FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Implementación de un método de identificación de electores basado en autenticación multifactor para mitigar la suplantación de identidad en el voto electrónico no presencial. Caso de estudio: Elecciones de APAFA.

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor:
Bach. Perez Chanduvi Sandro Paul
https://orcid.org/0000-0002-2723-1701

Asesor:
Mg. Ing. Bances Saavedra David Enrique
https://orcid.org/0000-0002-7164-8918

Línea de Investigación:
Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú
2023

IMPLEMENTACIÓN DE UN MÉTODO DE IDENTIFICACIÓN DE ELECTORES BASADO EN AUTENTICACIÓN MULTIFACTOR PARA MITIGAR LA SUPLANTACIÓN DE IDENTIDAD EN EL VOTO ELECTRÓNICO NO PRESENCIAL. CASO DE ESTUDIO: ELECCIONES DE APAFA.

Aprobación del jurado

_____

Mg. MEJIA CABRERA HEBER IVAN
Presidente del Jurado de Tesis

_____

Mg. ARCILA DIAZ JUAN CARLOS
Secretario del Jurado de Tesis

_____

Mg. DAVID ENRIQUE BANCES SAAVEDRA
Vocal del Jurado de Tesis

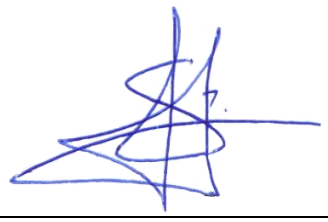
DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la **DECLARACIÓN JURADA**, soy egresado del Programa de Estudios de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Señor de Sipán S.A.C., declaro bajo juramento que soy autor del trabajo titulado:

IMPLEMENTACIÓN DE UN MÉTODO DE IDENTIFICACIÓN DE ELECTORES BASADO EN AUTENTICACIÓN MULTIFACTOR PARA MITIGAR LA SUPLANTACIÓN DE IDENTIDAD EN EL VOTO ELECTRÓNICO NO PRESENCIAL. CASO DE ESTUDIO: ELECCIONES DE APAFA.

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando al derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firma:

Perez Chanduvi Sandro Paul	DNI: 16790289	

Pimentel, 16 de setiembre del 2023.

Dedicatoria

A mis seres queridos, en especial a mis hijas, Paola, Stefany y Alisson, a quienes prive de mi presencia, compañía y apoyo, a lo largo de estos años, con el firme propósito de brindarles una mejor calidad de vida.

Agradecimientos

A Dios, por la vida y la salud que me brinda día a día.

A mis padres, por su apoyo en todas las etapas de mi vida.

A mis hermanos, quienes, a pesar de las dificultades que enfrentan, no dejan de apoyarme y motivarme.

A mis amistades, quienes, conocedores de mi realidad, me alientan a seguir adelante.

A mis maestros, quienes, a través de sus enseñanzas y conocimientos impartidos a lo largo de mi carrera profesional, lograban sacar lo mejor de mí para concluir con esta meta trazada, ser un profesional.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

Actualmente, uno de los principales delitos informáticos, es la suplantación de identidad, perjudicando de manera material o moral a una persona natural o jurídica. Para ello, el criminal burla los sistemas de seguridad a través de la tecnología, logrando accesar sin autorización a los sistemas informáticos. Estos accesos se dan básicamente por el solo uso de usuario y contraseña al momento de acceder a las aplicaciones informáticas, ya que este método de autenticación no ofrece las garantías necesarias para la protección de la información.

Con el fin de hacer frente a este tipo de delitos, a través de la presente investigación, se implementó un método de identificación de usuarios flexible basado en autenticación multifactor para mitigar la suplantación de identidad en el acceso a aplicaciones web, tomando como caso de estudio, las elecciones de APAFA, bajo la modalidad del voto electrónico no presencial.

A través del método implementado, el elector, además de ingresar su usuario y clave, debe proporcionar una contraseña de un solo uso, que es enviada a su celular o correo electrónico, previamente proporcionados en la fase de registro. Con ello, se comprueba que el elector es quien dice ser, debido a que proporciona algo que él sabe, como es la contraseña, y algo que posee, como es su celular.

Para la implementación del método de identificación se hizo uso de herramientas como la API Twilio, la cual permitió enviar mensajes de texto al elector, conteniendo la clave de acceso de un solo uso para poder accesar a la aplicación web.

Los resultados obtenidos fueron medidos a través de las métricas establecidas en la investigación y comparadas con resultados de investigaciones cuya naturaleza se asemejan al problema de investigación, comprobándose la efectividad del método implementado.

Palabras clave: Autenticación multifactor, contraseña, TOTP.

Abstract

Currently, one of the main computer crimes is identity theft, materially or morally damaging a natural or legal person. To do this, the criminal circumvents security systems through technology, gaining unauthorized access to computer systems. These accesses are basically given by the mere use of a username and password when accessing computer applications, since this authentication method does not offer the necessary guarantees for the protection of information.

In order to address this type of crime, through this research, a method of user identification based on multifactor authentication was implemented to mitigate impersonation in access to web applications, taking as a case study, the APAFA elections, under the modality of non-presential electronic voting.

Through the method implemented, the voter, in addition to entering his user name and password, must provide a one-time password, which is sent to his cell phone or e-mail, previously provided in the registration phase. This verifies that the voter is who he/she claims to be, since he/she provides something he/she knows, such as the password, and something he/she has, such as his/her cell phone.

For the implementation of the identification method, tools such as Twilio API were used, which allowed the sending of text messages to the voter, containing the one-time password to access the web application.

The results obtained were measured through the metrics established in the research and compared with research results whose nature is similar to the research problem, proving the effectiveness of the method implemented.

Keyword: Multi-factor authentication, password, TOTP.

I. INTRODUCCIÓN

1.1. Realidad Problemática

El incremento del uso de aplicaciones móviles [1], ha generado que muchas personas adquieran diferentes identidades digitales, las cuales deben proteger. Bajo este contexto, el solo uso de usuario/contraseña para salvaguardar el acceso a los servicios, no ofrece las garantías necesarias [2]; sobre todo, cuando las organizaciones hacen uso de la web para realizar sus operaciones [3].

En la encuesta realizada en el 2018 por la Secretaría de Comunicaciones y Transportes y la Organización de Estados Americanos (OEA), se observa un 62% (aumento de 20 puntos porcentuales respecto al año 2017) de encuestados que afirman haber sido, en algún momento, víctimas de robo/suplantación de identidad [4].

Bissada & Olmsted [5], afirman que, los incidentes de violación de datos y el robo de identidad, son cada vez más frecuentes, debido a que existe una población más grande que hace uso de tecnología y, sobre todo de dispositivos móviles para guardar y transmitir información confidencial; por lo que la implementación de medidas de seguridad y la autenticación mejorada, son más importantes que nunca.

Yang & Meng [6], refieren que, para todo sistema informático, la identificación es la clave y la base de la seguridad; por lo tanto, es el servicio de seguridad más importante, debido a que es la primera línea de defensa para la seguridad de un sistema informático, y otros servicios de seguridad deben basarse en él. Por ello, y como lo refieren Subrayan, Mugilan, Sivanesan, & Kalaivani [7], es en el proceso de autenticación donde se centra gran parte de las preocupaciones de seguridad.

La autorización y la autenticación siempre han sufrido ataques de hackers, por ser el primer paso para accesar a información sensible. Sin embargo, con la globalización y, sobre todo, con los avances y desarrollo de la tecnología, la frecuencia de tales ataques se ha incrementado exponencialmente. Respecto al fraude de transacciones en línea contra titulares de tarjetas de pago por país, las estadísticas afirman que, el país más

afectado es México (56%); seguido de Brasil (49%) y EEUU (47%). Hungría obtuvo el porcentaje más bajo (9%) [8].

Vaithyasubramanian, Lalitha, & Metilda [9], refieren que, debido a los métodos de ataque que se incrementan día a día, y a las vulnerabilidades que presentan los procesos de identificación de usuarios, los proveedores de servicios se han visto obligados a buscar diversas medidas alternativas con el fin de fortalecer el proceso de identificación, y de esta manera, garantizar la seguridad de los activos.

La implementación de un sistema de autenticación efectivo, es lo que toda institución pública o privada, sobre todo las instituciones financieras, debe priorizar para evitar perjuicios económicos, fraudes, robo/suplantación de identidad, acceso y/o manipulación de información confidencial, entre otros; que pongan en riesgo y perjudiquen al usuario o cliente [10].

Para evitar el fraude de las operaciones en línea, las partes interesadas de las empresas relacionadas han implementado varias prácticas de autenticación y autorización seguras en todos los niveles [11]. Estudios recientes afirman que, el 51% de las empresas han implementado métodos de autenticación multifactor (MFA), mientras que el 30% de empresas planean implementar este tipo de solución [12]. Los sistemas informáticos de las organizaciones latinoamericanas, implementan un promedio seis medidas de protección; siendo los sistemas de autenticación basados en contraseñas (58,2%) y los sistemas basados en rasgos biométricos (33,2%), los más adoptados como mecanismo de protección por estas empresas [13].

La autenticación multifactor es una forma más confiable de autenticación, debido a que mitiga de forma efectiva el robo de identidad en línea, gracias a la utilización de múltiples capas de autenticación [14]; por ello, existe una tendencia al alza en la implementación de métodos de autenticación que empleen más de un factor de autenticación [15], dificultando de esta manera, el acceso no autorizado. Aun así, una vez que el sistema de autenticación es vulnerado, todas las medidas de seguridad del sistema se romperán, y la información quedará a merced del atacante [6].

Los factores de autenticación incluyen conocimiento (por ejemplo, contraseña, pregunta secreta), posesión (por ejemplo, tarjeta inteligente, token, celular), e inherencia (por ejemplo, huella dactilar, reconocimiento facial). Cada uno de estos factores presenta sus propias fortalezas y debilidades. Un sistema de autenticación con contraseña es considerado menos seguro que uno que utiliza datos biométricos; sin embargo, es el más utilizado por la baja complejidad computacional, velocidad, escalabilidad y costo; por lo que resulta difícil encontrar un medio alternativo de autenticación que pueda reemplazar de manera efectiva y exitosa la contraseña tradicional [16]. La autenticación basada en posesión, es fácil de usar, pero está propensa a ser robada o extraviada. La autenticación biométrica es más segura que las antes mencionadas, pero una vez obtenida, no se puede revocar; asimismo, su implementación requiere inversión adicional [17].

La elección de autoridades es uno de los pilares en los países democráticos, en donde, a través del sufragio, los ciudadanos deciden quienes los van a dirigir o representar [18]. En la modalidad de voto convencional, el elector acude a los locales de votación, deposita una cédula en el ánfora de votación, se realiza el escrutinio de los votos públicamente y se llenan las actas con los resultados [19]. Esta modalidad obliga al elector a acudir a los locales de votación de forma presencial, lo que implica gastos económicos, y pérdida de tiempo para los electores [20]. En los sistemas de voto electrónico no presencial, los electores pueden emitir su voto desde cualquier lugar, lo cual aumenta la participación, elimina el traslado a los lugares de votación, permitiendo ahorrar tiempo y dinero [21].

La Ley N° 28044 – Ley General de Educación [22], en su artículo 54°, indica que les corresponde a los padres organizarse en asociaciones de padres de familia con el fin de contribuir al mejoramiento de los servicios educativos. En el proceso de elección de este tipo de organizaciones, surgen diversos conflictos por desconocimiento de los procedimientos electorales, generando malestar y quejas de los actores electorales, que muchas veces termina anulando el proceso de elección [23].

Antecedentes

Khattri & Singh [11], realizaron la investigación, *Implementation of an additional factor for secure authentication in online transactions*; en el Instituto de Administración Jaipuria - India. Con el aumento en el uso de pagos digitales, el fraude de transacciones en línea que se realiza con tarjetas de crédito/débito está en aumento, resultando un desafío sustancial para los comerciantes y bancos. Cuando el usuario inicia la transacción, el esquema identifica su ubicación y calcula la distancia entre el dispositivo donde se está realizando la transacción y el dispositivo móvil del usuario. Para que el sistema autentique la transacción, la distancia entre ambos dispositivos debe estar dentro de un límite permitido. La ubicación del usuario es obtenida mediante la activación del sistema de posicionamiento global (GPS) del equipo móvil, a través de una contraseña; luego envía la petición a la entidad financiera. A través de la triangulación satelital, se realiza el cálculo de la distancia entre ambos dispositivos, haciendo uso de la longitud y latitud obtenida del GPS. Si la distancia está fuera del límite permitido, la transacción no se realiza. El rendimiento y precisión del esquema propuesto es medido a través de cuatro parámetros, tales como: verdadero positivo (TP), verdadero negativo (TN), falso positivo (FP) y falso negativo (FN). Los dos primeros parámetros deben aproximarse al 100%; mientras que los dos últimos deben ser lo más cercano al 0%. Los resultados de la evaluación arrojaron una tasa de detección de fraude del 98.55% y una tasa de aciertos del 97.14%; mientras que la tasa de falsos positivos ascendió al 2% aproximadamente. Como factor adicional al método de autenticación se incorpora la distancia, lo cual permite que las transacciones en línea sean más seguras. Esto se evidencia con los resultados obtenidos del método propuesto.

Kordzo, Dorgbefu & Banning [24], realizaron la investigación, *Design and Implementation of Cost Effective Multi-Factor Authentication Framework for ATM Systems*; en la Universidad Tecnológica de Ghama. La mayoría de los ataques a los sistemas de cajeros automáticos (ATM) se debe en gran medida a las fallas de seguridad por parte de los propietarios de las cuentas. Estas fallas se originan por la facilidad de

adivinar los números de identificación personal (PIN), solicitud de ayuda a extraños durante las transacciones y exposición de tarjetas de cajero automático. La investigación utiliza tres factores para la implementación del proceso de autenticación, el cual consta de los módulos de registro y verificación de usuarios. En la fase de registro, el usuario ingresa un PIN, el cual, posteriormente es almacenado en un token físico. Adicional a ello, el sistema extrae las pulsaciones de teclas a medida que el usuario escribe el PIN, reconociendo, no lo que escribe, sino cómo escribe. En la fase de verificación, el sistema compara la contraseña ingresada con la contraseña almacenada. Asimismo, calcula y compara el ritmo y velocidad con la que ha sido ingresada. El marco propuesto se probó con 100 usuarios bajo los siguientes ataques: navegación de hombro, registro de información del usuario, ingeniería social, adivinación de contraseñas y fuerza bruta y ataques de diccionario. En la navegación de hombro, el 0% de los atacantes tuvieron éxito; en el registro de información del usuario, la tasa de falla es 100%; los ataques de ingeniería social tienen una tasa de éxito del 0%; la adivinación de contraseñas y fuerza bruta obtuvo el 0% de éxito. Debido a las diversas vulnerabilidades que presenta el solo uso de usuario y contraseña, resulta necesario la implementación de más de un factor de autenticación en la identificación de usuarios.

Fujita, Inomata & Kashiwasaki [25], realizaron la investigación, *Implementation and evaluation of a multi-factor web authentication system with individual number card and webUSB*, en la Universidad de Osaka-Japón. La identidad digital, muchas veces es usurpada debido al uso de métodos de autenticación no autorizada. Por ello, los métodos de autenticación multifactor han sido propuestos con la firme intención de mitigar esta realidad. Sin embargo, la implementación de estos métodos, hacen que dicho proceso dure más de lo habitual y, por ende, genera incomodidades por parte de los usuarios. La implementación del sistema propuesto introduce autenticación multifactor utilizando una MyNumberCard, la cual posee un certificado digital para firmar y un certificado digital para la certificación del usuario. Asimismo, para proporcionar accesos seguros desde páginas web a dispositivos USB, utiliza WebUSB (API de JavaScrip). El sistema lee la

clave pública como certificado de autenticación, la función firma para enviar mensajes usando la clave privada, la autenticación usando un código PIN; la API adquiere cuatro datos básicos de MyNumberCard, la dirección, nombre, edad y género. Los métodos empleados son *getMyNumber (pin)*: método para adquirir información de MyNumberCard; *getPersonalData (pin)*: método para adquirir datos personales en MyNumberCard; *getPublicKey*: método para adquirir la llave pública. Se comparó el tiempo promedio requerido y su desviación para la certificación entre el método propuesto y el método que combina la autenticación de contraseña y Time-based One Time Password – TOTP (Contraseña de un solo uso basado en el tiempo). El método propuesto se comparó con otros métodos de autenticación. Contraseña y TOTP arrojó un promedio de 17.6 segundos y una desviación estándar de 4.2 segundos; mientras que el método propuesto arrojó un promedio y desviación estándar de 3.5 segundos y 0.5 segundos, respectivamente. Los métodos de autenticación multifactor son los más recomendados para mitigar la autenticación no autorizada en sistemas informáticos, más aún en los servicios web. El uso de MyNumberCard y WebUSB hacen más rápido el proceso de autenticación, por lo que su uso en sistemas web es aconsejable.

Watanabe, Suzuki, Naito, & Watanabe [26], realizaron la investigación, *Proposal for user authentication method combining random number and password*, en la Escuela de Ciencia y Tecnología de la Universidad Meijo – Japón. Para hacer un proceso de autenticación más seguro, se debe trabajar con más de un factor de autenticación. Sin embargo, su implementación genera costos adicionales; asimismo, la usabilidad empeora, generando incomodidades para el usuario en el proceso de autenticación. En este artículo, se propuso un método de autenticación de múltiples factores que utiliza un número aleatorio suficientemente largo R, que se genera y almacena en la memoria no volátil del dispositivo del usuario. En el servidor, se calcula el valor hash RP en base al número aleatorio R y la contraseña de acceso del usuario. Al ingresar dicha contraseña, se calcula el hash RP y es enviado al servidor, quien verifica dicha información con la BD. El usuario es considerado válido si la información es correcta. Conjuntamente con

otros métodos de autenticación, se evaluó el costo, seguridad y usabilidad. La autenticación solo con contraseña es fácil de usar y económica, pero la seguridad es débil. Contraseña y biometría, resulta segura y no requiere operaciones adicionales, pero para su implementación es necesario una inversión inicial. Contraseña y TOTP tiene bajo costo y alta seguridad, pero algunas operaciones demandan más tiempo, generando malestar en el usuario. Contraseña y SMS resulta entendible y práctico; sin embargo, genera un costo adicional al hacer uso de telefonía. El método propuesto resultó 100% seguro, dado que el servidor no conoce R, por lo que no es posible descifrar las contraseñas; tiene costo S/ 0.00, debido a que utiliza como segundo factor el dispositivo móvil del usuario; asimismo, no tiene problemas de usabilidad, ya que no necesita de un dispositivo adicional al dispositivo móvil. Los resultados demuestran que se puede lograr la seguridad como la usabilidad, así como la suficiente fuerza contra ataques, ya que es seguro y económico.

Corredor, Pabón, Mora & Ardila [27], realizaron la investigación, Implementación de los servicios de autenticación fuerte multifactor y confidencialidad, para la protección de documentación electrónica; en la Universidad de Llanos, Colombia. Gran parte de la información que genera la sociedad se organiza en documentos electrónicos, por lo que su protección se ve afectada debido a fugas de información sensible, al no disponer de mecanismos tecnológicos que garanticen su confidencialidad y privacidad. En el método propuesto, el módulo de acceso obtiene Usuario (U) y contraseña (P); se genera el Hash de la contraseña (H[P]) y se transfiere U y H[P] al servidor web; el servidor valida la información de autenticación del usuario y busca la Huella del usuario (HuBD) en la Base de datos; el servidor genera dos Hash, el de la Huella obtenida de la BD y el del usuario, combinado con el Hash de la contraseña recibida del cliente. Estos datos junto con HuDB son enviados al cliente, quien genera el Hash de los datos recibidos H[u, H[P], H(Hu, BD)]; con la llave de sesión generada, el cliente consume el Web Service de autenticación, enviando por el método GET de HTTP la llave de sesión; el web Service valida la llave de sesión, permitiendo o denegando el acceso al módulo funcional. El

método implementado cumple las siguientes características: registro único, prevención de fraude, el password es cambiado libremente por el usuario, baja sobrecarga de la comunicación, prevención de ataques internos, establecimiento de llave de sesión. Además, se le incorporó teclado aleatorio, captcha, biometría de huella dactilar, control de acceso, y clasificación de información; por lo que la fuga de información sensible se redujo al 0% debido a la eficacia del método. Para un sistema de gestión documental, así como para cualquier otro sistema informático, es fundamental disponer permanentemente de módulos de autenticación y control de acceso y un módulo de reporte rápido para la toma de decisiones.

Sun, y otros [28], realizaron la investigación, *A lightweight multi-factor mobile user authentication scheme*; en la Universidad de Ingeniería Harbin, China. Los teléfonos inteligentes, debido a su amplio almacenamiento y contenido de información privada, son utilizados para realizar transacciones financieras, compras en línea, entre otras actividades personales y/o profesionales. Debido a los ataques de malware, ataques cibernéticos y robo de los mismos, se ha incrementado el acceso no autorizado, quebrantando la seguridad de estos dispositivos. El esquema implementado consta de registro, inicio de sesión y actualización. En la fase de registro, el usuario elige su ID y contraseña, ingresa su número de teléfono e incorpora la Identidad Internacional del Equipo Móvil – IMEI; luego el servidor almacena la información en la base de datos. Durante la fase de inicio de sesión, el usuario debe ingresar su ID y contraseña; el servidor genera un número aleatorio que es enviado al teléfono móvil, el cual es ingresado por el usuario y que a la vez es validado por el servidor. En la fase de actualización, el usuario puede actualizar su contraseña localmente sin contacto con el servidor. El algoritmo propuesto se expuso a ataques de repetición, hombre en el medio, acceso no autorizado, suplantación de identidad, phishing, adivinanza de contraseñas, pérdida de teléfono, información privilegiada y denegación de servicio. El 100% de estos ataques fueron detectados. El esquema se puede implementar en procesos de

autenticación en equipos móviles y escenarios donde se tenga que proteger información privada y confidencial.

Iftikhar, Hussain, Mansoor, Ali & Chaudhry [29], realizaron la investigación, *Symmetric-Key Multi-Factor Biometric Authentication Scheme*; en la Universidad de Islamabad, Pakistan. Los esquemas de autenticación multifactor existentes siguen siendo vulnerables y tienen lagunas en términos de ataques de reflexión; asimismo, el tiempo de ejecución es relativamente largo. El esquema propuesto consta de registro e inicio de sesión y autenticación, para lo cual, hace uso de contraseña, característica biométrica, función One-wayHash y tarjeta inteligente. En la etapa de registro, el usuario legítimo C presenta la identidad ID, contraseña PW y biométrica B al centro de registro R. Luego R envía a la tarjeta inteligente ID, PW, B y K. Luego realiza el proceso de Reinscripción y verifica el valor de v. Si el valor de v = vi, entonces la tarjeta inteligente tiene EID. En el Inicio de sesión y autenticación entre el usuario y el servidor, la plantilla biométrica B y el número aleatorio K del usuario C, se obtiene de la tarjeta inteligente; si h (B y K) es igual a f, entonces el usuario puede proceder. Cuando C proporciona el ID y PW, se calculan algunas ecuaciones. El EID se calcula con una tarjeta inteligente. El usuario envía una solicitud a EID, M2, M3 al servidor S para iniciar sesión, luego envía un mensaje al servidor S desde el usuario C. El servidor verifica el EID enviado por C. El S verifica que el EID enviado por C coincida con el EID guardado en la base de datos. Entonces, cuando el servidor S recibe M enviado por el usuario C, verifica M en la base de datos, si coincide, el usuario C y el servidor S se autentican entre sí. La herramienta utilizada para analizar el esquema propuesto fue ProVerif, por medio de la cual se realizó cuatro consultas, arrojando un valor verdadero en todas ellas. Las tres primeras consultas indican conexión entre usuario y servidor; mientras que la cuarta indica que no hay ataque posible. Asimismo, arrojó un costo de comunicación de 1024 bits y un tiempo de ejecución de 0.00576 ms. El esquema de autenticación biométrica multifactor propuesto resulta seguro y protegido contra ataques conocidos, por lo que su empleo en sistemas de identificación de usuarios resulta apropiado.

Uluagac, Liu & Beyah [30], realizaron la investigación, *A multi-factor re-authentication framework with user privacy*; en la Universidad de Miami, EEUU. La autenticación de usuarios en Internet juega un papel importante, sobre todo en sistemas altamente sensibles como el comercio minorista en línea y la banca electrónica, por lo que el uso de solo contraseñas resulta insuficiente porque presentan muchas debilidades, como el descifrado de contraseñas, la susceptibilidad al phishing y la reutilización de contraseñas entre sitios. La arquitectura del marco tiene cuatro componentes principales; (1) un programa de adquisición de perfiles de código abierto (PAP) que se ejecuta en el host local del usuario; (2) una base de datos de perfil de usuario (UPDB) que almacena la información del usuario de una manera que preserva la privacidad; (3) un servidor de autenticación (AS) que procesa y valida las solicitudes de autenticación del usuario en el servidor; y (4) un servidor de contenido. El marco de autenticación, durante el registro del usuario, crea, codifica y encripta su perfil con clave pública. Luego, el ID, contraseña y perfil del usuario, pasa al AS, quien interactúa con la UPDB. Cada vez que el usuario se autentique, ingresará su ID y contraseña, siendo el AS el encargado de determinar la identidad del usuario. De ser verdadera, enviará un ticket de servicio al usuario conteniendo un ID de sesión y una contraseña de un solo uso. El marco propuesto comprobó que mientras se prolongue más el tiempo de recojo de datos, se mejora el rendimiento del sistema, tanto en recuperación (Recall), como en tasa de falsos positivos (FPR). Cuando el tiempo de recopilación de datos es tan largo como 30 minutos, se logra un resultado óptimo con una recuperación del 80.8% y una FPR del 14.7%. Sin embargo, la usabilidad disminuye. En cuanto a la utilización de recursos, el marco propuesto requiere un promedio del 3% de los recursos de la CPU y 15 MB de RAM aproximadamente. El marco propuesto es indicado para sistemas sensibles, así como también para equipos de escritorio, redes corporativas, redes sociales, y demás aplicaciones donde se almacene información confidencial y personal.

He, Neeraj, Lee & Sherratt [31], realizaron la investigación, *Enhanced three-factor security protocol for consumer USB mass storage devices*; en la Universidad de Wuhan,

China. Los bus serie universal (USB), al ser utilizados como dispositivos de almacenamiento masivo (MSD) está propenso a que cualquier persona lea o robe de manera fácil la información contenida en él, debido a que ésta es almacenada sin formato, permitiendo al usuario no autorizado, interceptar y alterar la información transmitida debido a la inseguridad que presenta el canal de transmisión entre la computadora y el dispositivo. El protocolo propuesto implementa tres fases (registro, verificación y cifrado de datos, y acuerdo clave). En la fase de registro, el usuario U ingresa su característica biométrica y proporciona su contraseña pw e ID de identidad, y la envía al servidor de autenticación (AS). Al recibir los datos, AS calcula eu y su, y los guarda en el dispositivo de almacenamiento de forma segura. En la fase de verificación y cifrado de datos, cuando el usuario quiere acceder al USB MSD deberá ingresar su ID, pw y característica biométrica. El dispositivo verifica si los datos ingresados son iguales. Si son iguales, el dispositivo genera un número aleatorio z y lo envía a AS, quien verifica la identidad del usuario. Si no es cierto, rechaza la solicitud; de lo contrario, AS genera un número al azar b y envía el mensaje m a U. Al recibir el mensaje m, AS verifica si son iguales, autenticando a U o deteniendo la sesión. En la tercera fase (acuerdo clave), efectuada la autenticación de forma recíproca, una clave cifrada K=h (ID n) es calculada por U, quien, al intentar acceder al USB MSD, hace uso de la clave para cifrar un archivo como E, garantizando la integridad de la información almacenada en el dispositivo. Cuando U requiere descifrar el archivo, sigue los mismos pasos en el MSD. El total del costo computacional de los protocolos de Yang et al., Lee et al., y el protocolo propuesto ascienden a 0.20488s, 0.08248s y 0.09958s respectivamente. Si bien es cierto, el protocolo propuesto tiene un ligero costo adicional, elimina las falencias que presenta el protocolo de Lee et al., por lo que resulta adecuado debido a su confiabilidad y eficiencia computacional.

Aldwairi & Aldhanhani [32], realizaron la investigación, *Multi-Factor Authentication Systems*; en la universidad Jordan. El mundo gira en torno al intercambio de información, por lo que la importancia de la autenticación juega un papel sumamente importante para

controlar el acceso a datos y sistemas confidenciales, preservar la privacidad y disuadir el robo de identidad. El sistema propuesto consta de cuatro etapas de autenticación. Para la primera etapa, durante el registro, los usuarios dibujan un patrón haciendo clic en una cuadrícula y seleccionando un mínimo de 8 cuadros. Para pasar la primera etapa, se muestra la misma cuadrícula, pero con un carácter aleatorio dentro de cada cuadro. Los usuarios deben seguir el mismo patrón y escribir los caracteres correspondientes en los cuadros. En la segunda etapa, los usuarios eligen un código de acceso numérico (PIN) al registrarse. Durante el inicio de sesión, deben ingresar cinco caracteres seleccionados de un conjunto de diez caracteres con posiciones correspondientes a los dígitos del código de acceso. Se usa el mismo conjunto de caracteres de la etapa uno, se muestra al azar y se actualiza después de un tiempo de espera. Para la tercera etapa, el sistema proporciona a los usuarios un valor inicial que deberán ingresar en la aplicación de su teléfono inteligente para generar un código de acceso para ingresar al sistema. Para la cuarta etapa, los usuarios deberán responder dos preguntas de seguridad seleccionadas al azar de un conjunto de preguntas (al menos tres) creadas en el registro. El sistema solicita al usuario que cree preguntas sobre hechos que solo pueden responder. El sistema se bloquea durante 15 minutos, después de cinco intentos fallidos de inicio de sesión. También usa el cierre de sesión automático por inactividad. En la etapa uno, la probabilidad de adivinar el patrón correcto llega a 2.688E-42 cuando el número de cuadrados es igual a 36. Para el caso específico de nuestra implementación, utilizamos cinco caracteres y eso hace que la probabilidad sea 3.3E-5. A medida que aumenta el número de cuadros seleccionados, la probabilidad disminuirá, sin embargo, con ocho seleccionados, la probabilidad total para ambas etapas es igual a 2.7E-17. El factor múltiple es una técnica de autenticación popular y está obteniendo una amplia aceptación para otorgar acceso a servicios críticos.

Justificación e importancia del estudio

Para que una persona no autorizada pueda suplantar la identidad y/o disponer de información sensible, crítica o confidencial, lo primero que tiene que hacer es accesar al sistema o red informática. Es ahí donde el proceso de autenticación juega un papel transcendental para preservar la confidencialidad, integridad y disponibilidad de la información; por ello, y por lo descrito en la realidad problemática del presente trabajo de investigación, se hace necesario la implementación de un método de autenticación más confiable y robusto, sin dejar de lado la usabilidad, que permita, no solo combinar más de un método de autenticación para contrarrestar las debilidades de los mecanismos de un solo factor, como es el uso del afamado usuario y contraseña, si no que, también brinde la alternativa de usar más de un medio para recibir la clave TOTP en caso de prescindir del celular, y de esta forma poder mitigar la suplantación o robo de identidad.

1.2. Formulación del Problema

¿Qué método de identificación de usuarios flexible permitirá mitigar la suplantación de identidad en el proceso de voto electrónico no presencial?

1.3. Hipótesis

Mediante la implementación de un método de identificación de usuarios basado en autenticación multifactor se mitigará la suplantación de identidad en el proceso de voto electrónico no presencial.

1.4. Objetivos

Objetivo general

Implementar un método de identificación de usuarios basado en autenticación multifactor que permita mitigar la suplantación de identidad en el proceso de voto electrónico no presencial.

Objetivos específicos

- Seleccionar los principales métodos de autenticación en la identificación de usuarios.
- Diseñar un método de autenticación multifactor que mitigue la suplantación de identidad.
- Codificar el método de autenticación multifactor que mitigue la suplantación de identidad en una plataforma web.
- Desarrollar pruebas de suplantación de identidad para accesar al módulo de voto electrónico no presencial.

1.5. Teorías relacionadas al tema

1.5.1. Seguridad informática

Gómez [33], sostiene que la seguridad informática es toda medida adoptada para evitar la ejecución de procesos no autorizados en una red o sistema informático, cuyos efectos dañen la información almacenada, comprometan su confidencialidad, autenticidad o integridad, bloqueen el acceso de usuarios, mermen la productividad y/o generen pérdidas económicas.

Por su parte, Baca [34], define a la seguridad informática como, disciplina que se basa a las normas internas y externas de la empresa para proteger la integridad y confidencialidad de la información almacenada en un sistema informático, ante todo tipo de admonición, con la firme intención de mitigar los riesgos físico y/o lógicos, a los que se expone.

Seguridad informática, como la define Paucar [35], son medidas para evitar la ejecución de procesos no autorizados en una red o sistema informático, las mismas que pueden ser procedimientos, reglas, instructivos, planes o herramientas.

1.5.2. ISO/IEC 27001

La ISO/IEC 27001 es el estándar internacional principal y certificable de las normas que forman la serie 27000, mediante el cual se proporciona los requisitos para que las empresas o entidades implementen un Sistema de Gestión de Seguridad de la Información.

En nuestro país, a través de la Resolución Ministerial N° 129-2012-PCM, el gobierno, aprueba la Norma Técnica Peruana “NTP-ISO/IEC 27001:2008 EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información. Requisitos”. Asimismo, exige el cumplimiento de dicha norma a las entidades que conforman el Sistema Nacional de Informática, con el firme propósito de normalizar, en las entidades nacionales, la administración de la seguridad de la información.

A través de la implementación de un método de identificación de usuarios basado en autenticación multifactor, se estaría dando cumplimiento a objetivos de control y controles, propios de esta norma certificable, tales como: A.10.6.1 – Controles de red, debido a que lograría y mantendría la seguridad en la red, sistemas y aplicaciones de usuarios. A.10.10.1 – Registro de auditoría, el acceso de los usuarios sería registrado, con el propósito de asistir a auditorías y monitoreo de accesos. A.10.10.4 – Registros de administrador y operador, el registro de las actividades de los usuarios que accedan al sistema, al margen del perfil que posea. A.11.4.2 – Autenticación de usuarios para conexiones externas, la autenticación multifactor mitigaría el acceso no autorizado a los usuarios que se conecten de manera remota. A.11.5.1 – Procedimientos seguros de conexión, el uso de más de un factor de autenticación permite el acceso seguro a los servicios de información. A.11.5.2 – Identificación y autenticación del usuario, lo cual se consigue no solo con el tradicional usuario y contraseña, sino que, además se necesitará de un factor adicional para lograr tener acceso al sistema, garantizando la identidad del usuario. A.11.5.3 – Sistema de gestión de contraseñas, el factor adicional lo constituirá una clave de un solo uso, la cual será única por cada inicio de sesión.

1.5.3. Identificación

La identificación es la afirmación de quiénes somos. Esto incluye quién afirmamos ser como persona, quién dice ser el origen de un correo electrónico, qué autoridad afirmamos tener o transacciones similares. El proceso de identificación no implica la verificación o validación de la identidad que se reclama, de ello se encarga la autenticación, y es una transacción separada [36].

La identificación consiste en la comparación entre la información ingresada por el usuario y la información almacenada previamente en la base de datos [37].

1.5.3.1. Verificación de identidad

La verificación de identidad precede a la identificación, y antecede la autenticación. Se utiliza en nuestras interacciones personales, pero también en los sistemas informáticos. Cuando se envía un correo electrónico, la identidad que se proporciona es considera verdadera, sin que se tome medidas adicionales para autenticarnos. Tales brechas en la seguridad contribuyen a la enorme cantidad de tráfico de spam que vemos, que se estima que representó el 56.26% del total de correos electrónicos enviados en el tercer trimestre de 2019 [38].

1.5.3.2. Autenticación

Modo que aporta el usuario que permita verificar que es quien dice ser, ya sea mediante el uso de una contraseña, posesión de un objeto o característica biométrica [39].

El Organismo Internacional de Normalización - ISO [40], a través de su norma ISO/IEC 27000:2018, afirma que la autenticación es un proceso que garantiza y confirma la identidad del usuario, por lo cual, es un aspecto básico en la seguridad de la información, que permite salvaguardar los tres pilares de la seguridad de la información, como son: confidencialidad, integridad y disponibilidad.

Para Romero, y otros [41], la autenticación es un proceso en el que se busca confirmar algo como verdadero, no se busca verificar un usuario, ya que la autenticación no siempre está relacionada con éstos, en muchos casos se requiere saber si un cambio o un dato es correcto, no se debe cometer el error que solamente las personas necesitan este proceso, este puede ser para cualquiera, un sistema, un dispositivo, una persona.

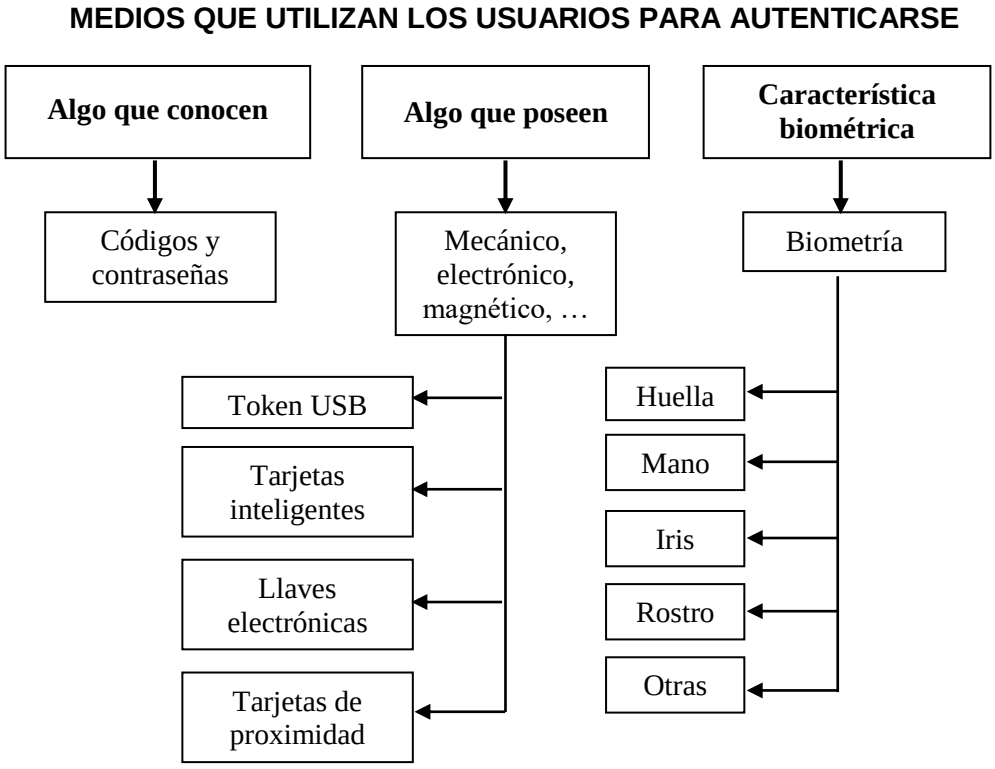


Figura 1. Medios que utilizan los usuarios para autenticarse.
Fuente: [57].

1.5.3.3. Proceso de autenticación

Para el National Institute of Standards and Technology - NIST, [42], en su publicación especial de junio del 2017, afirma que el proceso de autenticación establece la identidad del Reclamante R ante el Verificador V. Este proceso inicia cuando R demuestra el conocimiento, la posesión y/o el rasgo inherente, está vinculado a la identidad afirmada a V, a través de un protocolo de autenticación (AP). Demostradas una o más características, V interactúa con el proveedor de servicios de credenciales (CSP) para determinar si la credencial sigue siendo válida.

El proceso de autenticación permite asegurar que la identidad que asevera tener el usuario es verdadera; por consiguiente, debe proporcionar herramientas lo suficientemente robustas para poder comprobar la identidad del reclamante [43].

Durante el proceso de autenticación, la interacción entre V y R es lo más importante, pues de ello depende la seguridad del sistema. Por consiguiente, la protección de la integridad y confidencialidad del tráfico entre V y R durante y después del proceso de autenticación, depende de que tan efectivo es el protocolo diseñado, ya que limitará o eliminará los efectos negativos que puede ocasionar un atacante.

1.5.3.4. Protocolo de autenticación (AP)

NIST [42], define a un AP como la secuencia definida de mensajes entre R y V que demuestra que R tiene el control de un token válido para establecer su identidad y, opcionalmente, demuestra a R que se está comunicando con el Verificador previsto. Un intercambio de mensajes entre R y V que resulta en autenticación (o negación de autenticación) entre las dos partes es una ejecución del AP. Durante o después de una ejecución exitosa del AP, se puede crear una sesión de comunicación protegida entre ambas partes; la cual se puede usar para intercambiar, tanto los mensajes restantes de la ejecución del AP o los datos de sesión entre las dos partes.

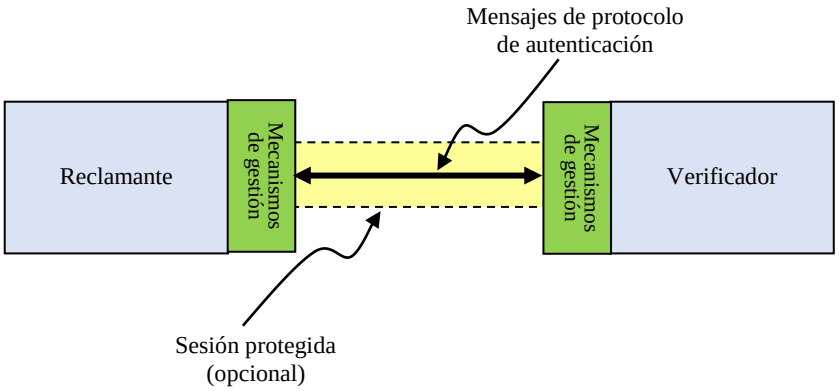


Figura 2. Modelo de proceso de autenticación.
Fuente: [42].

Una vez autenticado, los usuarios de la información tendrán distintos privilegios sobre ella, que puede ser de solo lectura o lectura y escritura [44].

1.5.4. Autenticación multifactor

Kim, Kang, Jo, & Oakley [45], refieren que la autenticación multifactor es un mecanismo de seguridad que presenta más de un tipo de esquema o factor de autenticación, los mismos que proporcionan protocolos de seguridad más sólidos y confiables.

El objetivo de la MFA es la creación de una defensa a través de capas, dificultando, de esta manera, a que personas no autorizadas, accedan a ubicaciones físicas, dispositivos informáticos, redes o base de datos. Si un atacante vulnera un factor, tendrá por lo menos un factor más que vulnerar para poder cumplir con su objetivo [46].

La MFA combina de dos a más factores de autenticación. Los métodos de MFA más conocidos son a través del conocimiento, propiedad y herencia [47]; respecto al conocimiento, por lo general es una contraseña; en cuanto a la propiedad, puede ser una tarjeta inteligente; en lo que se refiere a herencia, conocida también como autenticación biométrica, puede ser un rasgo físico como huella digital [48].

En un método de MFA, el factor de verificación adicional no se ejecuta mientras no se haya corroborado que la contraseña ingresada por el usuario sea la misma que está almacenada en la base de datos. Asimismo, si el atacante lograría obtener la contraseña del usuario, al no tener el teléfono (posesión), o la huella digital (inherencia), no podrá completar el proceso de inicio de sesión [49].

El Grupo Evidian [50], afirma que en la autenticación multifactor, para que el usuario pueda autenticarse, debe proporcionar al menos dos elementos, siendo los de mayor uso, los siguientes:

1.5.4.1. Identificador y contraseña

Este tipo de autenticación es el más conocido y utilizado, debido a su simplicidad. El nivel de seguridad de este método depende de que tan compleja sea la contraseña.

1.5.4.2. Identificador y contraseña TOTP

A través de este método de autenticación, el usuario posee un dispositivo especializado que, por medio de una solicitud, genera una contraseña de un solo uso y con una duración temporal; es decir, en un nuevo inicio de sesión, se deberá generar una nueva contraseña.

1.5.4.3. Certificados PKI sobre tarjetas inteligentes o Token USB

Los certificados con Infraestructura de clave pública (PKI – Public Key Infrastructure) utilizan una tecnología avanzada de codificación, la misma que a través de una clave, permite firmar mensajes. Para que el usuario pueda hacer uso de los diferentes elementos criptográficos que posee la tarjeta inteligente o token, debe proporcionar una clave o código PIN. Estos certificados digitales son proporcionados por una autoridad de certificación, que en nuestro país es el Registro Nacional de Identificación y Estado Civil (RENIEC).

1.5.4.4. Identificador y contraseña sobre una tarjeta inteligente

La tarjeta inteligente almacena el ID y contraseña del usuario, los mismos que garantizaran la posesión y conocimiento en un proceso de autenticación. La complejidad de la contraseña dependerá del usuario, la misma que puede ser cambiada de forma regular.

1.5.4.5. Biométrica

Este tipo de autenticación se basa en la verificación de un rasgo físico del usuario, ya sea a través de la huella digital, iris, rostro, mano, etc., los mismos que pueden almacenarse en una tarjeta inteligente, o ingresados directamente a través de un dispositivo biométrico.

1.5.4.6. Definición sin contacto

Un chip con tecnología de Identificación por Radiofrecuencia (RFID – Radio Frequency Identification) es adherido a una tarjeta y posee un número de identificación, el cual es asociado a un usuario, ya sea de sistemas informáticos, ambientes restringidos, entre otros. Esta tarjeta transmite la identidad del usuario por medio de ondas de radio, sin necesidad de tener contacto directo con el dispositivo lector.

1.5.5. Suplantación de identidad

El Diario Gestión [51], describió dentro de su contenido, la definición de suplantación de identidad, proporcionada por el jurista Aldo Cárdenas, quien refiere que la suplantación de identidad consiste en que una persona se hace pasar por otra de forma fraudulenta, con el propósito de accesar a sus cuentas bancarias, disponer de información privilegiada o tener acceso a beneficios propios de un usuario legítimo.

Los términos “robo de identidad” y “suplantación de identidad” suelen utilizarse con el mismo propósito. Sin embargo, la Asociación Portuguesa de Apoyo a la Víctima [52], hace una distinción entre estos dos términos, definiendo al robo de identidad como la obtención de información personal sin su conocimiento o consentimiento; mientras que la suplantación de identidad es el uso de la identidad de otra persona en alguna actividad, ya sea para la solicitud de créditos, bienes o servicios en nombre de la víctima o para el uso fraudulento de información de la víctima.

Un atacante puede suplantar la identidad de otra persona de diversas formas, ya sea haciendo uso en forma directa del dispositivo o equipo de cómputo de la víctima, obteniendo de diversas formas el ID y contraseña de acceso, así como también falsificando o clonando las identificaciones digitales o electrónicas [35].

En lo que respecta a la gestión de riesgos, el Instituto Nacional de Tecnologías de la Comunicación – INTECO [37], refiere que la suplantación de identidad, como en cualquier método de autenticación, representa una de las principales amenazas.

1.5.6. Voto electrónico no presencial

Antes de dar la definición de voto electrónico no presencial (VENP), definiremos lo que es el voto electrónico (VE). Busaniche [53], define al VE como todo sistema informático diseñado para el acto de emitir y escrutar los votos en una mesa de sufragio a través de dispositivos electrónicos, donde los electores acuden para expresar su voluntad popular. Estos dispositivos electrónicos pueden ser computadoras, laptops, tablets, cabinas de votación electrónicas, entre otros dispositivos semejantes, los cuales permiten realizar la emisión y conteo automático de los votos.

Por su parte, la Oficina Nacional de Procesos Electorales – ONPE [54], entidad encargada de planificar, organizar y ejecutar los procesos electorales, referéndum y otros tipos de consulta popular en nuestro país, define al VE como una forma de sufragar haciendo uso de medios electrónicos para automatizar los tres momentos de la jornada electoral (instalación, sufragio y escrutinio), ofreciendo una solución tecnológica, confiable, accesible y segura.

Respecto al voto electrónico no presencial, o voto electrónico por Internet, Busaniche [53], afirma que se trata de mecanismos que permiten emitir su voto desde una computadora, laptop, tablet o celular, que cuente con conexión a Internet, permitiendo a los electores emitir su voluntad desde sus propios hogares, sitios de acceso público, e incluso desde otro país.

Para Qureshi, Megías & Rifa-Pous [55], refieren que el voto electrónico no presencial permite a los electores, emitir su voto desde cualquier dispositivo informático que tenga acceso a Internet, en cualquier parte del mundo, permitiendo de esta manera a los electores beneficios como accesibilidad y conveniencia.

En nuestro país, el VENP es un sistema de votación electrónica que hace uso de una aplicación administrada por la ONPE, la misma que permite al elector expresar su voluntad popular haciendo uso de un dispositivo electrónico conectado a Internet, con altas previsiones de seguridad [54].

Uno de los grandes problemas que presenta este tipo de votación es la identificación del elector, lo cual resulta imprescindible para asegurar la transparencia del mecanismo. A través de un método de autenticación robusto se evitaría que un elector sufrague en nombre de otra persona, emita su voto más de una vez, o que vote sin estar habilitado para hacerlo.

En la actual forma de sufragar, a través del VENP, se utiliza un sobre ciego en donde se indica el PIN y contraseña de elector/afiliado, adicional a ello, la aplicación solicita un código de verificación que muestra en la pantalla para poder continuar con la votación.

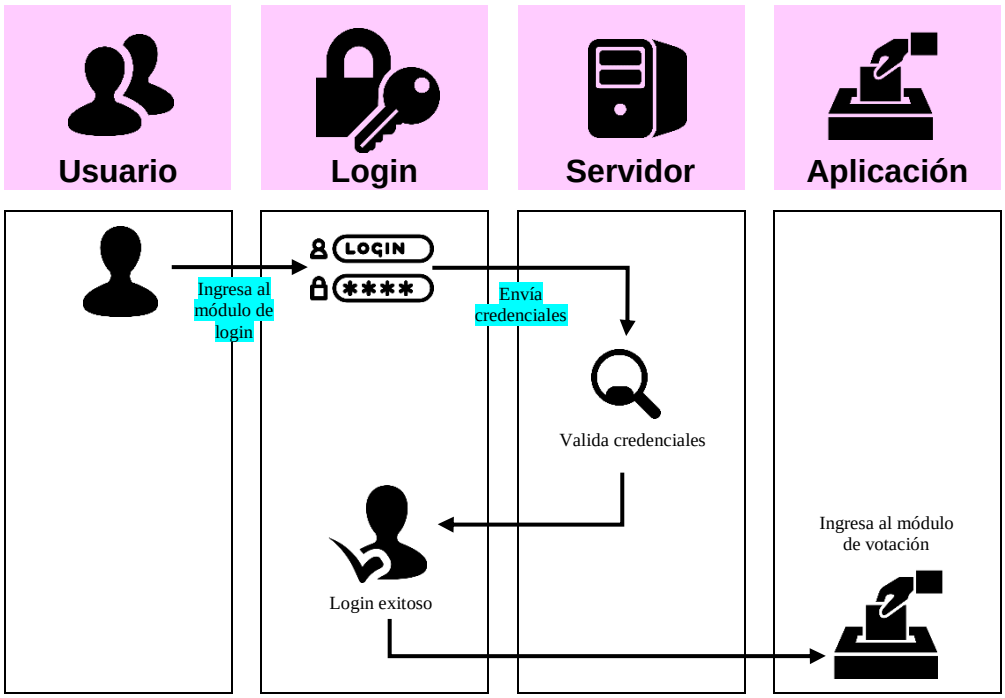


Figura 3. Proceso actual de autenticación en el VENP en nuestro país.
Fuente: Elaboración propia.

II. MATERIALES Y MÉTODO

2.1. Tipo y diseño de investigación

2.1.1. Tipo de investigación

El tipo de investigación es cuantitativa. Este tipo de investigación utiliza técnicas estadísticas, matemáticas y computacionales, a través de las cuales se obtuvo los resultados de nuestra investigación.

2.1.2. Diseño de investigación

El diseño de investigación es cuasi-experimental, debido a que la muestra de estudio se seleccionó por conveniencia y en base a los objetivos de la investigación.

2.2. Variables, operacionalización

Tabla 1

Operacionalización de variables.

Variables	Dimensión	Indicador	Fórmula	Técnica e instrumentos de recolección de datos
V.I. Método de identificación de usuarios	Consumo de recursos	Consumo de CPU	$Cc = \sum_{j}^{n} \frac{cc_j}{n}$	Registro electrónico
		Consumo de memoria	$Cm = \sum_{j}^{n} \frac{cm_j}{n}$	
		Tiempo de respuesta	$Tr = \sum_{j}^{n} \frac{tf_j - tf_i}{n}$	
V.D. Suplantación de identidad	Identificación	Precisión	$Precisión = \frac{VP}{VP + FP}$	
		Recall	$Recall = \frac{VP}{VP + FN}$	
		Exactitud	$Exactitud = \frac{VP + VN}{VP + VN + FP + FN}$	

2.3. Población y muestra

2.3.1. Población

Entre los métodos de autenticación de usuarios tenemos: identificador y contraseña, OTP, TOTP, token USB, tarjeta inteligente PKI, llave, tarjeta inteligente con identificador y contraseña, soluciones biométricas, RFID activo, entre otros.

2.3.2. Muestra

Se realizó un muestreo por conveniencia, el cual es una técnica de muestreo no probabilístico y no aleatorio. Los métodos seleccionados son el uso de contraseña y TOTP, los mismos que se eligieron después de realizar un análisis de los métodos de autenticación existentes y en base a los objetivos de la investigación.

El uso de contraseña, como mecanismo de protección, es el más implementado por las empresas [13]. El uso de TOTP en un proceso de autenticación agrega un factor adicional además de la contraseña, [56], logrando tanto la seguridad como la usabilidad [26]. Asimismo, esta contraseña solo podrá ser utilizada una sola vez y durante un tiempo determinado, ya que, para un próximo proceso de autenticación, se generará una nueva contraseña de acceso [10], garantizando de esta manera la identidad del usuario.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Para la presente investigación se utilizó instrumentos mecánicos y electrónicos, debido a que se realizaron mediciones y registro de métricas como el consumo de CPU, consumo de memoria, tiempo de respuesta, precisión, recall y exactitud, cuyas fórmulas se detallan en la Tabla 1. Los resultados del consumo de CPU, consumo de memoria y el tiempo de respuesta, fueron registrados en el formato del anexo 2.

2.5. Procedimiento de análisis de datos

Para evaluar el método de autenticación de usuarios se utilizó los siguientes indicadores:

Consumo de CPU:

$$Cc = \sum_{j}^{n} \frac{cc_j}{n}$$

Donde:

Cc: Consumo de CPU

Cc_j: Consumo de CPU en la prueba j

n: Total de pruebas

Consumo de memoria:

$$Cm = \sum_{j}^{n} \frac{cm_j}{n}$$

Donde:

Cm: Consumo de memoria

Cm_j: Consumo de memoria en la prueba j

n: Total de pruebas

Promedio de tiempo de respuesta:

$$Tr = \sum_{j}^{n} \frac{tf_j - tf_i}{n}$$

Donde:

Tr: Tiempo de respuesta

Tf_j: Tiempo final de respuesta

Tf_i: Tiempo inicial de respuesta

n: Total de pruebas

Precisión.

Permite medir la calidad del método de autenticación en la identificación de usuarios. Es decir, mide la proporción de casos identificados como positivos que son realmente positivos.

$$Precisión = \frac{VP}{VP + FP}$$

Donde:

VP = Total de verdaderos positivos.

FP = Total de falsos positivos.

Recall (Exhaustividad).

Nos informa sobre la cantidad de usuarios que el método de autenticación es capaz de identificar. Es decir, mide la proporción de casos positivos que se han identificado correctamente.

$$Recall = \frac{VP}{VP + FN}$$

Donde:

VP = Total de verdaderos positivos.

FN = Total de falsos negativos.

F1-Score

Proporciona una medida equilibrada de la precisión y el recall. Es decir, la precisión y el recall tienen igual importancia.

$$F1 - score = 2\frac{precisión * recall}{precisión + recall}$$

Donde:

precisión = Casos positivos realmente positivos.

recall = Casos positivos identificados correctamente.

2.6. Criterios éticos

Derechos de autor

La presente investigación respeta la autoría y propiedad intelectual de cada una de las investigaciones citadas y referenciadas para respaldar la autenticidad de la información.

Confidencialidad

La identidad de las instituciones y participantes en la investigación se mantuvo en anonimato, salvo consentimiento expreso de las mismas.

Búsqueda del bien

Debido al exponencial crecimiento de delitos informáticos, y sobre todo de los delitos de suplantación de identidad, esta investigación genera un aporte para la seguridad de la información, ya que a través de un método de autenticación flexible que combine más de un factor de autenticación, se mitiga el acceso no autorizado a sistemas informáticos y la suplantación de identidad.

Fiabilidad

El método implementado obtuvo resultados estables y consistentes debido a que se aplicó fórmulas que permiten minimizar el margen de error y garantizan la fiabilidad de la investigación.

Transferibilidad

Los resultados obtenidos podrán ser transferidos a cualquier investigador que pretenda seguir con la misma línea de investigación.

III. RESULTADOS Y DISCUSIÓN

3.1. Resultados en Tablas y Figuras

Implementado el método de identificación de usuarios, se procedió a realizar las mediciones de acuerdo a los indicadores de la investigación, tales como consumo de CPU, consumo de memoria y tiempo de respuesta. Para ello se hizo uso de herramientas informáticas como el Monitor de Recursos del Administrador de Tareas de Windows y WebPageTest.

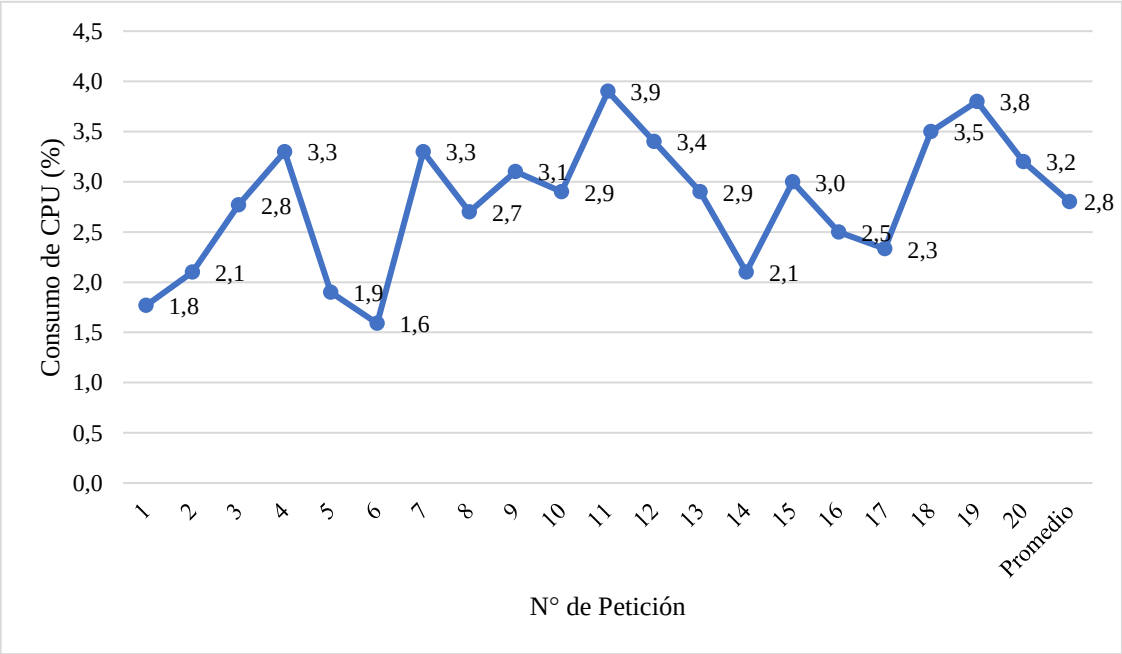


Figura 4. Consumo de CPU.
Fuente: Elaboración propia.

En la figura 4 se aprecia el consumo del CPU, el cual arroja un consumo promedio del 2.8% del total disponible. Asimismo, alcanzó picos de hasta el 3.9% y valores mínimos del 1.6%. Esta información refleja el bajo consumo del procesamiento al momento de la verificación de las credenciales del usuario, permitiendo dejar libre un gran porcentaje de CPU para la ejecución de otras tareas propias del equipo informático y de las que el usuario crea conveniente hacer uso.

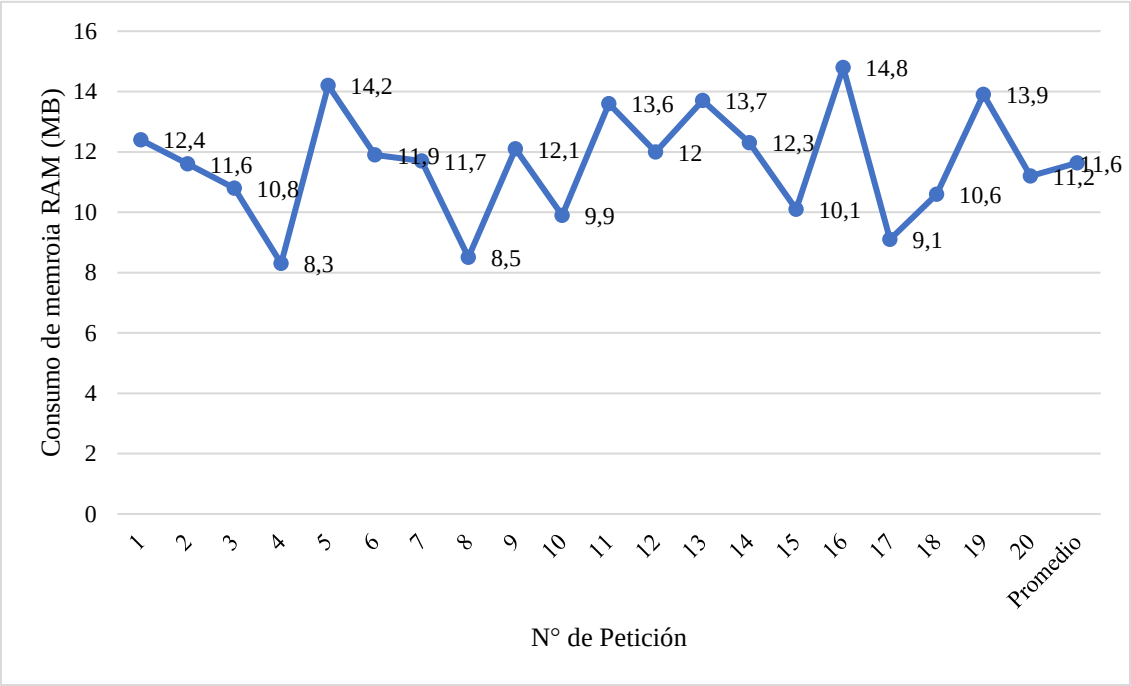


Figura 5. Consumo de memoria.
Fuente: Elaboración propia.

El consumo de la memoria RAM se midió a través del Monitor de Recursos del Administrador de Tareas de Windows, simulando solicitudes de usuarios. La memoria del equipo informático tiene una disponibilidad de 8.0 GB y con la simulación de solicitudes de usuario, alcanzó un uso de 11.6 MB, dejando disponible gran parte de memoria para que pueda ser empleada por otros usuarios y aplicaciones.

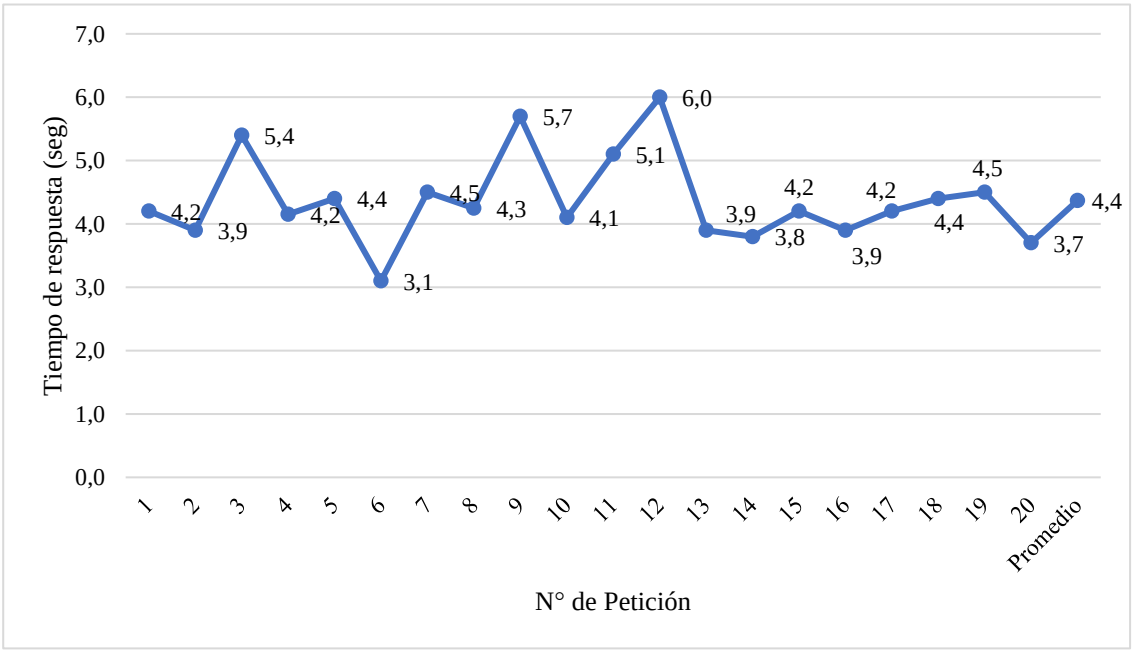


Figura 6. Tiempo de respuesta.
Fuente: Elaboración propia.

Para tomar el tiempo de respuesta de la aplicación web se empleó WebPageTest, la cual arroja un valor para la carga inicial y un valor para la carga total de la aplicación. En la figura 6 podemos visualizar el tiempo de respuesta de la aplicación, el cual arroja un tiempo de respuesta promedio de 4.4 segundos. Este indicador es muy importante en un proceso de autenticación múltiple, debido a que la aplicación se toma más tiempo en autenticar las credenciales del usuario y verificar que la TOTP ingresada es correcta, lo cual genera malestar al usuario, ya que tiene que esperar más tiempo para accesar a la aplicación que en un proceso de autenticación de un solo factor. Estos resultados pueden variar de acuerdo a la velocidad de conexión doméstica y a la distancia física del servidor.

Entre los indicadores a medir en la variable dependiente Suplantación de identidad, se encuentran la precisión, recall y exactitud. Para medir las métricas de rendimiento de esta variable hay cuatro parámetros involucrados en la evaluación de la detección de suplantación de identidad en la implementación del método propuesto: Verdadero positivo (TP), Verdadero negativo (TN), Falso positivo (FP) y Falso negativo (FN). Los valores de FP y FN deben minimizarse y los de TP y TN deben maximizarse. De estos valores derivan los indicadores: Precisión, Recall y Exactitud.

Tabla 2

Ataques efectuados al método de autenticación implementado.

Ataque	Pruebas	Aciertos	Fallas
Surf sobre el hombro	20	0	20
Fuerza bruta	20	0	20
Diccionario	20	0	20

Fuente: Elaboración propia

El ataque de surf sobre el hombro se probó en 20 usuarios, de los cuales, el 0% de los ataques tuvieron éxito; es decir, ninguno de los atacantes pudo accesar al módulo de votación. Asimismo, aunque los atacantes hubiesen podido obtener las credenciales del usuario, incluyendo la TOTP; esta última no sería la misma cuando el usuario desearía ingresar nuevamente a la aplicación web.

A través de la aplicación Hydra, la cual viene instalada y configurada en Kali Linux, la misma que es gratuita y de código abierto, se realizaron pruebas experimentales de ataques de fuerza bruta para comprobar si las contraseñas registradas por los usuarios son lo suficientemente fuertes o susceptibles a ser vulneradas, obteniendo como resultado que el 0% de las pruebas realizadas en los 20 usuarios fue capaz de completar el ataque, debido al segundo factor implementado; es decir, la TOTP que recibe el usuario para accesar al módulo de votación, llega a su celular y no se almacena en el dispositivo o equipo en donde realiza la autenticación, como si se da en el caso de la contraseña, imposibilitando de esta manera que el ataque de fuerza bruta se concrete, y por ende, la suplantación de identidad y el acceso no autorizado al módulo de votación se vea vulnerado.

Para la realización de las pruebas de ataques de diccionario, también se utilizó la aplicación Hydra, cuyos resultados fueron del 0% de éxito en las pruebas realizadas, debido a las consideraciones al momento de crear la contraseña y al segundo factor de autenticación implementado.

De los resultados obtenidos durante las pruebas de ataques efectuadas al método implementado, podemos determinar los valores de los indicadores, los cuales resultaron muy satisfactorios debido al segundo factor implementado.

Tabla 3

Porcentaje de rendimiento según indicadores.

Indicador	Porcentaje
Precisión	100%
Recall	100%
Exactitud	100%

Fuente: Elaboración propia

Los datos de la tabla 3 son muy alentadores, toda vez que ninguno de los ataques efectuados pudo vulnerar el método implementado, debido a que el atacante no tiene acceso al dispositivo que cumple la función de recepción para la TOTP en el segundo

factor de autenticación, como es en este caso, el celular personal del usuario; asimismo, cuando el usuario desea accesar nuevamente a la aplicación, recibirá otra TOTP para su acceso.

3.2. Discusión de resultados

Los resultados obtenidos en la investigación se compararon con los resultados de las investigaciones analizadas. Así tenemos que, a través del método propuesto en la investigación de Uluagac, Liu & Beyah [30], denominada *Implementation and evaluation of a multi-factor web authentication system with individual number card and webUSB*, alcanzó un consumo promedio del 3% de los recursos de la CPU, y 15 MB aproximado del consumo de la memoria RAM; mientras que el consumo de la CPU y de la memoria RAM del presente método implementado, obtuvo un consumo promedio de 2.8% y 11.6 MB respectivamente.

En la investigación realizada por Fujita, Inomata & Kashiwasaki [25], denominada *Implementation and evaluation of a multi-factor web authentication system with individual number card and webUSB*, obtuvo un tiempo de respuesta promedio de 3.5 segundos, y la comparó con el tiempo promedio de Rivert et al, el cual arrojo un valor de 17.6 segundos; mientras que el tiempo de respuesta del presente método de autenticación implementado arrojo un valor de 4.2 segundos.

Si bien es cierto, el método propuesto tiene un tiempo de respuesta superior al método de Fujita et al., soporta ataques de surf sobre el hombre, ataques de fuerza bruta y ataques de diccionario; por lo que resulta apropiado para el acceso a aplicaciones web. Asimismo, debido a que permite recibir la clave TOTP por celular, aumenta la usabilidad en procesos como elección de APAFA por medio del Voto electrónico no presencial.

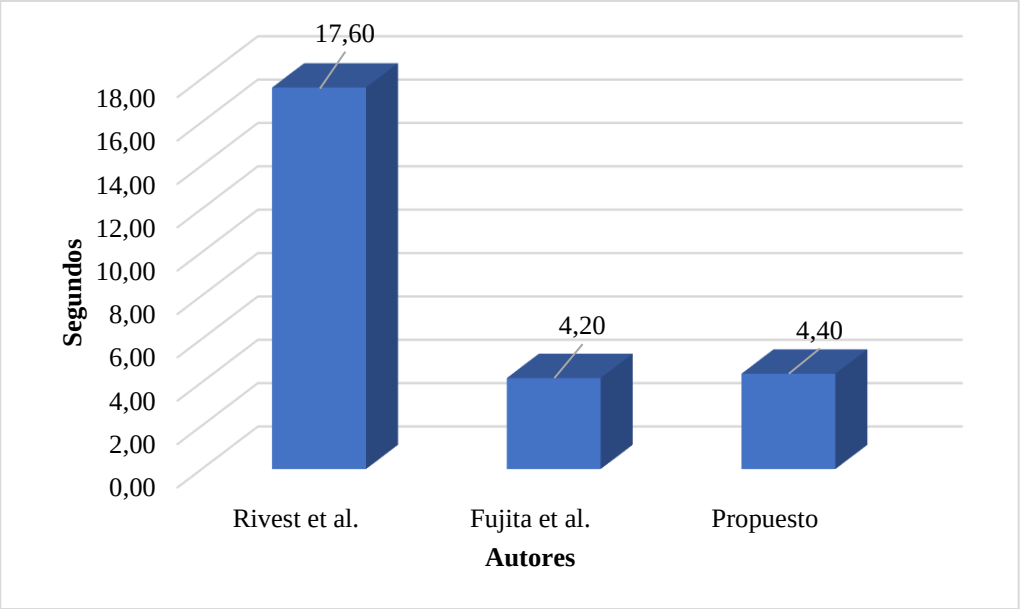


Figura 7. Comparación de tiempo de respuesta.
Fuente: Elaboración propia.

Kordzo, Dorgbefu & Banning [24], en su investigación, *Design and Implementation of Cost Effective Multi-Factor Authentication Framework for ATM Systems*; probó su marco propuesto con 100 usuarios bajo los siguientes ataques: navegación de hombro, registro de información del usuario, ingeniería social, adivinación de contraseñas y fuerza bruta, y ataques de diccionario. En la navegación de hombro, el 0% de los atacantes tuvieron éxito; en el registro de información del usuario, la tasa de falla es 100%; los ataques de ingeniería social tienen una tasa de éxito del 0%; la adivinación de contraseñas y fuerza bruta obtuvo el 0% de éxito. Los resultados de esta investigación coinciden con los de Kordzo, Dorgbefu & Banning, ya que se obtuvieron los mismos resultados en las pruebas de ataques realizados al método implementado. Coincidiendo también que el solo uso de usuario y contraseña para el acceso a sistemas informáticos resulta muy peligroso, debido a que no garantiza la confidencialidad e integridad de los recursos y la información que dispone, por lo que resulta necesario la implementación de más de un factor de autenticación en la identificación de usuarios.

Watanabe, Suzuki, Naito, & Watanabe [26], en su estudio *Proposal for user authentication method combining random number and password*, concluyen afirmando que el uso de contraseña y TOTP en la identificación de usuarios tiene un bajo costo y alta seguridad, coincidiendo con los resultados de esta investigación. Adicional a ello, el método propuesto, no tiene problemas de usabilidad, ya que no necesita de un dispositivo adicional al dispositivo móvil para recibir la TOTP, logrando de esta manera, la seguridad como la usabilidad, así como la suficiente fuerza contra ataques, ya que es seguro y económico.

Khattri & Singh [11], en su estudio, *Implementation of an additional factor for secure authentication in online transactions*; implementa un esquema de autenticación que incorpora la distancia entre el usuario y el ATM, identificando la ubicación del usuario y calcula la distancia entre el dispositivo donde se está realizando la transacción y el dispositivo móvil del usuario. Los resultados de la evaluación arrojaron una tasa de detección de fraude del 98.55% y una tasa de aciertos del 97.14%; mientras que la tasa de falsos positivos ascendió al 2% aproximadamente. Los resultados de esta investigación superan los de Khattri & Singh, ya que tienen una precisión del 100% tras haberse efectuado los ataques de surf sobre el hombro, ataques de fuerza bruta y ataques de diccionario.

3.3. Aporte práctico

La presente investigación tuvo como objetivo implementar un método de identificación de usuarios basado en autenticación multifactor que permita mitigar la suplantación de identidad en el proceso de voto electrónico no presencial.

Para ello, se identificó y seleccionó los principales métodos de autenticación en la identificación de usuarios; luego se diseñó un método de autenticación multifactor que mitigue la suplantación de identidad. Posteriormente, se codificó el método de autenticación multifactor en una plataforma web. Finalmente, se desarrollaron pruebas

de suplantación de identidad en el proceso de voto electrónico no presencial para determinar la efectividad del método implementado.

La selección de los métodos de autenticación en la identificación de usuarios, según lo indicado en el diseño de investigación y la selección de la muestra, fue por conveniencia y en base a los objetivos de la investigación. Asimismo, se realizó una revisión sistemática de la literatura científica publicada hasta el año 2022, en donde se comprobó que el identificador y contraseña es el medio normal de autenticación; es decir, es el primer factor de autenticación. Asimismo, se identificaron los métodos de autenticación adicionales y los periféricos más utilizados en la identificación de usuarios, los mismos que se detallan en la Tabla 04.

Tabla 04

Métodos de Autenticación y Periféricos más utilizados en la identificación de usuarios.

N°	Método	Periférico utilizado	Título de la investigación	Autor	Base de datos
1	Contraseña TOTP GPS	Dispositivo móvil.	*Implementation of an additional factor for secure authentication in online transactions*	Vipin Khattri & Deepak Kumar Singh	Journal of Organizational Computing and Electronic Commerce. DOI: 10.1080/10919392.2019.1633123
2	Contraseña TOTP Comportamiento	Token USB	*Design and Implementation of Cost Effective Multi-Factor Authentication Framework for ATM Systems*	Nuku Atta Kordzo Abiew, Samuel Osei Banning, Maxwell Dorgbefu Jnr.	Asian Journal of Research in Computer Science DOI: 10.9734/ajrcos/2020/v5i330135
3	Contraseña TOTP	Tarjeta inteligente	*Implementation and evaluation of a multi-factor web authentication system with individual number card and webUSB*	Yuki Fujita, Atsuo Inomata, Hiroki Kashiwaza	IEEExplore. DOI: 10.23919 / APNOMS.2019.8893134
4	Contraseña TOTP	Dispositivo móvil.	*Proposal for user authentication method combining random number and password*	Yuga Watanabe, Hidekazu Suzuki, Katsuhiro Naito, Akira Watanabe	IEEExplore. DOI: 10.1109 / GCCE46687.2019.9015618
5	Contraseña Característica biométrica	Lector biométrico	Implementación de los servicios de autenticación fuerte multifactor y confidencialidad, para la protección de documentación electrónica	Felipe Andrés Corredor, Leonel Álvarez Pabón, Diana Cristina Franco Mora, Andrés Felipe Ardila	IEEExplore. DOI: 10.18687 / LACCEI2015.1.1.247

6	Contraseña Característica biométrica	Dispositivo móvil. Lector biométrico	*A lightweight multi-factor mobile user authentication scheme*	Jianguo Sun, Qi Zhong, Liang Kou, Wenshan Wang, Qingan Da, Yun Lin	IEEExplore. DOI: 10.1109/INFCOMW.2018.8406952
7	Contraseña Característica biométrica	Tarjeta inteligente Lector biométrico	*Symmetric-Key Multi-Factor Biometric Authentication Scheme*	Jawad Iftikhar, Sajid Hussain, Khwaja Mansoor, Zeeshan Ali, Shehzad Ashraf Chaudhry	IEEExplore. DOI: 10.1109 / C-CODE.2019.8680999
8	Contraseña TOTP	Dispositivo móvil	*A multi-factor re-authentication framework with user privacy*	Selcuk Uluagac, Wenyi Liu, Raheem Beyah	IEEExplore. DOI: 10.1109 / CNS.2014.6997526
9	Contraseña Pregunta secreta TOTP	Dispositivo móvil	*Multi-Factor Authentication Systems*	Monther Aldwairi, Saoud Aldhanhani	IEEExplore. DOI: 10.23919 / ICITST.2017.8356383

Fuente: Elaboración propia.

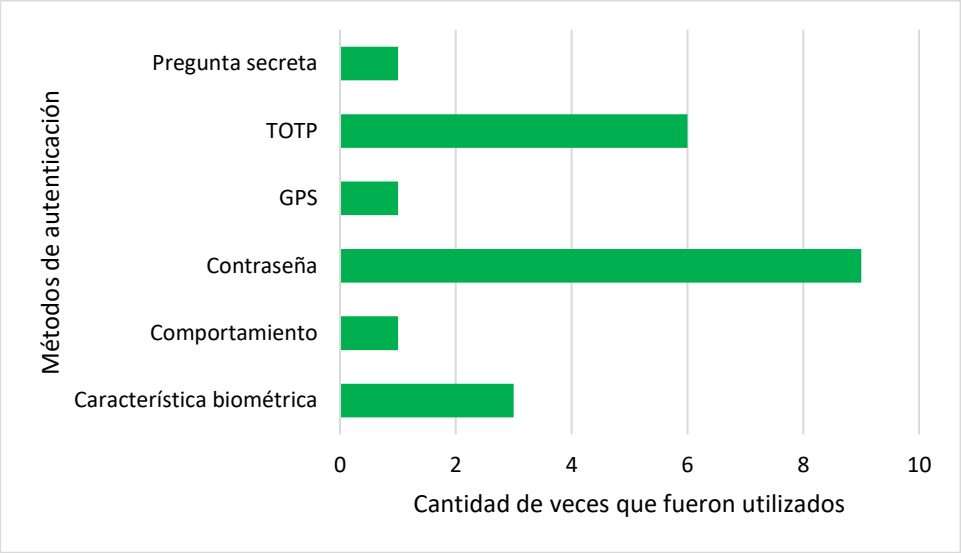


Figura 8. Métodos de Autenticación más utilizados en la identificación de usuarios.
Fuente: Elaboración propia.

Según la Tabla 02 y la Figura 08, los métodos de autenticación que hacen uso de CONTRASEÑA y TOTP son los que más se utilizaron en casos cuya naturaleza se asemejan al problema de investigación, los mismos que fueron seleccionados en el presente estudio.

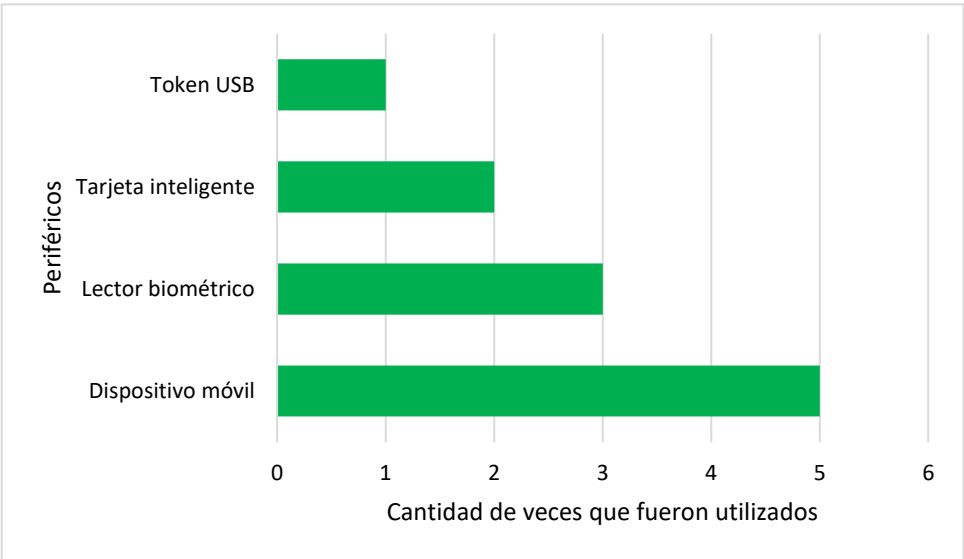


Figura 9. Periféricos más frecuentes que se utilizaron en los sistemas de autenticación analizados.
Fuente: Elaboración propia.

Asimismo, la Figura 9 muestra la frecuencia de los periféricos utilizados en las investigaciones analizadas, necesarios para completar el proceso de autenticación, siendo el dispositivo móvil o smartphone el periférico más adoptado en los sistemas propuestos. Adicional a ello, y por tratarse de una votación electrónica no presencial, en donde el acceso a Internet es un requisito indispensable para realizar este tipo de elección, se seleccionó el correo electrónico como medio alterno para recibir la TOTP.

Los métodos de autenticación y el periférico seleccionado en la presente investigación concuerdan con la investigación realizada por Barkadehi y otros (2018), denominada *Authentication Systems: A Literature Review and Classification*, en donde se realiza una revisión de la literatura científica, e identifica al dispositivo móvil como periférico más empleado en los sistemas propuestos.

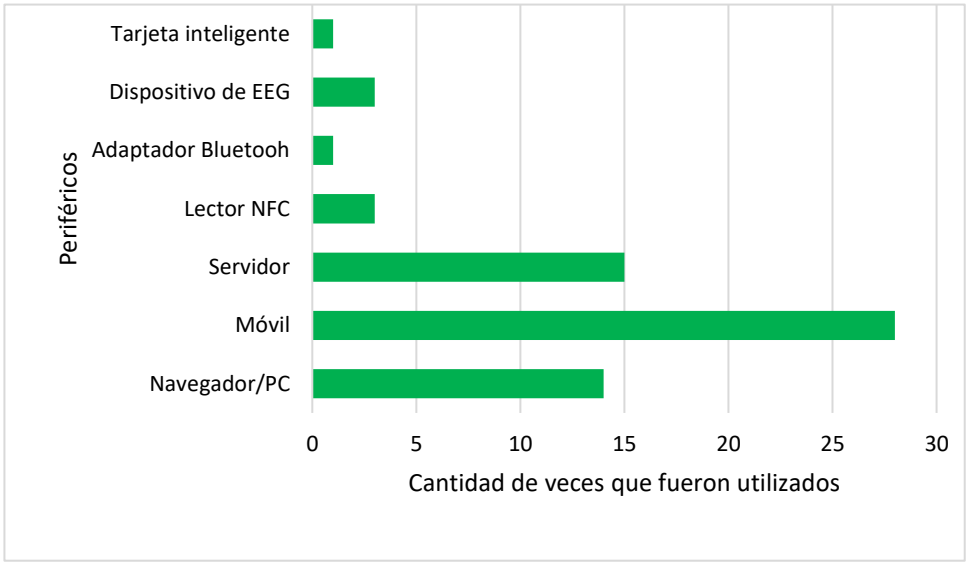


Figura 10. Periféricos más frecuentes que se utilizaron en sistemas de autenticación.
Fuente: (Barkadehi y otros, 2018)

Seleccionados los métodos de autenticación, se procedió a diseñar un método de autenticación multifactor que mitigue la suplantación de identidad en el proceso de voto electrónico no presencial, el mismo que constó de tres fases: registro, autenticación y votación.

Se debe tener presente que, el objeto de esta investigación es la implementación del método de autenticación multifactor, por ello, el diseño del método se centra en la fase de autenticación.

Fase 1: Registro

Desde el módulo de registro, los padres de familia proporcionan su información personal, como DNI (que representa su ID), nombres, apellidos, correo electrónico, número de celular y contraseña. Este último campo, por ser de tipo password, muestra a través de asteriscos el contenido ingresado; por lo que el usuario deberá ingresar dos veces la misma clave, evitando de esta manera un error de digitación.

Cada campo es obligatorio y validado. Caso contrario, la aplicación emitirá un mensaje de advertencia para poder corregir el dato erróneo o vacío. Validada esta información, se procede a almacenar la información proporcionada y concluir con la fase de registro.

Entre las validaciones, y con el propósito de garantizar la identidad del padre de familia, el número de celular y correo electrónico deben únicos por cada usuario, debido a que éstos serán los medios por los cuales el padre de familia podrá recibir su clave TOTP.

Asimismo, siendo el objetivo principal de esta investigación, mitigar la suplantación de identidad, es necesario que, durante esta fase, la aplicación realice validaciones específicas al momento de crear la contraseña, entre las cuales están, que la contraseña debe tener al menos 8 caracteres; estos caracteres deben tener números, letras mayúsculas y minúsculas, y caracteres especiales. Si la contraseña creada por parte del usuario no cumple con estos requisitos; es decir, solo tiene letras y/o números, y no tiene un caracter especial, entonces, la aplicación solicitará que se cambie dicha contraseña.

Una vez que el padre de familia se registre de forma satisfactoria, la aplicación lo dirige a la fase de inicio de sesión para que pueda accesar al sistema.

Fase 2: Autenticación

En los métodos de autenticación tradicional, el usuario ingresa su ID y contraseña para accesar al sistema. El servidor valida las credenciales ingresadas, y acepta o deniega el acceso.

En esta fase, el usuario ingresa al módulo de Login de la aplicación web, ingresa su DNI, que representa el ID, la contraseña que creó en la fase de registro, y selecciona el medio por el cual desea recibir la clave TOTP, ya sea a través de un mensaje de texto a su número de celular o a través de su correo electrónico, los mismos que indicaron en la fase de registro. Dando clic en el botón Validar, la aplicación determina si los datos proporcionados son correctos. Si el usuario ingresa su DNI y/o contraseña inexactos, la aplicación emite un mensaje indicando que los datos son erróneos, por lo que debe corregir dicha información para poder continuar con el proceso de autenticación.

Validado el DNI y contraseña, e indicado el medio por el cual desea recibir la clave TOTP, el usuario obtiene un código de verificación como respuesta, el mismo que deberá ingresar en la casilla correspondiente, para luego dar clic en el botón Accesar. En caso de que el usuario ingrese información incorrecta, se emite un mensaje para que pueda corregir dicha información. El código de verificación recibido solo puede ser usado en cada inicio de sesión; es decir, si el usuario desea ingresar nuevamente, la aplicación envía otro código de verificación TOTP. Una vez que el usuario ingrese de forma correcta la TOTP recepcionada, puede accesar al módulo de votación.

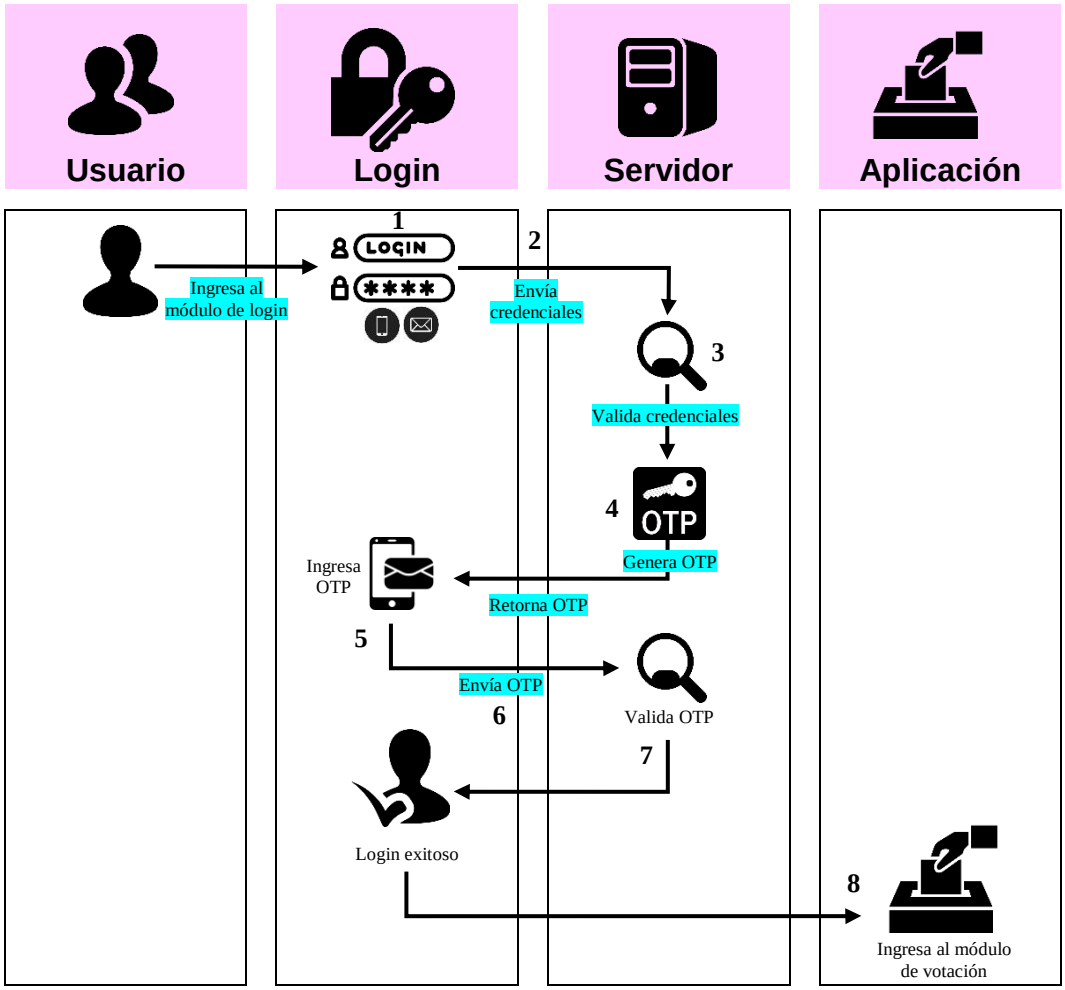


Figura 11. Método de autenticación propuesto.
Fuente: Elaboración propia.

Paso 1. El usuario accede al módulo de autenticación, ingresa su ID y contraseña, e indica el medio por el cual desea recibir la TOTP.

Paso 2. La aplicación envía el ID y contraseña ingresada.

Paso 3. El servidor de autenticación valida las credenciales ingresadas.

Paso 4. El servidor de autenticación genera la TOTP y la envía al celular o correo electrónico indicado por el usuario.

Paso 5. El usuario recibe la TOTP y la ingresa en el módulo de autenticación.

Paso 6: La aplicación envía la TOTP ingresada por el usuario.

Paso 7. El servidor de autenticación compara la TOTP ingresada con la TOTP generada.

Paso 8. Si todas las credenciales proporcionadas por el usuario son correctas, el servidor de autenticación permite el acceso al módulo de votación, de lo contrario, rechaza el acceso.

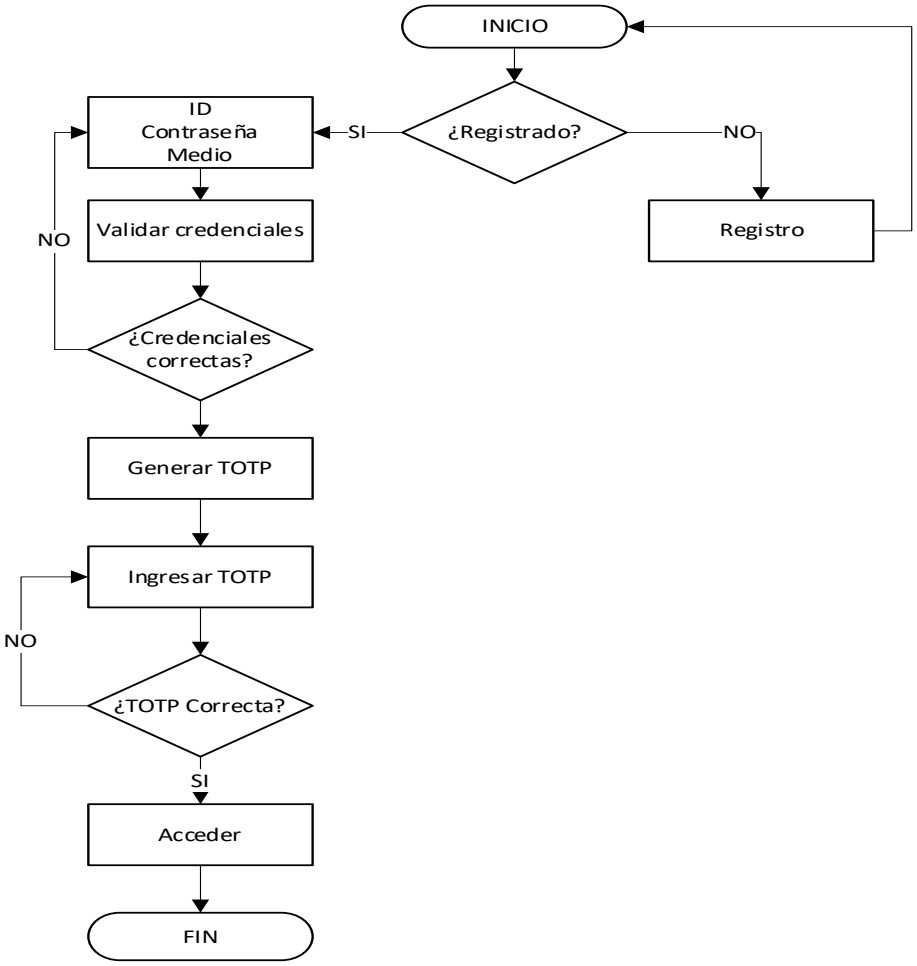


Figura 12. Diagrama de flujo del método de autenticación propuesto.
Fuente: Elaboración propia.

Fase 3: Voto Electrónico No Presencial

Verificada la identidad del elector, se apertura el módulo de votación, en donde se visualiza una ventana con las indicaciones del proceso de votación. Asimismo, se muestra la cantidad de accesos al módulo y el tiempo que dura la sesión.

La aplicación presenta las listas participantes en la elección de APAFA, en donde el elector selecciona la lista de su preferencia, para luego dar clic en Siguiente.

La aplicación muestra la lista elegida. Si el elector desea cambiar su voto, puede dar clic en el botón Cambiar o continuar con la votación a través del botón Votar. Si da clic en el botón Cambiar, la aplicación regresa a la ventana anterior para que el elector pueda modificar su elección.

Concluido el proceso de votación, se visualiza un mensaje de confirmación en donde se indica que su votación se ha efectuado de forma satisfactoria. Asimismo, se envía un mensaje de confirmación.

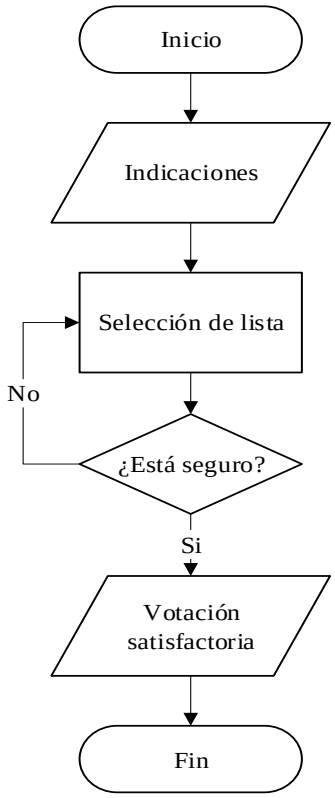


Figura 13. Flujo del proceso de votación electrónica no presencial.
Fuente: Elaboración propia.

Diseñado el método de autenticación, se realizó la codificación del método de autenticación multifactor que mitigue la suplantación de identidad en el proceso de voto electrónico no presencial, para lo cual se utilizó como servidor de plataforma XAMPP, debido a que es un software libre, que trabaja con base de datos MySQL, servidor web

Apache; además permite evaluar el trabajo de forma local, sin necesidad de contar con acceso a Internet.

Respecto al lenguaje de programación utilizado para realizar la codificación, fue PHP debido a que es de código abierto, muy utilizado en la creación de páginas web dinámicas, compatible con XAMPP, cuenta con diversas librerías y frameworks, entre ellos Laravel, el cual nos brinda una estructura y herramientas que facilitaron el desarrollo de la aplicación.

El patrón de arquitectura utilizado fue el Modelo-Vista-Controlador, mediante el cual se estructuró de forma apropiada los datos, la interfaz gráfica y los diferentes procesos que se implementaron en la aplicación; respecto al editor de código empleado se utilizó Visual Studio Code, debido a su fácil uso, resaltado de sintaxis, finalización inteligente de código, entre otras bondades.

Como se mencionó anteriormente, la aplicación consta de tres fases: registro, autenticación y votación; centrándose en la fase de autenticación.

En la fase de Registro, y con el objetivo de mitigar la suplantación de identidad, la aplicación permitirá la creación de contraseñas robustas, para lo cual realiza validaciones específicas al momento de crear la contraseña. El Script para validar la contraseña creada por el usuario se puede visualizar en la Figura 14.

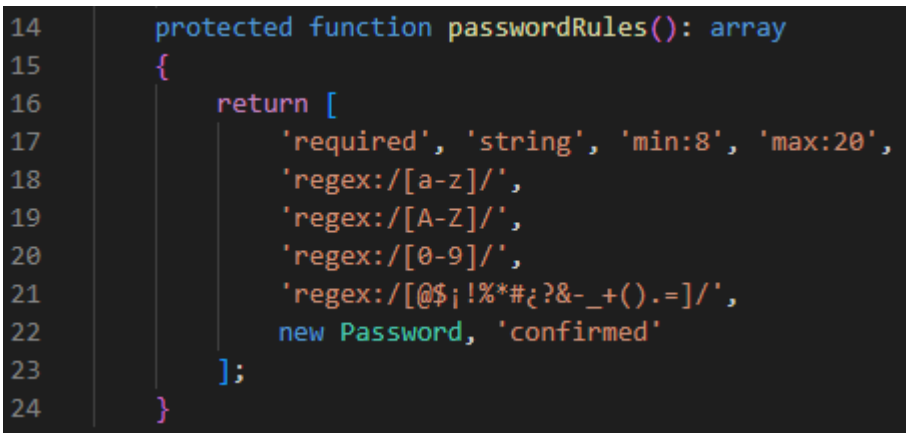


Figura 14. Script de validación de la contraseña.
Fuente: Elaboración propia.

En la fase de Autenticación, el usuario ingresa su ID y contraseña, e indica el medio por el cual desea recibir la TOTP. La aplicación valida las credenciales ingresadas, y de ser correctas, se genera la TOTP y la envía al celular o correo electrónico indicado por el usuario. El Script para generar la TOTP y determinar el medio por el cual el usuario recibirá dicha clave se puede visualizar en la Figura 15, Figura 16 y Figura 17.

```
83      public function generateTwoFactorCode()
84      {
85          $this->timestamps = false;
86          $this->two_factor_code = rand(100000, 999999);
87          $this->two_factor_expires_at = now()->addMinutes(2);
88          $this->save();
89      }
```

Figura 15. Script para generar la TOTP.
Fuente: Elaboración propia.

```
50  protected function authenticated(Request $request, $user)
51  {
52    $user->generateTwoFactorCode();
53
54    if($_REQUEST['typeVerification'] == 'Email') {
55      $user->notify(new TwoFactorCode());
56      } else {
57      $basic  = new \Nexmo\Client\Credentials\Basic('e5b[redacted]', 'Xk1W[redacted]');
58      $client = new \Nexmo\Client($basic);
59      $message = $client->message()->send([
60        'to' =>"51$user->phone",
61        'from' => 'AppVotos',
62        'text' => "Código de Verificacion: $user->two_factor_code"
63        ]);
64      $tempUser = auth()->user();
65      if(auth()->check() && $tempUser->two_factor_code)
66      {
67        if($tempUser->two_factor_expires_at<now()) //expired
68          {
69            $tempUser->resetTwoFactorCode();
70            auth()->logout();
71            return redirect()->route('login')
72            ->withMessage('Su código ha caducado. Por favor, inicie sesión denuevo.');
73          }
74          if(!$request->is('verify*')){
75            return redirect()->route('verify.index');
76          }
77        }
78        return true;
79      }
80  }
```

Figura 16. Script para enviar la TOTP al celular del usuario.
Fuente: Elaboración propia.

```php
class TwoFactorCode extends Notification
{
    use Queueable;
    public function via($notifiable)
    {
        return ['mail'];
    }
    public function toMail($notifiable)
    {
        return (new MailMessage)
            ->line('Su código de Acceso es '.$notifiable->two_factor_code)
            ->action('Verifique Aquí', route('verify.index'))
            ->line('El código caducará en 2 minutos.')
            ->line('Si no ha intentado iniciar sesión, ignore este mensaje.');
    }
}
```

Figura 17. Script para enviar la TOTP al correo electrónico del usuario.
Fuente: Elaboración propia.

Para el envío de la clave TOTP, se hizo uso de Twilio, la cual es una plataforma de desarrollo que integra servicios de SMS, MMS, voz, video, autenticación, y verificación de números telefónicos. Twilio ofrece una API que permite incorporar la funcionalidad de comunicación en aplicaciones web y equipos móviles.

Al registrarse en Twilio, nos brinda un Identificador de la cuenta y un Token de autenticación, tal como se muestra en la Figura 18; asimismo, nos permite asignar un número de teléfono de pruebas desde donde se envían los mensajes con la clave TOTP para accesar a la aplicación. Estos valores proporcionados por la cuenta de prueba, serán necesarios para integrarlos a la API, como se puede visualizar en la Figura 19.

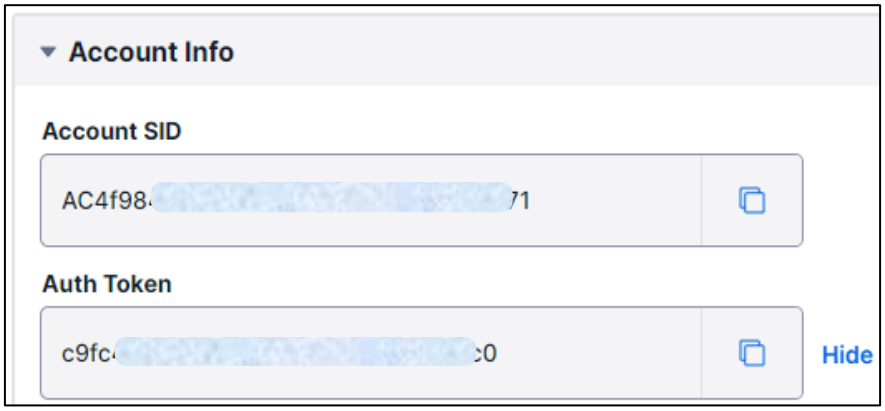


Figura 18. Identificador de la cuenta y Token de autenticación, proporcionados por Twilio.
Fuente: Elaboración propia.

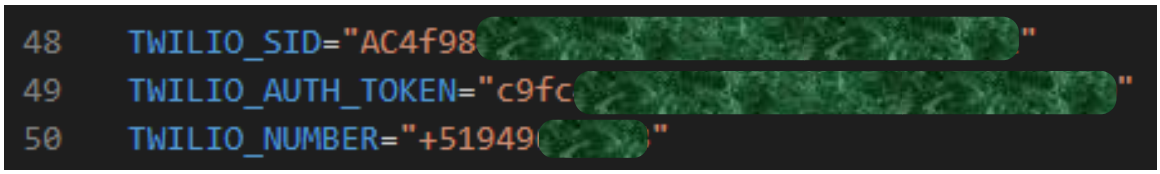


Figura 19. Valores asignados en el archivo .env de Laravel.
Fuente: Elaboración propia.

Codificado el método de autenticación, se realizaron pruebas de suplantación de identidad para poder accesar al módulo de voto electrónico no presencial, las cuales consistían en ataques como Surf de hombro, fuerza bruta y ataques de diccionario.

Los ataques de surf sobre el hombro se realizan de forma directa; es decir, se mira por encima del hombro del usuario al momento de ingresar su usuario y contraseña, y en este caso, también el ingreso de la TOTP; y de esta manera, obtener sus credenciales para poder acceder a la aplicación web. Este tipo de ataque también se puede realizar con binoculares y cámaras de alta definición colocados en lugares estratégicos para poder captar lo ingresado por el usuario. El ataque de surf sobre el hombro es más efectivo en lugares concurridos, por lo que, para proteger este tipo de ataques, los especialistas en seguridad informática, recomiendan cubrir con su cuerpo o con una de sus manos el teclado al momento de ingresar sus credenciales.

Para el caso de estudio, este tipo de ataque no tuvo éxito, debido a que la votación electrónica se efectuó desde la comodidad del hogar del elector; es decir, el usuario no estuvo expuesto a miradas de extraños con el fin de obtener las credenciales de acceso a la aplicación; asimismo, la TOTP ingresada, como su mismo nombre lo dice (contraseña de un solo uso basada en el tiempo), solo puede ser utilizada una sola vez, ya que si el usuario desea ingresar nuevamente, se le enviará una nueva TOTP para accesar a la aplicación web.

En los ataques de fuerza bruta, los atacantes prueban todas las combinaciones posibles hasta obtener la contraseña cifrada; para ello hacen uso de diferentes herramientas como scripts, herramientas de línea de comando, o software de hacking especializado. El ataque resultará efectivo si la contraseña es corta o débil, por lo que,

para protegerse de este tipo de ataques se debe utilizar contraseñas complejas y seguras que incluyan letras mayúsculas, minúsculas, números y símbolos. De ello depende el tiempo que tardará el atacante para obtener la contraseña, lo cual puede tardar minutos, horas, e incluso años.

En el método propuesto, en la fase de Registro, la creación de la contraseña por parte del usuario juega un papel muy importante en el sistema de autenticación, toda vez que, mientras más compleja sea la contraseña, será más complicado la obtención de la misma por parte de los atacantes. Para ello, el método propuesto realiza validaciones para mitigar la obtención de la contraseña por medio de este tipo de ataques. Entre las validaciones implementadas están, la contraseña debe tener como mínimo ocho caracteres; asimismo, debe estar formada por letras mayúsculas y minúsculas, números y símbolos; caso contrario, la aplicación emitirá un mensaje advirtiendo que la contraseña creada no cumple con los requisitos mínimos para su aceptación.

Las pruebas de ataques se realizaron con Kali Linux, el cuál es una distribución de Linux basada en Debian, ampliamente utilizada para realizar pruebas de pentesting o pruebas de penetración y pruebas de seguridad. Contiene una gran cantidad de herramientas de seguridad y hacking.

La herramienta utilizada para aplicar el ataque de fuerza bruta fue “Hydra”, la cual viene instalada en Kali Linux y es utilizada para realizar ataques de fuerza bruta en diferentes servicios de autenticación, entre ellos HTTP. La línea de comando utilizada se muestra en la Figura 20.

Figura 20. Ataque de Fuerza bruta a través de la herramienta “Hydra”.
Fuente: Elaboración propia.

En la línea de comando de la Figura 20, se utilizaron los siguientes parámetros:

- “hydra”: herramienta utilizada para realizar ataques de fuerza bruta.
- “-l 16790289”: permite indicar el usuario al cual se realizará el ataque de fuerza bruta (16790289).
- “-P 10kpassword.txt”: archivo de texto que contiene 10000 contraseñas con el cual se realizará el ataque de fuerza bruta.
- “appmultifactor.000webhostapp.com”: sitio web al cual se ejecutará el ataque de fuerza bruta.
- “http-post-form”: tipo de método que se está utilizando durante la petición.
- “/login.php”: ruta a la cual se realizará la fuerza bruta.
- “dni=^USER^”: parámetro enviado durante la petición en el campo ‘dni’.
- “password=^PASS^”: parámetro por el que pasarán cada una de las contraseñas que se encuentran en el archivo ‘10kpassword.txt’.
- “S-main”: parámetro para determinar si el ataque tuvo éxito.

Para obtener los datos necesarios para realizar el ataque de fuerza bruta a través de Hydra, se empleó la herramienta “Burp Suite”, que viene instalado en Kali Linux. Burp Suite contiene diferentes herramientas, entre ellas un proxy de red, escáner de vulnerabilidades, secuenciador, interceptor de solicitudes y respuestas, analizador de contenido, herramientas de decodificación y codificación; así como también proporciona un entorno de trabajo para realizar el análisis de tráfico HTTP/HTTPS, y la manipulación de solicitudes y respuestas; y de esta manera, poder mejorar la seguridad de las mismas. Es utilizado por profesionales de seguridad para encontrar vulnerabilidades en aplicaciones web. Los resultados de la intercepción de la petición se muestran en la Figura 21.

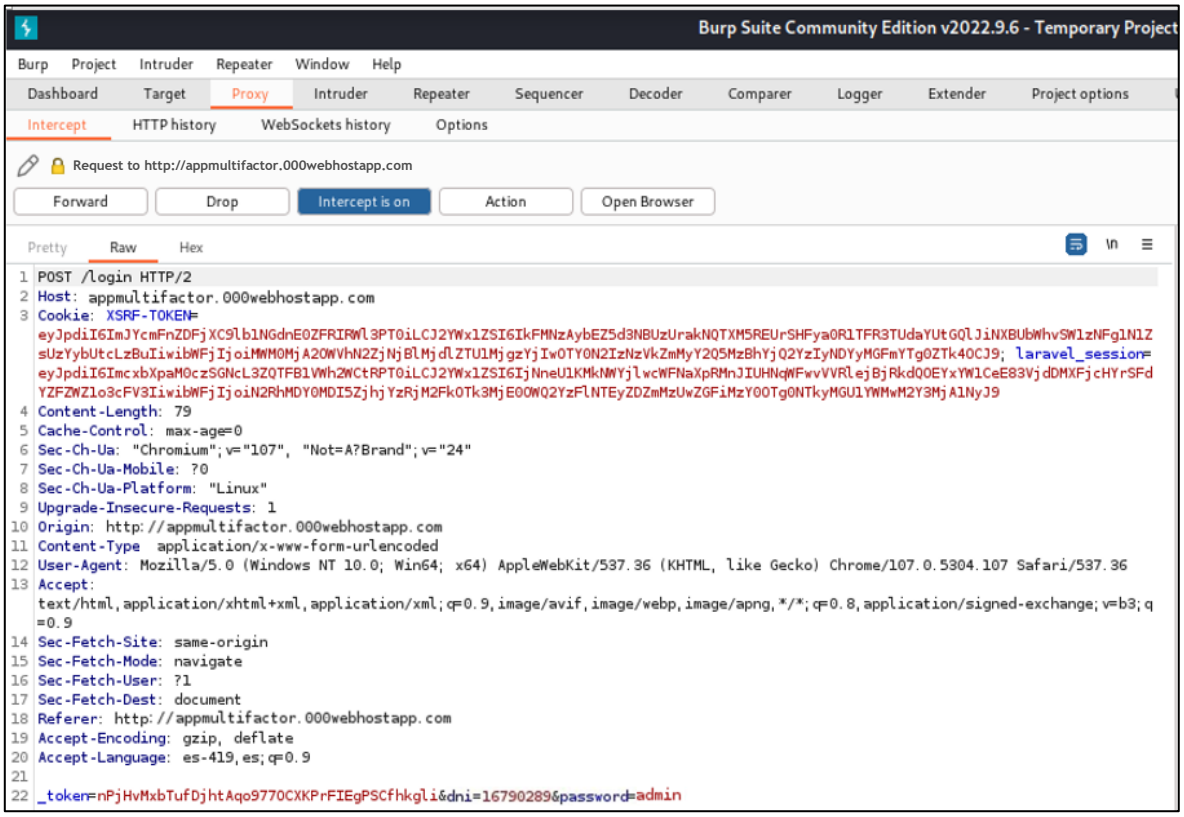


Figura 21. Tráfico interceptado mediante la herramienta “Burp Suite”.
Fuente: Elaboración propia.

Los resultados demuestran la efectividad del método implementado, debido a las consideraciones que se tienen al momento de creación de la contraseña, y al segundo factor implementado en la autenticación; por lo que la probabilidad de éxito de este tipo de ataque resultó nula, tal como se puede apreciar en la Figura 22.

```
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-04-05 10:29:18
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries (l:1/p:10000), ~625 tries per task
[DATA] attacking http-post-forms://gallitodelasrocas.com.pe:443/login.php:usuario=^USER^&password=^PASS^:S=main
[STATUS] 228.00 tries/min, 228 tries in 00:01h, 9772 to do in 00:43h, 16 active
[STATUS] 236.33 tries/min, 709 tries in 00:03h, 9291 to do in 00:40h, 16 active
[STATUS] 238.29 tries/min, 1668 tries in 00:07h, 8332 to do in 00:35h, 16 active
[STATUS] 238.80 tries/min, 3582 tries in 00:15h, 6418 to do in 00:27h, 16 active
[STATUS] 238.39 tries/min, 7390 tries in 00:31h, 2610 to do in 00:11h, 16 active
[STATUS] 236.22 tries/min, 8504 tries in 00:36h, 1496 to do in 00:07h, 16 active
[STATUS] 235.85 tries/min, 9670 tries in 00:41h, 330 to do in 00:02h, 16 active
[STATUS] 236.02 tries/min, 9913 tries in 00:42h, 87 to do in 00:01h, 16 active
[STATUS] 232.56 tries/min, 10000 tries in 00:43h, 1 to do in 00:01h, 3 active
```

Figura 22. Resultados del ataque de fuerza bruta.
Fuente: Elaboración propia.

En los ataques de diccionario, el atacante se agencia de programas que albergan una lista de palabras que son probadas para adivinar las contraseñas. Muchas veces este tipo de ataques resulta más efectivo que los ataques de fuerza bruta, toda vez que los usuarios suelen tener como mala práctica, el uso de contraseñas con palabras comunes.

En el método implementado, tal como se describió anteriormente, para la creación de contraseñas, la aplicación exige un mínimo de ocho caracteres, la combinación de letras, números y símbolos, para que una contraseña sea aceptada.

Las pruebas de ataques de diccionario se realizaron con la herramienta “Hashcat”, la cual viene instalada en Kali Linux y es utilizada para probar la seguridad de las contraseñas y evaluar su fortaleza. La línea de comando utilizada se muestra en la Figura 23.

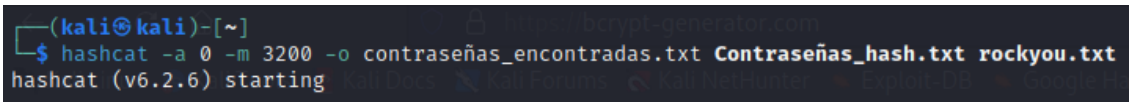


Figura 23. Ataque de diccionario a través de la herramienta “hashcat”.
Fuente: Elaboración propia.

En la línea de comando de la Figura 23, se utilizaron los siguientes parámetros:

- “hashcat”: herramienta utilizada para fines de seguridad informática.
- “-a 0”: modo de ataque: Diccionario (0).
- “-m 3200”: tipo de hash: bcrypt.
- “-o contraseñas_encontradas.txt”: archivo de salida en el que se almacenarán las contraseñas que coinciden con el diccionario de contraseñas.
- “Contraseñas_hash.txt”: archivo que contiene las contraseñas hash que se compararán con el diccionario de contraseñas.
- “rockyou.txt”: archivo de texto que contiene más de 14 millones de contraseñas utilizado para pruebas de seguridad y cracking de contraseñas.

Los resultados demuestran la efectividad del método implementado, comprobándose una vez más su efectividad, debido a las consideraciones que se tienen al momento de creación de la contraseña, y al segundo factor implementado en la autenticación; por lo que la probabilidad de éxito de este tipo de ataque resultó nula, tal como se puede apreciar en la Figura 24.

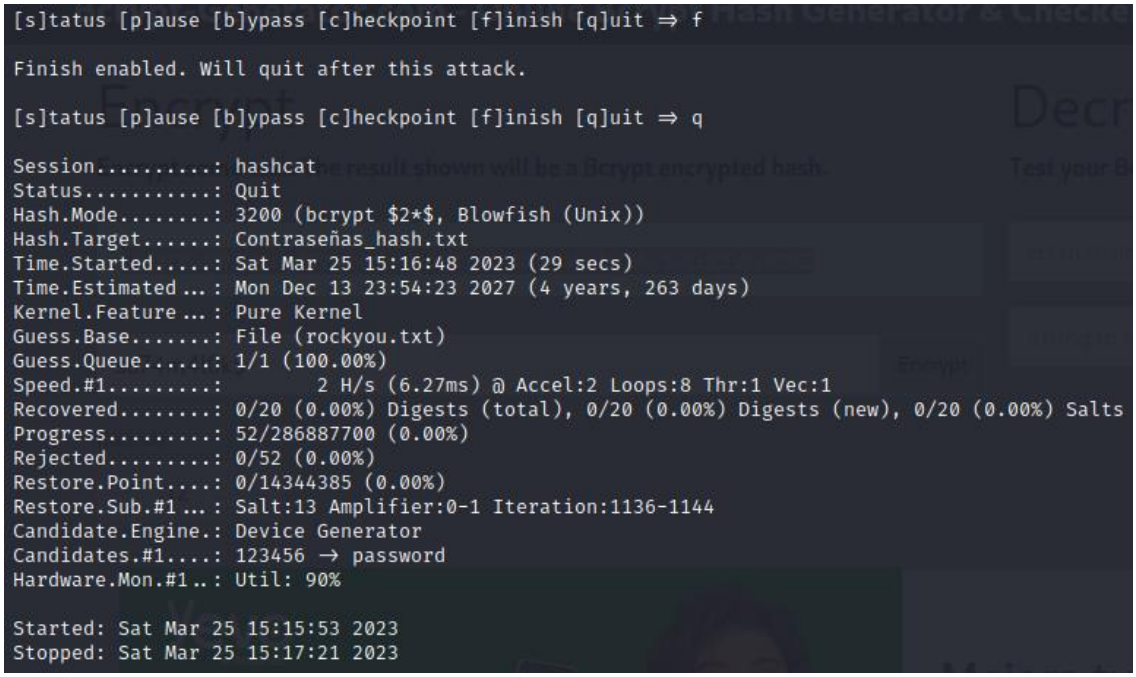


Figura 24. Resultados del ataque de diccionario.
Fuente: Elaboración propia.

Para evaluar, identificar vulnerabilidades, y determinar si se está utilizando el protocolo de seguridad TLS v1.2 (Transport Layer Security), el cual es un protocolo de seguridad que se utiliza para cifrar las comunicaciones en línea y proteger la confidencialidad e integridad de los datos transmitidos (en este caso, el envío de la TOTP), entre un cliente y un servidor en una aplicación web, se utilizó la herramienta de escaneo de seguridad Qualys SSL Labs, mediante la cual se ingresó la dirección ip de la aplicación, y se procedió a realizar el escaneo respectivo.

Los resultados del escaneo efectuado por la herramienta Qualys SSL Labs demuestran que la clave TOTP enviada desde el servidor al cliente, se encuentra debidamente encriptada a través del algoritmo SHA384 con RSA, garantizando la

confidencialidad e integridad de la clave enviada. Los resultados de dicho escaneo se pueden apreciar en la Figura 25.

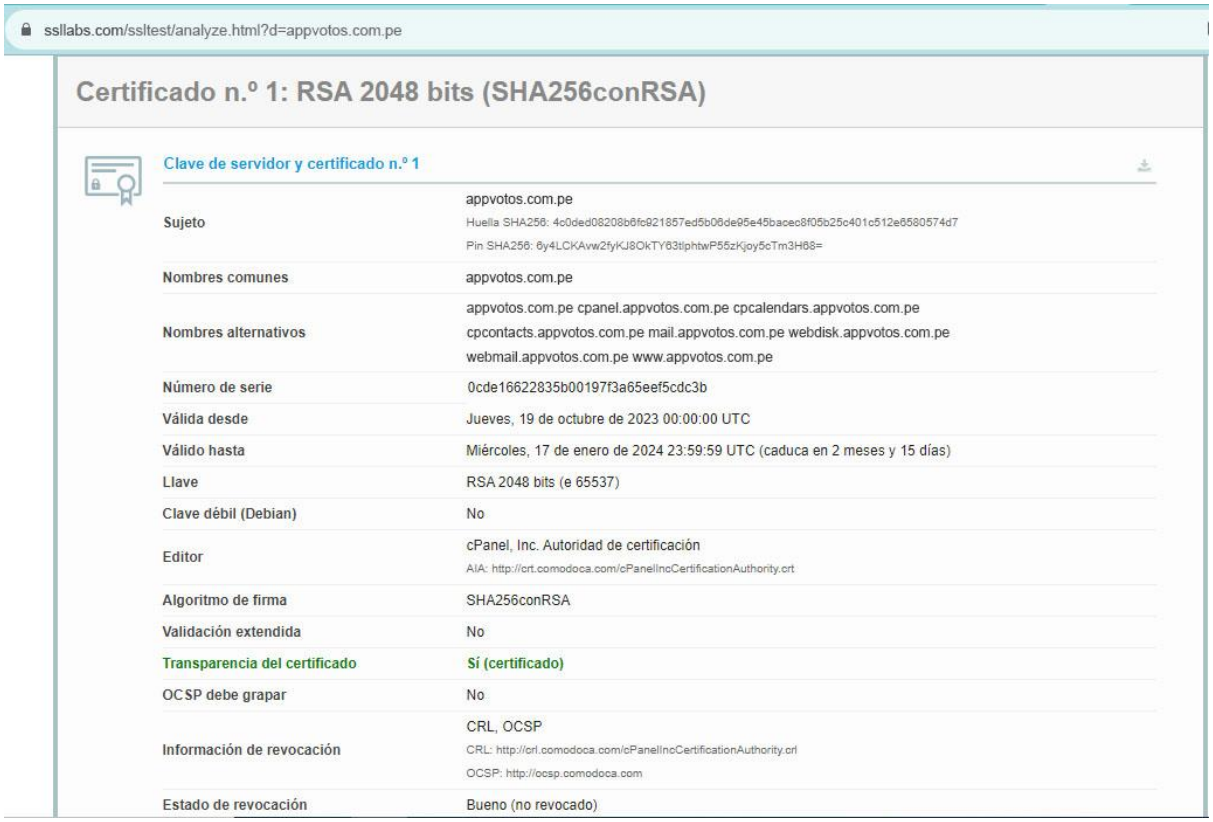


Figura 25. Resultados del escaneo efectuado con la herramienta Qualys SSL Labs.
Fuente: Elaboración propia.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

La selección de los métodos de autenticación en la identificación de usuarios se basó en la revisión sistemática de la literatura científica publicada hasta el año 2022, en donde el uso de la Contraseña y TOTP son los métodos más utilizados en casos cuya naturaleza se asemejan al problema de investigación. Asimismo, en dicha revisión se comprobó que el periférico más utilizado para recibir la TOTP, necesario para completar el proceso de autenticación, es el dispositivo móvil o smartphone, por lo que se optó, en esta investigación, utilizar este periférico, como medio de recepción de la TOTP.

El diseño del método de identificación de usuarios, consideró elementos como seguridad y usabilidad, fundamentándose en los aportes teóricos de las investigaciones analizadas, las mismas que consideran, como característica principal de la TOTP, su uso único en cada inicio de sesión. Asimismo, refieren que el uso de la TOTP, como segundo factor de autenticación, al no requerir un dispositivo dedicado o adicional, más que el uso del equipo móvil personal, permite al usuario autenticarse con la misma usabilidad que solo con contraseña.

La codificación del método implementado se rigió al uso del patrón de arquitectura Modelo-Vista-Controlador, lo cual permitió implementar el método de autenticación multifactor de forma adecuada y organizada, debido a que crea independencia de funcionamiento, dificultando de esta manera el acceso no autorizado. Asimismo, se hizo uso de Middlewares para controlar y modificar el flujo de las peticiones realizadas por los usuarios, facilitando la implementación de la seguridad, autenticación y la autorización en la aplicación.

Las pruebas de suplantación de identidad efectuadas al método implementado, permitieron comprobar la efectividad del mismo, validando la identidad del elector en un proceso de votación electrónica no presencial; tal es así que, en la prueba de ataque de surf sobre el hombro, el 0% de los ataques tuvieron éxito; en las pruebas experimentales de ataques de fuerza bruta, el 0% fue capaz de completar el ataque, debido al segundo factor implementado; asimismo, para la realización de las pruebas de ataques de diccionario, los resultados fueron del 0% debido a las consideraciones al momento de crear la contraseña y al segundo factor de autenticación implementado.

El método de identificación de usuarios, basado en autenticación multifactor implementado, permitió mitigar la suplantación de identidad toda vez que, al incorporar un factor más de autenticación al proceso de Login, redujo considerablemente la suplantación de identidad y por ende, el acceso no autorizado al módulo de votación, obteniendo un 100% de precisión, exhaustividad y exactitud.

4.2. Recomendaciones.

El método de autenticación que hace uso de la TOTP, así como, el uso del dispositivo móvil, como medio para obtenerla, resulta apropiado en aplicaciones que trabajan con información sensible, por lo que su empleo en la implementación de métodos de autenticación multifactor resulta aconsejable para preservar la Confidencialidad, Integridad y Disponibilidad de la Información.

A través del método de identificación de usuarios, basado en autenticación multifactor, se reduce considerablemente la suplantación de identidad, por lo que su incorporación en los módulos de Login, sobre todo, de las entidades que cuentan con información sensible o crítica, resulta recomendable para mitigar el acceso no autorizado, lo cual acarrea consigo, pérdida o manipulación de información confidencial, perjuicios económicos, entre otros.

Las aplicaciones informáticas que emplean para su implementación, el patrón de arquitectura Modelo-Vista-Controlador, crean independencia de funcionamiento, dificultando de esta manera el acceso no autorizado; por lo cual, debe ser empleado no solo en aplicaciones web, sino que, además debe ser empleado en aplicaciones móviles y otras aplicaciones en las cuales se implementes interfaces gráficas.

El uso de una misma contraseña para acceder a las diferentes redes sociales, correo electrónico, aplicaciones web, es una mala práctica de la gran mayoría de personas, debido a que sí, personas mal intencionadas logran obtener su usuario y clave, podrán acceder a todas las aplicaciones mencionadas.

Si se tiene que ingresar el usuario y contraseña en aplicativos donde hay mucha concurrencia de personal, se debe cubrir con el cuerpo y mano el teclado; asimismo, la contraseña creada debe ser lo suficientemente larga y combinar caracteres alfanuméricos, como números, letras mayúsculas y minúsculas, y caracteres especiales, con la firme intención de imposibilitar los ataques de fuerza fruta y de diccionario.

Para mitigar el riesgo de un ataque de hombre en el medio se debe evitar conectarse a redes Wi-Fi públicas, utilizar conexiones seguras HTTPS, el código TOTP debe transmitirse cifrado en la comunicación entre el usuario y el servidor, debido a que, en este tipo de ataque, el ciberdelincuente puede interceptar la información y utilizar las credenciales para acceder a la cuenta del usuario.

Referencias

[1] D. Gestión, «Aplicaciones móviles en Perú han incrementado en 63% la productividad empresarial,» 10 Octubre 2017. [En línea]. Available: https://gestion.pe/tendencias/management-empleo/aplicaciones-moviles-peru-han-incrementado-63-productividad-empresarial-220422-noticia/?ref=gesr. [Último acceso: 29 Agosto 2020].

[2] Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A., «Uso de autenticación multi-factor en sistemas y aplicaciones I,» Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A., Sevilla, 2016.

[3] M. Misbahuddin, B. Bindhumadhava y B. Dheeptha, «Design of a Risk Based Authentication System using Machine Learning Techniques,» *IEEE Xplore,* p. 6, 2017.

[4] Organización de los Estados Americano, «Estado de la Ciberseguridad en el Sistema Financiero Mexicano,» Organización de los Estados Americano, México, 2019.

[5] A. Bissada y A. Olmsted, «Mobile Multi-Factor Authentication,» *IEEE Xplore,* p. 2, 2017.

[6] S. Yang y J. Meng, «Research on multi-factor bidirectional Dynamic identification based on SMS,» *IEEE Xplore,* p. 5, 2018.

[7] S. Subrayan, S. Mugilan, B. Sivanesan y S. Kalaivani, «Multi Factor Authentication Scheme for Shadow Attacks in Social Network,» *IEEE Xplore,* p. 5, 2017.

[8] J. Kiernan, «Credit card & debit card fraud statistics,» *IEEEXplore,* p. 5, 2016.

[9] S. Vaithyasubramanian, D. Lalitha y M. Metilda, «Multifactor authentication - A study on user preference, remembering ability,error rate and time consumption,» *Revista Internacional de Rehabilitación Psicosocial,* p. 6, 24 Abril 2019.

[10] A. Bani, M. Majdalweieh y A. AlShamsi, «Online Authentication Methods Used in Banks and Attacks Against These Methods,» *Science Direct,* p. 8, 2019.

[11] V. Khattri y D. Singh, «Implementation of an Additional Factor for Secure Authentication in Online Transactions,» *Organizational Computing and Electronic Commerce,* p. 17, 29 Julio 2019.

[12] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen y Y. Koucheryavy, «Multi-Factor Authentication: A Survey,» *Publisher of Open Access Journals,* p. 31, 2018.

[13] J. Cano y G. Saucedo, «VIII Encuesta Latinoamericana de Seguridad de la Información,» Asociación Colombiana de Ingenieros de Sistemas, Bogotá, 2016.

[14] V. Venukumar y V. Pathari, «Multi-Factor Authetication Using Threshold Cryptography,» *IEEE Xplore,* p. 5, 2016.

[15] B. Maciej y M. Kurkowski, «Multifactor Authentication Protocol in a Mobile Environment,» *IEEE Access,* p. 15, 22 Octubre 2019.

[16] K. Ramatsakane y W. Leung, «Pick Location Security: Seamless Integrated Multi-Factor Authentication,» *International Information Management Corporation,* p. 10, 9 Noviembre 2017.

[17] J. Sun, Q. Zhong, L. Kou, W. Wang, Q. Da y Y. Lin, «A lightweight multi-factor mobile user authentication scheme,» *IEEE Xplore,* p. 6, 9 Julio 2018.

[18] T. Vásquez, «Los partidos políticos como factores de discusión racional: Deliberación y Elecciones,» *Revista Mejicana de Opinión Pública,* p. 18, 01 Junio 2016.

[19] P. Corvetto Salinas, Interviewee, *Elecciones generales de 2021.* [Entrevista]. 16 Setiembre 2020.

[20] X. Selvarani, M. Shruthi, R. Geethanjali, R. Syamala y S. Pavithra, «Secure voting system through SMS and using smart phone Application,» *IEEExplore,* p. 3, 14 Diciembre 2017.

[21] K. Sudharsan, V. Ambeth Kumar, R. Venkatesan, V. Sathyapreiya y G. Saranya, «Two Three Step Authentication in ATM Machine to Transfer Money and for Voting Application,» *ScienceDirect,* p. 7, 11 Diciembre 2019.

[22] L. N. 28044, «Ley General de Educación N° 28044,» 28 Julio 2013. [En línea]. Available: http://www.minedu.gob.pe/p/ley_general_de_educacion_28044.pdf.

[23] O. N. P. E. ONPE, «Manual para organizar elecciones es una asociación de padres de familia,» 01 Setiembre 2019. [En línea]. Available: https://www.onpe.gob.pe/modAsistenciaTecnica/docs/Manual-APAFA.pdf.

[24] N. Kordzo, M. Dorgbefu y S. Banning, «Design and Implementation of Cost Effective Multi-Factor Authentication Framework for ATM Systems,» *Asian Journal of Research in Computer Science,* p. 15, 27 Abril 2020.

[25] Y. Fujita, A. Inomata y H. Kashiwasaki, «Implementation and Evaluation of a Multi-Factor Web Authentication System with Individual Number Card and WebUSB,» *IEEE Xplore,* p. 4, 7 Noviembre 2019.

[26] Y. Watanabe, H. Suzuki, K. Naito y A. Watanabe, «Proposal for User Authentication Method Combining Random Number and Password,» *IEEE Xplore,* p. 2, 27 Febrero 2019.

[27] F. Corredor, L. Pabón, D. Mora y A. Ardila, «Implementation of Multi-Factor Strong Authentication Services and Confidentiality, for the Protection of Electronic Documentation,» *Latin American and Caribbean Consortium of Engineering Institutions,* p. 7, 29 Julio 2016.

[28] J. Sun, Z. Qi, L. Kou, W. Wang, Q. Da y Y. Lin, «A lightweight multi-factor mobile user authentication scheme,» *IEEE Xplore,* p. 6, 9 Julio 2018.

[29] J. Iftikhar, S. Hussain, K. Mansoor, Z. Ali y S. Chaudhry, «Symmetric-Key Multi-factor Biometric Authentication Scheme,» *IEEE Xplore,* p. 5, 4 Abril 2019.

[30] S. Uluagac, W. Liu y R. Beyah, «A Multi-Factor Re-authentication Framework with User Privacy,» *IEEE Xplore,* p. 2, 29 Diciembre 2016.

[31] D. He, K. Neeraj, J.-H. Lee y S. Sherratt, «Enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices,» *IEEE Xplore,* p. 8, 1 Febrero 2016.

[32] M. Aldwairi y S. Aldhanhani, «Multi-Factor Authentication System,» *American Scientific Publishers,* p. 7, Agosto 2017.

[33] A. Gómez, Enciclopedia de la Seguridad Informática, Segunda ed., México: Alfaomega Grupo Editor, 2014, p. 801.

[34] G. Baca, Introducción a la Seguridad Informática, Primera ed., vol. 1, J. E. Callejas, Ed., México: Grupo Editorial Patria, 2016, p. 361.

[35] G. Paucar, Seguridades Informáticas, Quito: Instituto Superior Tecnológico "David Ausubel", 2008, p. 80.

[36] J. Andress, Fundamentos de la Seguridad de la Información, Walthan: Project Manager, 2011.

[37] INTECO, Estudio sobre las tecnologías biométricas aplicadas a la seguridad, León: INTECO, 2011, p. 100.

[38] Kaspersky, «Spam y phishing en el tercer trimestre de 2019,» 2019. [En línea]. Available: https://securelist.com/spam-report-q3-2019/95177/. [Último acceso: 03 Julio 2019].

[39] J. Costas, Seguridad y Alta Disponibilidad, Madrid: Ra-Ma, 2011, p. 258.

[40] Organismo Internacional de Normalización, «ISO 27001,» 2018. [En línea]. Available: https://normaiso27001.es/referencias-normativas-iso-27000/. [Último acceso: 03 Julio 2020].

[41] M. Romero, G. Figueroa, D. Vera, J. Álava, G. Parrales, C. Álava, Á. Murillo y M. Castillo, Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades, Primera ed., Alicante: Área de Innovación y Desarrollo, 2018, p. 124.

[42] National Institute of Standards and Technology - NIST, «Electronic Authentication Guideline,» National Institute of Standards and Technology, Gaithersburg, 2017.

[43] J. Areitio, Seguridad de la Información: Redes, informática y sistemas de información, Madrid: Parainfo, 2008.

[44] F. Roa, Seguridad informática, Segunda ed., Madrid: Mc Graw Hill, 2013, p. 226.

[45] S. Kim, J. Kang, Y. Jo y I. Oakley, «Development of a multi-modal personal authentication interface,» *Asociación de Procesamiento de Señal e Información de Asia-Pacífico (APSIPA ASC),* p. 4, Noviembre 2017.

[46] E. Montañez, «MFA and Identity Federations,» *Universitat Oberta de Catalunya,* p. 48, Junio 2019.

[47] L. Doskálek, «Multi-Factor Authentication Modeling,» *IEEE Xplore,* p. 4, 1 Agosto 2019.

[48] L. Pérez, «Desarrollo de un servicio de autentificación de factor múltiple,» Universidad de Alicante, Alicante, 2019.

[49] Microsoft, «Autenticación multifactor para Microsoft 365,» 17 Julio 2020. [En línea]. Available: https://docs.microsoft.com/es-es/microsoft-365/admin/security-and-compliance/multi-factor-authentication-microsoft-365?view=o365-worldwide.

[50] Grupo Evidian, «Los 7 métodos de Autentificación más utilizados,» 2015. [En línea]. Available: https://www.evidian.com/pdf/wp-strongauth-es.pdf.

[51] Diario Gestión, «¿Qué hacer ante una suplantación de identidad en operaciones bancarias?,» 22 Octubre 2019. [En línea]. Available: https://gestion.pe/tu-dinero/finanzas-personales/que-hacer-ante-una-suplantacion-de-identidad-en-operaciones-bancarias-noticia/. [Último acceso: 15 Junio 2020].

[52] Asociación Portuguesa de Apoyo a la Víctima, Robo de identidad, Lisboa: PROTEUS, 2015, p. 94.

[53] B. Busaniche, Voto electrónico: una solución en busca de problemas, Buenos Aires: Cooperativa de Trabajo Triaco Ltda., 2017, p. 162.

[54] O. N. d. P. E. ONPE, «Voto Electrónico,» 15 Junio 2020. [En línea]. Available: https://www.web.onpe.gob.pe/modElecciones/elecciones/elecciones2017/em-dic2017/voto-electronico.

[55] A. Qureshi, D. Megías y H. Rifa-Pous, «SEVEP-Secure and verifiable electronic polling system,» *IEEE Access,* p. 25, 7 Febrero 2019.

[56] K. Taher, T. Nahar y S. Hossain, «Enhanced Cryptocurrency Security by Time-Based Token Multi-Factor Authentication Algorithm,» *IEEE Xplore,* p. 5, 21 Febrero 2019.

[57] P. Aguilera, Seguridad Informática, Madrid: Editex, 2010.

[58] Microsoft. [En línea]. Available: https://docs.microsoft.com/es-es/microsoft-365/admin/security-and-compliance/multi-factor-authentication-microsoft-365?view=o365-worldwide.

[59] O. N. d. P. Electorales, «Manual APAFA,» 01 Setiembre 2019. [En línea]. Available: https://www.onpe.gob.pe/modAsistenciaTecnica/docs/Manual-APAFA.pdf.

Anexo 1. Resolución de Aprobación de Tesis.

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°1322-2020/FIAU-USS

Pimentel, 17 de julio de 2020

VISTO:
El Acta de reunión N°1606-2020, de fecha 16 de junio de 2020 del Comité de investigación de la Escuela profesional de INGENIERIA DE SISTEMAS, para la ejecución : **"IMPLEMENTACIÓN DE UN MÉTODO DE IDENTIFICACIÓN DE ELECTORES BASADO EN AUTENTICACIÓN MULTIFACTOR PARA MITIGAR LA SUPLANTACIÓN DE IDENTIDAD EN EL VOTO ELECTRÓNICO NO PRESENCIAL. CASO DE ESTUDIO ELECCIONES DE APAFA"**, presentado por el(los) tesista(s) **PÉREZ CHANDUVÍ SANDRO PAÚL,** del Programa de estudios **INGENIERIA DE SISTEMAS**, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48º que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y *tesis* son *aprobados por el Comité de Investigación* y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El *periodo de vigencia de los mismos será de dos años*, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24º señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; *es individual o en pares para obtener un título profesional*. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, en el Acta de reunión N°1606-2020 de fecha 16 de junio de 2020, del Comité de investigación de la Escuela profesional de INGENIERIA DE SISTEMAS, se indica entre los acuerdos la aprobación del Proyecto de tesis denominado "IMPLEMENTACIÓN DE UN MÉTODO DE IDENTIFICACIÓN DE ELECTORES BASADO EN AUTENTICACIÓN MULTIFACTOR PARA MITIGAR LA SUPLANTACIÓN DE IDENTIDAD EN EL VOTO ELECTRÓNICO NO PRESENCIAL. CASO DE ESTUDIO ELECCIONES DE APAFA" de la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de PÉREZ CHANDUVÍ SANDRO PAÚL en condición de estudiante, del Programa de estudios INGENIERIA DE SISTEMAS.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1°: APROBAR, el Proyecto de denominado **"IMPLEMENTACIÓN DE UN MÉTODO DE IDENTIFICACIÓN DE ELECTORES BASADO EN AUTENTICACIÓN MULTIFACTOR PARA MITIGAR LA SUPLANTACIÓN DE IDENTIDAD EN EL VOTO ELECTRÓNICO NO PRESENCIAL. CASO DE ESTUDIO ELECCIONES DE APAFA",** perteneciente a la línea de investigación de **INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE**, a cargo de **PÉREZ CHANDUVÍ SANDRO PAÚL**, del Programa de estudios **INGENIERIA DE SISTEMAS.**

ARTÍCULO 2°: ESTABLECER, que la inscripción del Título de Proyecto de tesis se realice a partir de emitida la presente resolución y tendrá una vigencia de dos (02) años.

ARTÍCULO 3°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Dr. Mario Fernando Ramos Moscol
Decano - Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

MBA. María Noelia Sialer Rivera
Secretaria Académica / Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Anexo 2. Instrumento de recolección de datos – Registro electrónico.

Petición	Consumo		Tiempo de respuesta
	CPU (%)	RAM (Mb)	
1	1.8	12.4	4.2
2	2.1	11.6	3.9
3	2.8	10.8	5.4
4	3.3	8.3	4.2
5	1.9	14.2	4.4
6	1.6	11.9	3.1
7	3.3	11.7	4.5
8	2.7	8.5	4.3
9	3.1	12.1	5.7
10	2.9	9.9	4.1
11	3.9	13.6	5.1
12	3.4	12	6.0
13	2.9	13.7	3.9
14	2.1	12.3	3.8
15	3.0	10.1	4.2
16	2.5	14.8	3.9
17	2.3	9.1	4.2
18	3.5	10.6	4.4
19	3.8	13.9	4.5
20	3.2	11.2	3.7
Promedio	**2.8**	**11.6**	**4.4**

Anexo 3. Interfaz de usuario.

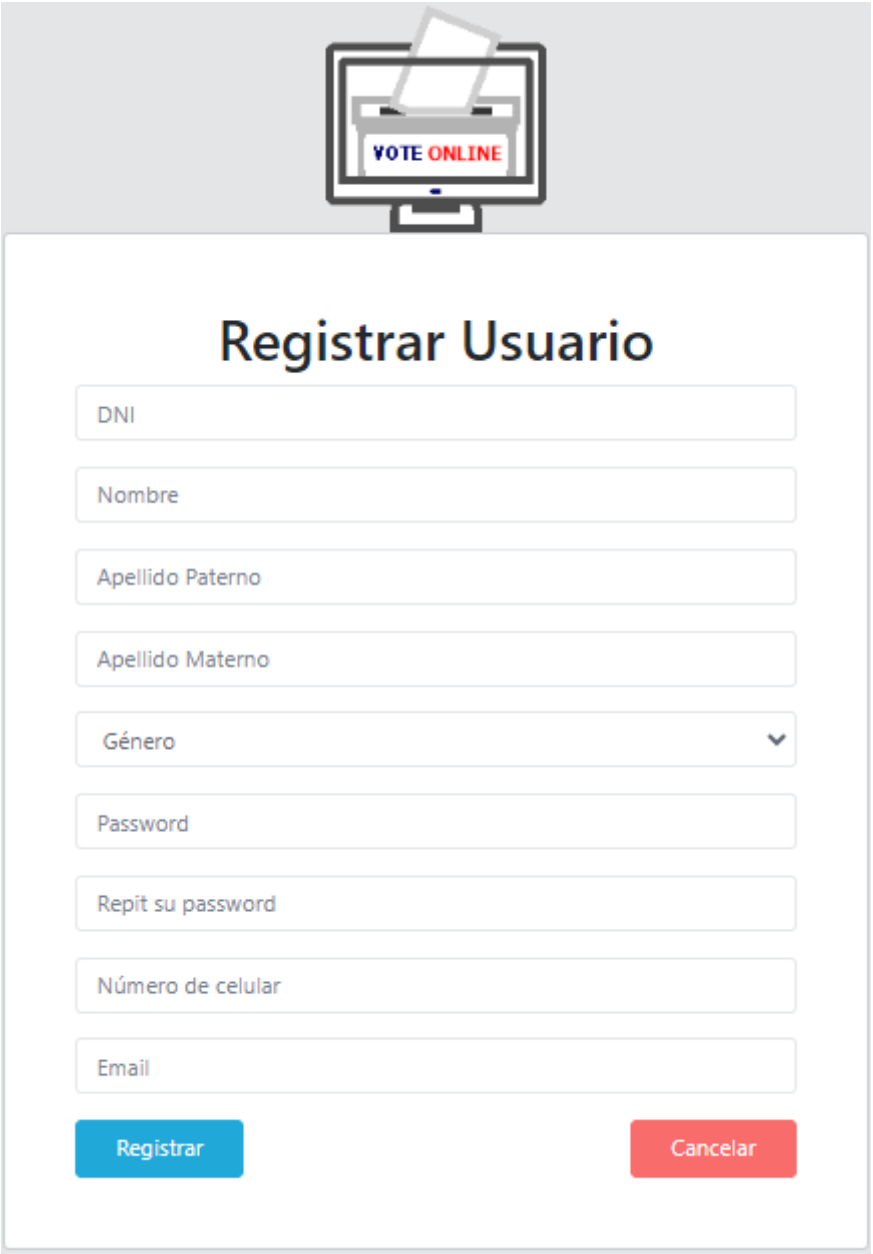


Figura 26. Diseño de interfaz de registro.

Fuente: Elaboración propia.

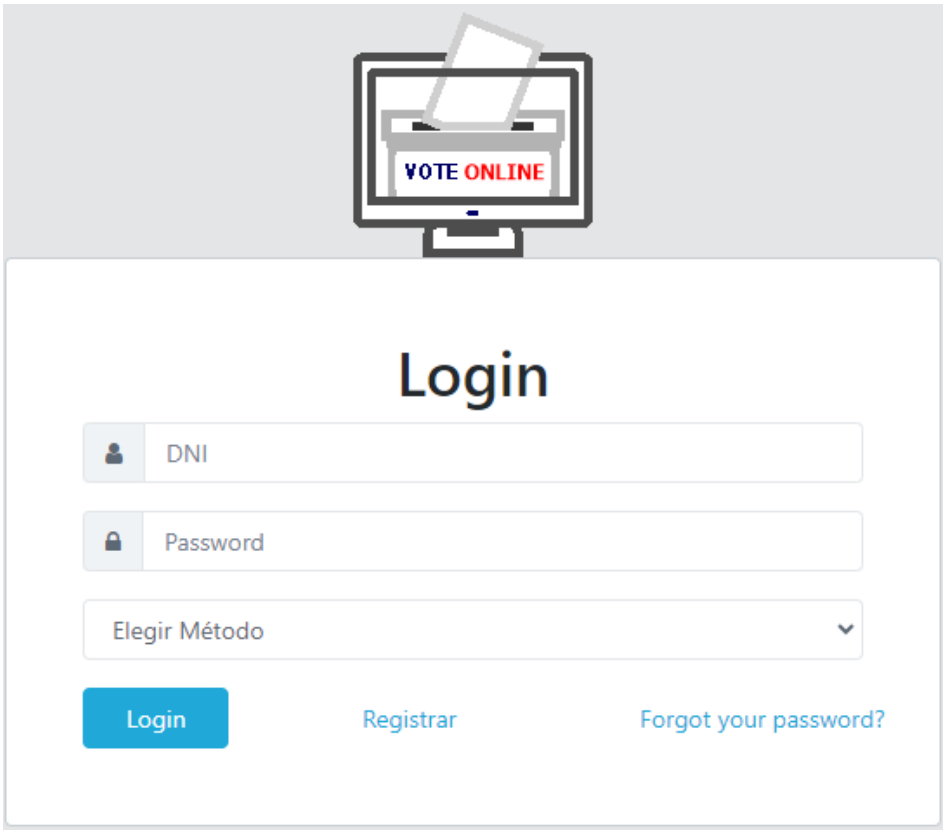


Figura 27. Diseño de interfaz de login.

Fuente: Elaboración propia.

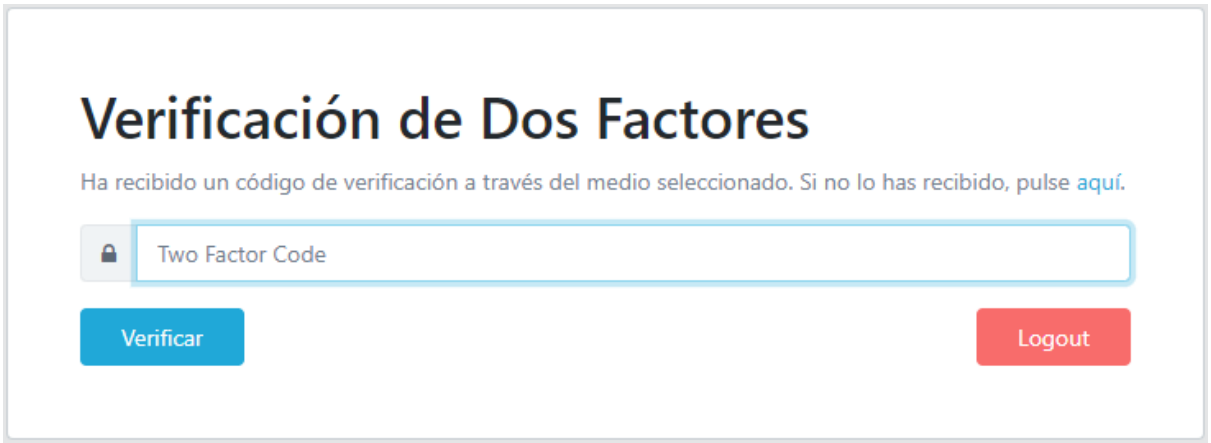


Figura 28. Diseño de interfaz de verificación.

Fuente: Elaboración propia.

NOMBRE DEL TRABAJO
PEREZ_CHANDUVI_SANDRO_PAUL-TURNITIN.docx

AUTOR
Sandro Perez Chanduvi

RECUENTO DE PALABRAS
13614 Words

RECUENTO DE CARACTERES
74171 Characters

RECUENTO DE PÁGINAS
58 Pages

TAMAÑO DEL ARCHIVO
1.7MB

FECHA DE ENTREGA
Nov 14, 2023 11:09 AM GMT-5

FECHA DEL INFORME
Nov 14, 2023 11:12 AM GMT-5

14% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base d

- 12% Base de datos de Internet
- 3% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr
- 8% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)