA es aceptable.

3.RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

3.1 Resultados

El usuario al usar el servicio y emplear demasiado tiempo en autenticarse y verificar que es el quien dice ser, el usuario no se sentirá cómodo al usar ese servicio y lo más probable es que deserte de usar ese servicio.

Basandonos en esta incomodidad que generaria al usuario se va a mostrar la Tabla 4, que contiene el tiempo generado para la obtener la contraseña de un solo uso OTP y el tiempo que se demora el sistema en enviar esta contraseña al correo electrónico del usuario. La Tabla 4 muestra una prueba realizada con 10 envíos y la suma en tiempos de generar y enviar la contraseña de un solo uso.

Tabla 4. Tiempos de envío

Envíos	Generar OTP milisegundos	Envío de contraseña milisegundos	Total milisegundos
1	61,92	12970	13031,92
2	60,68	11450	11510,68
3	58,99	13567	13625,99
4	61,02	12790	12851,02
5	63,4	15981	16044,4
6	57,64	11345	11402,64
7	52,93	12456	12508,93
8	51,05	13967	14018,05
9	81,3	16782	16863,3
10	56,19	14231	14287,19
Promedio	60,512	13553,9	13614,412

Para realizar esta prueba se utilizó una laptop con las siguientes características:

- Laptop HP 14 notebook
- Sistema Operativo: Windows 10
- Procesador: Intel(R) Core (TM) i5-4210U CPU @ 1.70GHz 2.40 GHz
- Memoria RAM de 4GB
- Sistema de 64 bits

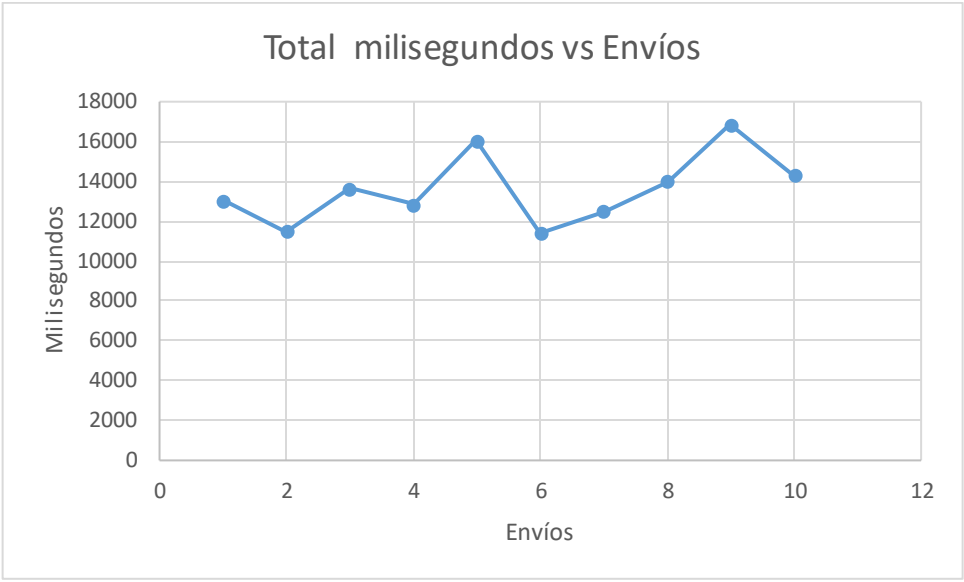


Figura 21. Milisegundos vs Envíos

En la Figura 22, se muestra el número de envíos de correo electrónico con la contraseña de un solo uso generada y el tiempo en milisegundos que se demora en entregar cada envío. Como se observa que los tiempos son muy similares y no se distorsionan mucho.

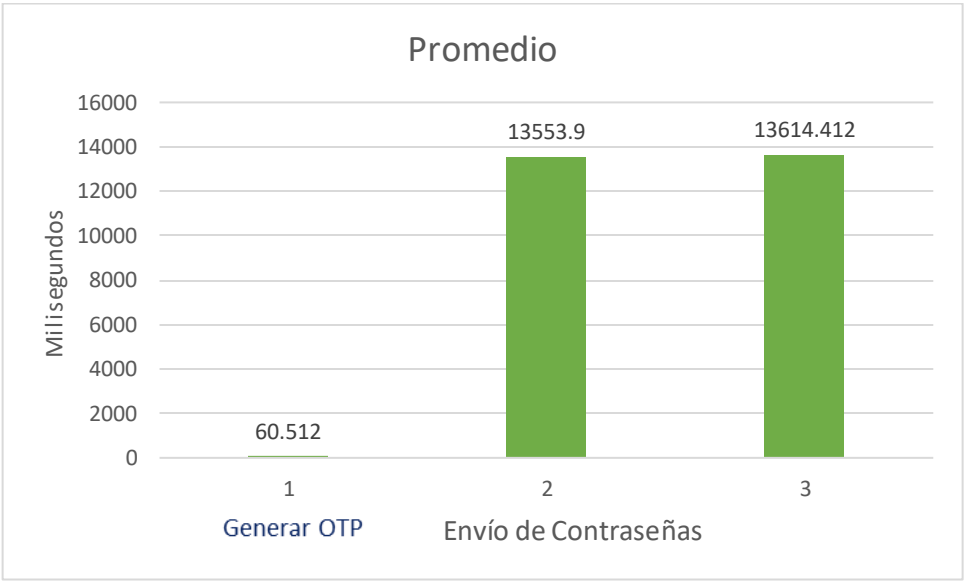


Figura 22. Promedio

En la Figura 22, se muestra un promedio en milisegundos de cada barra, es decir, el promedio para generar una contraseña de uso único OTP es de 60,512 milisegundos y para él envió de las contraseñas generadas mediante correo electrónico es de 13553,9 milisegundos. Esto quiere decir que un promedio de generar y enviar la contraseña OTP es de 13614,412 milisegundos.

Todas las pruebas realizadas tuvieron éxito, tomando en cuenta que su tiempo al generar y enviar variaba.

Como resultados esperados se ha logrado cumplir con los objetivos establecidos, se ha llegado a realizar un prototipo de un sistema de doble factor de autenticación, se generó una contraseña de un solo uso HOTP y mediante el estudio del arte se conoce mucho sobre el tema de seguridad informática, factores de autenticación, generación de códigos de un solo uso, se utilizó diferentes herramientas con los cuales llegamos a desarrollar todo el trabajo establecido desde un principio y culminar de la mejor forma este trabajo.

3.2 Conclusiones

Mediante el estudio del arte se observa una gran problemática en el ámbito de la seguridad informática el cual es el sistema de autenticación de un solo factor, cabe mencionar que este proceso se lo realiza desde hace mucho tiempo, pero con los ciberdelincuentes al asecho y poseer contraseñas débiles o fáciles de recordar, como usuarios damos facilidad a estos delincuentes cibernéticos a que puedan acceder a nuestras cuentas. En base a esta problemática se dio solución haciendo uso de un segundo factor de autenticación, protegiendo la integridad de nuestros datos o información que se tenga en cualquier sistema.

Con la finalización de este trabajo (prototipo de sistema de doble factor de autenticación) se ha logrado alcanzar los objetivos específicos establecidos a un inicio. Con el uso de este prototipo se ha realizado pruebas para la generación de contraseñas de un solo uso, con el uso del lenguaje de programación Python. Al hacer uso de un segundo factor de autenticación la seguridad aumenta significativamente, ya que, si un ciberdelincuente tiene acceso a nuestra contraseña, necesitaría tener acceso al segundo factor de autenticación que en este caso es el correo electrónico para acceder a la cuenta y esto dificulta a los ciberdelincuentes el acceso a las cuentas de los usuarios. Cabe mencionar que, si se aplica más de un segundo factor de autenticación, puede llevar a ocasionar malestar o vivir una mala experiencia por parte del usuario.

La elección del segundo factor de autenticación debe basarse en la conveniencia y facilidad de uso para el usuario, pero también en su capacidad para proporcionar una mayor seguridad, de esta manera se proporciona una capa adicional de seguridad para proteger la cuenta del usuario.

Al elegir un algoritmo OTP (One-Time Password) para un sistema de autenticación de dos factores, es importante tener en cuenta varios factores, como la seguridad, la facilidad de implementación, también es importante seguir las mejores prácticas de seguridad y asegurarse de que el algoritmo (HOTP) implementado sea de manera segura y así evitar vulnerabilidades.

En conclusión, un sistema de doble factor de autenticación es una medida de seguridad extra que aumenta la protección en los sistemas de autenticación. Al implementar un 2FA, los proveedores de servicios brindar a los usuarios una capa extra de seguridad, al mismo tiempo que deben tener en cuenta los posibles problemas que puedan surgir al hacer el proceso de autenticación, ya que, esto puede representar una molestia para el usuario final.

Y con miras en cumplir las fechas del plan de trabajo, se ha trabajo con las fechas ya establecidas tratándolas de cumplir con exactitud y aunque por momentos si se retrasaba con el trabajo, se ha logrado cumplir con el tiempo establecido y los objetivos.

3.3 Recomendaciones

Una recomendación principal es que antes de empezar a trabajar en el prototipo debemos definir claramente los requisitos del sistema de doble factor de autenticación. Es decir, establecer los objetivos, los componentes, la plataforma a usar, si el sistema desarrollar es web o móvil y cualquier otra especificación por más insignificante que sea, para más adelante tomarlo en cuenta o descartarlo.

Es importante elegir de forma correcta un segundo factor de autenticación para el sistema a desarrollar. Porque existen múltiples opciones como: tokens físicos, aplicaciones móviles, mensajes de texto, correos electrónicos, llamadas telefónicas, huellas dactilares, reconocimiento facial y para uso practico de este trabajo se ha elegido correo electrónico.

Es importante considerar la experiencia del usuario al diseñar el sistema de doble factor de autenticación. Ya que este proceso de autenticación debe facilitar la autenticación de quien dice ser y no que el usuario se lleve una mala experiencia.

Es importante considerar la seguridad total del prototipo de sistema de doble factor de autenticación y adoptar las medidas que sean necesarias para evitar cualquier tipo de vulnerabilidad. Ya que un sistema web o móvil puede albergar información sensible de los usuarios y con un correcto sistema de 2FA desarrollado se pueda garantizar que no se expongan a riesgos de seguridad informática.

Una vez que el prototipo se encuentre listo para funcionar se deben de realizar pruebas para garantizar que el sistema de doble factor de autenticación funcione correctamente. En el caso de este proyecto solo se realizaron pruebas de medición de tiempo para generar las contraseñas OTPs y el envió de la contraseña generada por correo electrónico al usuario y que el proceso de autenticación sea fácil y rápido de usar.

Después de realizar las pruebas al prototipo, es importante obtener retroalimentación por parte de los usuarios. Y tener muy en cuenta sus comentarios y opiniones, para poder realizar mejoras el sistema a futuro en base a sus sugerencias y necesidades que se presenten.

4. REFERENCIAS BIBLIOGRÁFICAS

[1] R. O. Andrade, S. G. Yoo, I. Ortiz-Garces, and J. Barriga, "Security Risk Analysis in IoT Systems through Factor Identification over IoT Devices," *Applied Sciences (Switzerland)*, vol. 12, no. 6, Mar. 2022, doi: 10.3390/app12062976.

[2] J. J. Barriga and S. G. Yoo, "Securing End-Node to Gateway Communication in LoRaWAN With a Lightweight Security Protocol," *IEEE Access*, vol. 10, pp. 96672–96694, 2022, doi: 10.1109/ACCESS.2022.3204005.

[3] G. Lee, D. Howard, D. Ślęzak, K.-Y. Park, S.-G. Yoo, and J. Kim, "Security Requirements Prioritization Based on Threat Modeling and Valuation Graph," 2011.

[4] J. Guerrero Ramírez, "Autenticación de doble factor mediante OTPs."

[5] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent Two-Factor Authentication," *IEEE Access*, vol. 6, pp. 32677–32686, 2018, doi: 10.1109/ACCESS.2018.2844548.

[6] D. de Borde, "Selecting a two-factor authentication system," *Network Security*, vol. 2007, no. 7, pp. 17–20, Jul. 2007, doi: 10.1016/S1353-4858(07)70066-1.

[7] G. Sciarretta, R. Carbone, S. Ranise, and L. Viganò, "Formal Analysis of Mobile Multi-Factor Authentication with Single Sign-On Login," *ACM Transactions on Privacy and Security*, vol. 23, no. 3, pp. 1–37, Aug. 2020, doi: 10.1145/3386685.

[8] S. Ruoti and K. Seamons, "End-to-End Passwords," 2017, doi: 10.1145/3171533.

[9] E. Erdem and M. T. Sandikkaya, "OTPaaS—One Time Password as a Service," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 743–756, Mar. 2019, doi: 10.1109/TIFS.2018.2866025.

[10] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines: revision 3," Gaithersburg, MD, Jun. 2017. doi: 10.6028/NIST.SP.800-63-3.

[11] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm," Dec. 2005. doi: 10.17487/rfc4226.

[12] D. Marco del IEEE, D. Marco, and L. de Evolución Del Concepto Seguridad, "International Security. An Analytical Survey. Lynne Rienner Publishers," 2005.

[13] "La seguridad vista desde sus inicios | INCIBE." https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio (accessed Feb. 11, 2023).

[14] "Identificación y autenticación - Documentación de IBM." https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009740--htm (accessed Feb. 11, 2023).

[15] "The Basics of Information Security Second Edition."

[16] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines: revision 3," Gaithersburg, MD, Jun. 2017. doi: 10.6028/NIST.SP.800-63-3.

[17] R. A. Española and R. A. Española, *autenticación*, 23.ª. Accessed: Feb. 11, 2023. [Online]. Available: https://dle.rae.es/autenticaci%C3%B3n

[18] "Introducción a la autenticación: cómo probar que realmente eres tú | WeLiveSecurity." https://www.welivesecurity.com/la-es/2016/05/04/autenticacion-como-probar-que-eres-tu/ (accessed Feb. 11, 2023).

[19] E. Erdem and M. T. Sandikkaya, "OTPaaS-One time password as a service," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 743–756, 2018, doi: 10.1109/TIFS.2018.2866025.

[20] S. Roy, M. Rutherford, and C. H. Crawshaw, "Towards designing and implementing a secure one time password (OTP) authentication system," in *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, Dec. 2016, pp. 1–2. doi: 10.1109/PCCC.2016.7820604.

[21] L. Lamport, "Password authentication with insecure communication," *Commun ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981, doi: 10.1145/358790.358797.

[22] W.-B. Leea, T.-H. Chen, W.-R. Sun, and K. I.-J. Ho, "An S/Key-like One-Time Password Authentication Scheme Using Smart Cards for Smart Meter," in *2014 28th International Conference on Advanced Information Networking and Applications Workshops*, May 2014, pp. 281–286. doi: 10.1109/WAINA.2014.78.

[23] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, "OTP-Based Two-Factor Authentication Using Mobile Phones," in *2011 Eighth International Conference on Information Technology: New Generations*, Apr. 2011, pp. 327–331. doi: 10.1109/ITNG.2011.64.

[24] A. L. Bement, "FIPS PUB 198 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION The Keyed-Hash Message Authentication Code (HMAC) CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY," 2002.

[25] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm," Dec. 2005. doi: 10.17487/rfc4226.

[26] R. A. Grimes, "One-Time Password Attacks," in *Hacking Multifactor Authentication*, 2021, pp. 205–226. doi: 10.1002/9781119672357.ch9.

[27] "Prototipo: qué es y cómo hacer prototipado | FREED." https://freed.tools/blogs/ux-cx/prototipo (accessed Feb. 15, 2023).

[28] "contraseña | Definición | Diccionario de la lengua española | RAE - ASALE." https://dle.rae.es/contrase%C3%B1a (accessed Feb. 16, 2023).

[29] "Lista de las 200 contraseñas más comunes de 2022 | NordPass." https://nordpass.com/es/most-common-passwords-list/ (accessed Feb. 16, 2023).

[30] UCSD *et al.*, "HOTP: un algoritmo de contraseña de un solo uso basado en HMAC," Dec. 2025. https://www.ietf.org/rfc/rfc4226.txt (accessed Feb. 16, 2023).

[31] Alex. Martelli, "Python : guía de referencia," 2007.

[32] "NodeJS." https://desarrolloweb.com/home/nodejs (accessed Feb. 16, 2023).

[33] “Introducción a Express/Node - Aprende sobre desarrollo web | MDN.” https://developer.mozilla.org/es/docs/Learn/Server-side/Express_Nodejs/Introduction (accessed Feb. 16, 2023).

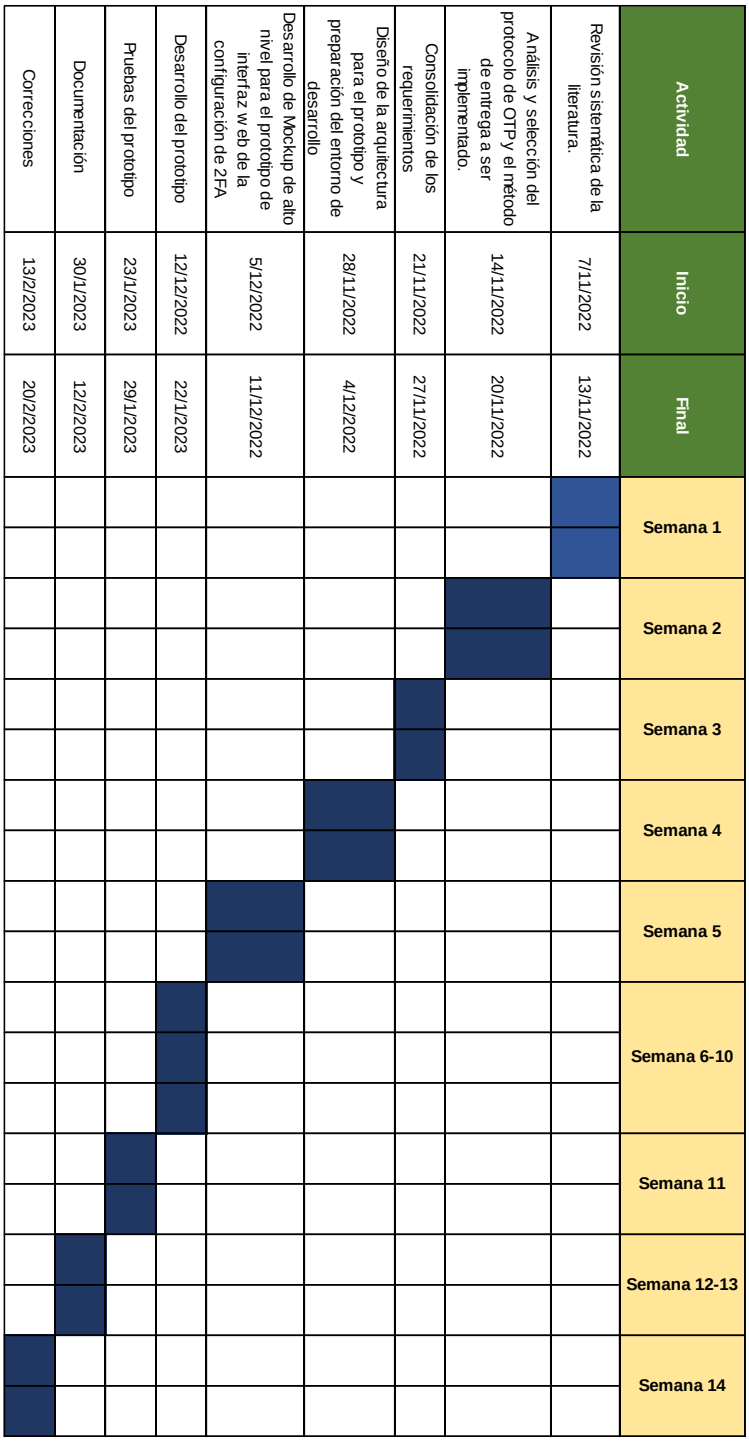
[34] R. Gonzalez and R. Gonzalez, “Figma Wants Designers to Collaborate Google-Docs Style,” *WIRED*, Jul. 2017, Accessed: Feb. 16, 2023. [Online]. Available: https://www.wired.com/story/figma-updates/

[35] “Cómo medir la usabilidad con un SUS — uiFromMars.” https://www.uifrommars.com/como-medir-usabilidad-que-es-sus/ (accessed Mar. 01, 2023).

5. ANEXOS

5.1 ANEXO I

Diagrama de GANTT Planificación Estimada del Trabajo



5.2 Anexo 2

Enlace del código: https://github.com/BladimirPillajo/Proyecto-2FA.git