Revista Internacional de Investigación e Innovación Tecnológica

Página principal: www.riiit.com.mx

SisVal: prototipo de sistema de validación de identidad para trámites personales en México

SisVal: identity validation system prototype for personal procedures in Mexico

Silva-Peña, A.V.[a], Aviña-Luna, J.C.[a], Meléndez-Sánchez, U.[b], Rodríguez-González, L.[c], Muñoz-González, E.D.[d], Parra-Michel, J.R.[a], Martínez-Peláez, R.[a]

[a] Facultad de Tecnologías de Información; Universidad De La Salle Bajío; C.P. 37150, León, Guanajuato, México.
[b] Universidad de Guadalajara – Centro Universitario de la Ciénega; C.P. 47820, Ocotlán, Jalisco. México.
[c] Instituto Tecnológico de la Piedad; C.P. 59370, La Piedad de Cavadas, Michoacán, México.
[d] Instituto Politécnico Nacional; C.P. 07340, Gustavo A. Madero, Ciudad de México, México.
asp64722@udelasalle.edu.mx, jal63533@udelasalle.edu.mx, uriel_ms_19@hotmail.com, rod.glez.leonardo@gmail.com, chevereforever@gmail.com, jrparra@delasalle.edu.mx, rmartinezp@delasalle.edu.mx

Innovación tecnológica: Sistema que permite verificar la información de identidad impresa en la credencial para votar expedida por el INE a través de la lectura y consulta del código de identificación de la credencial en una base de datos de uso particular para la propuesta.

Área de aplicación industrial: Banco, centro de salud, comercio, dependencia de gobierno, institución de educación superior, casillas para votar, y negocio donde se requiera comprobar la identidad del ciudadano durante un proceso en específico, por ejemplo, cambio de cheque, contrato de un servicio, control de acceso, solicitud de empleo, solicitud de crédito, entre otros.

Recibido: 14 mayo 2020
Aceptado: 09 junio 2021

Abstract

In Mexico, the most popular means of identification is the voting credential issued by the National Electoral Institute (INE). The credential is requested to carry out different procedures within the national territory which includes, account opening, credit contracting, access control, room reservation, job application, among others. However, the processes that involve identity verification through the voting credential present the following security vulnerabilities: 1) the security measures of the credential are not verified, limiting themselves to a visual verification of the name, photograph, and signature; and 2) there is no system to validate that the data presented in the credential is legitimate, assuming that the data is true. Consequently, the attackers who are

dedicated to identity theft and identity fraud take advantage of the two security breaches to commit crimes that affect the economic and social stability of the victims, causing losses of 24,870 million pesos at the end of 2020. With the intention of reducing the impact of identity theft and identity fraud, the prototype SisVal is presented as an alternative solution to corroborate that the identity information of the citizen is correct, without using biometric data. Laboratory tests show that SisVal is easy to implement and contributes greatly to validate the identity of a citizen.

Key word: authentication, bank fraud, clients, fingerprint, identity theft, prevention.

Resumen

En México, el medio de identificación más popular es la credencial para votar expedida por el Instituto Nacional Electoral (INE). La credencial es solicitada para realizar distintos trámites dentro del territorio nacional que incluyen, apertura de cuentas, contratación de créditos, control de acceso, reserva de habitaciones, solicitud de empleo, entre otros más. Sin embargo, los procesos que involucran la verificación de identidad por medio de la credencial para votar presentan las siguientes vulnerabilidades de seguridad: 1) no se verifican las medidas de seguridad de la credencial, limitándose a una comprobación visual del nombre, fotografía y firma; y 2) no existe un sistema que permita validar que los datos presentados en la credencial son legítimos, asumiendo que los datos son verdaderos. En consecuencia, los delincuentes que se dedican al robo y fraude de identidad aprovechan las dos brechas de seguridad para cometer delitos que afectan la estabilidad económica y social de las víctimas, ocasionando pérdidas por 24 mil 870 millones de pesos al cierre de 2020. Con la intención de reducir el impacto del robo y fraude de identidad, se presenta el prototipo de Sistema de Validación de Información de Identidad (SisVal) como alternativa para corroborar que la información de identidad del ciudadano es correcta, sin utilizar un rasgo biométrico. Las pruebas de laboratorio demuestran que SisVal es fácil de implementar, tiene una baja tasa de error y contribuye en la validación de identidad de un ciudadano para reducir el robo y fraude de identidad.

Palabras clave: autenticación, clientes, fraudes bancarios, huella dactilar, prevención, robo de identidad.

I. Introducción

De acuerdo a la convención internacional sobre los derechos del niño, se estableció el derecho a una identidad, que otorga pertenencia a un territorio, sociedad y familia [1]. Además, el término identidad hace referencia a: 1) similitud en todo lo que constituye la realidad objetiva de una cosa y 2) al carácter distintivo o personalidad de un individuo [2]. También se hace referencia de una manera más amplia a la identidad de una persona a través del concepto de datos personales, que se define como [3]: "*es cualquier información concerniente a una persona física identificada o identificable*", y se hace diferencia con los datos personales sensibles. Los datos personales sensibles son aquellos datos personales que afectan a la persona en su círculo social, económico y laboral [3]. Por lo tanto, la identidad de una persona se utiliza para saber que es quien dice ser y toda actividad se pueda vincular a una identidad.

Desafortunadamente, en los últimos años, se ha incrementado el número de víctimas por el delito de robo de identidad, y, en consecuencia, las pérdidas económicas asociadas [4]. De acuerdo al reporte presentado por GIACT Systems LLC [5], en el año 2016, 16.7 millones de consumidores fueron víctimas con un costo estimado de 16 billones de dólares, tan solo en Estados Unidos. En el caso particular de México, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) presentó el informe de reclamaciones imputables a un posible robo de identidad 2011-2015 (primer semestre) donde se hace evidente el crecimiento del delito en nuestro país [6], pasando de 4,564 reclamaciones en 2011 a 28,258 reclamaciones en 2015. Lo anterior se confirma en el reporte presentado por la Asociación de Bancos de México (ABM), en donde, se expone que durante el año 2017 existieron 16 mil 596 casos de robo de identidad, lo que representó un incremento de 213% con respecto al 2016 [7]. En términos económicos, el robo de identidad costó dos mil novecientos sesenta y cinco millones de pesos al mes de septiembre de 2019 [8], y al cierre de 2020, la cifra ascendió a 24 mil 870 millones de pesos [9].

En México, el término de robo de identidad se encuentra definido por la CONDUSEF de la siguiente manera: "*es cuando una persona obtiene, transfiere, utiliza o se apropia de manera indebida, de los datos personales de otra sin la autorización de ésta última, usualmente para cometer un fraude o delito*" [10]; sin embargo, en el proceso definido en [2], [11], se explica que el primer paso realizado por un delincuente es el robo de identidad, siendo el proceso inicial mediante el cual, se recolectan diferentes datos personales de la víctima. El segundo paso hace referencia al fraude de identidad, utilizando la identidad de la víctima, para adquirir bienes y servicios en beneficio del delincuente.

El delincuente puede obtener los datos personales de la víctima a través de acceder a dispositivos personales, buscar en la basura, obtener confianza de la víctima, revisar la correspondencia, y robar documentos [12], [13], [14], [15]. Además, se tiene el enorme descuido de los ciudadanos en cuanto a resguardar sus datos personales; es decir, se entregan documentos, o copias de los mismos, en diferentes instancias públicas y privadas, día a día, compartiendo la seguridad y protección de dichos documentos con terceros [14], [16], [17]. Una vez que el delincuente obtiene los datos personales, los utiliza para acceder a servicios de telecomunicaciones, abrir cuentas, conseguir beneficios del gobierno, obtener un trabajo, realizar fraudes con tarjetas de crédito/débito, y otros crímenes [1], [18].

Debido al aumento en el número de reclamaciones imputables a un posible robo de identidad y a las consecuencias económicas que representa para todos los afectados, la Comisión Nacional Bancaria y de Valores (CNBV) en colaboración con el Instituto Nacional Electoral (INE) desarrollaron una propuesta basada en el uso de datos biométricos para realizar una identificación más segura [19]. Además, el nuevo proceso mantendrá la solicitud de documentos de identidad oficiales, como son la credencial para votar del INE, pasaporte y licencia de conducir.

En el presente artículo, se propone un prototipo que busca contribuir a reducir el impacto del robo y fraude de identidad, en transacciones personales, a través de la verificación de los datos personales contenidos en la credencial para votar y la validación de propiedad de dichos datos; es decir, que los datos correspondan al

propietario original. La contribución utiliza el código de barras unidimensional y número de clave de identificación de la credencial (CIC) para realizar una búsqueda en una base de datos específica donde solo contiene cierta información de identificación, y no se accede a toda la base de datos gestionada por el INE, reduciendo brechas de seguridad. Para validar que los datos corresponden al propietario original, se muestra la fotografía y se calcula la edad para que el verificador pueda validar que realmente es el propietario. La propuesta puede ser implementada en el sector financiero, educativo, laboral, y en elecciones, incrementado la certidumbre que la persona es quien dice ser.

II. Revisión de la literatura

Robo de Identidad

El concepto de robo de identidad es el uso de la información de identificación personal de una víctima sin su consentimiento [20]; sin embargo, es importante comprender que el delito tiene su forma en el mundo real [1], [21], [22] y en el mundo virtual [1], [23], [24]. En ambos casos, el robo de identidad requiere la obtención de la información de identidad y el uso de la misma para afectar la buena reputación, estado emocional, y economía de las víctimas [25], [26].

En el mundo real, el delincuente obtiene la información de identificación personal de la víctima por medio de 1) descuidos del propietario de la identidad; se refiere a que muchas víctimas comparten documentos de su información personal y no se ocupan por el tratamiento de sus datos personales [4]; 2) herramientas tecnológicas; se refiere a que el delincuente utiliza cámaras, escáner, y lectores para copiar o duplicar la información de la víctima; 3) robo de los documentos; se refiere a que el delincuente obtiene los documentos completos de la víctima; y 4) vishing; se refiere a la técnica que utilizan los delincuentes para obtener información de la víctima a través de una llamada utilizando ingeniería social. Una vez que el delincuente obtiene suficiente información personal de la víctima puede continuar con cualquier otra actividad ilegal, principalmente el fraude de identidad.

Por otra parte, en el mundo virtual, el delincuente obtiene la información de identidad de la víctima mediante el uso de herramientas tecnológicas y aprovechando del desconocimiento que existe entre la ciudadanía acerca de los riesgos de seguridad. Entre las principales herramientas tecnológicas se encuentran 1) phishing, se refiere al uso de la tecnología para simular un sitio web amigable/familiar o un correo electrónico proveniente de algún conocido con la finalidad de obtener/recolectar información personal de la víctima; 2) spyware, se refiere a un programa de cómputo que se instala en el equipo de cómputo de la víctima, permitiendo al delincuente recolectar información y obtener documentos.

Los costos ocasionados por este delito incluyen a) costos incurridos en su prevención; b) costos incurridos como consecuencia; y c) costos incurridos en la respuesta [4], [27] [28]. En términos económicos, para el caso mexicano, y de acuerdo a la presentada por la CONDUSEF en su sitio web (https://www.condusef.gob.mx/?p=estadisticas), las perdidas en el tercer trimestre del 2020 ascendieron a 4,414,658 millones de pesos a través del fraude por un medio digital, y a 2,012,111 millones de pesos a través del fraude tradicional. Los fraudes por un medio digital pasaron del 32% en el año 2016 al 69% en el tercer trimestre de 2020; mientras que, los fraudes tradicionales han

disminuido del 68% en 2016 al 31% en el mismo periodo.

Credencial para Votar en México

La credencial para votar es un documento gratuito al que tiene derecho cualquier mexicano al cumplir la mayoría de edad (18 años), brindando la posibilidad de ejercer su derecho al voto. Desde su aparición en 1992, por el extinto Instituto Federal Electoral, la credencial se ha convertido en el medio más utilizado para acreditar la identidad ante cualquier institución pública y/o privada, convirtiéndose en el instrumento de identificación oficial en México [29].

Debido a la importancia e impacto que tiene la credencial para votar, se han agregado medidas de seguridad para reducir actividades ilegales que vulneren los procesos democráticos en el país y/o afecten la integridad de los ciudadanos. Por lo tanto, cada vez que se crean nuevos modelos de la credencial para votar, las credenciales previas dejan de ser válidas con el transcurso del tiempo [30].

Los modelos A, B y C fueron emitidos en 1992, 2002 y 2008, respectivamente, siendo válido el modelo C para votar, durante la realización del presente proyecto. Es importante mencionar que, los tres modelos eran emitidos en territorio nacional y que el modelo útil para votar, durante la realización del presente proyecto, es el modelo C; sin embargo, los tres modelos carecen de un código de barras unidimensional, número de clave de identificación de la credencial (CIC), entre otras características [30].

Los modelos D, E y F fueron emitidos en 2013, 2014 y 2016, respectivamente, siendo válidos para votar los tres modelos. El modelo F fue emitido en el extranjero, siendo la primera vez que se emitió la credencial para votar fuera del territorio nacional. Los tres modelos incluyen un código de barras unidimensional y CIC [30].

Riesgos del uso de Datos Biométricos

Los datos biométricos son cada vez más utilizados como medio de identificación y verificación de identidad [31] [32]. Los datos biométricos utilizados como identificación permiten reconocer a una persona en base a sus características físicas almacenadas en una base de datos; mientras que, los datos biométricos utilizados como verificación permiten validar que la persona es quien dice ser en base a sus características físicas registrados previamente.

Los rasgos biométricos que podemos utilizar son limitados, por ejemplo, el número de huellas dactilares son 10 – considerando que se puedan leer correctamente en cada uno de los dedos de las manos – o el reconocimiento facial o la lectura del iris, entre otros más; sin embargo, también se debe considerar la comodidad para el usuario final. En este sentido, el dato biométrico más utilizado, tanto por aceptación como por comodidad, es la huella dactilar a pesar de no ser el más seguro.

Como consecuencia del uso masivo de datos biométricos por instancias gubernamentales y/o privadas, se tiene un aumento considerable de su almacenamiento en distintas bases de datos. En México, la Ley Federal de Protección de Datos Personales en Posesión de Particulares publicada en 2010 [3] y la Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados publicada en 2017 [33] definen las medidas para su almacenamiento, tratamiento y seguridad. Además, se presentan las diferencias entre un dato personal y un dato personal sensible, siendo evidente la diferencia en su procesamiento

por parte de los departamentos de tecnologías de información y de talento humano de las empresas. También se presentan los derechos ARCO (Acceso, Rectificación, Corrección, y Oposición) que tiene todo ciudadano en México.

Sin embargo, en el trabajo [34] se evidencia que muchos ingenieros – administradores de base de datos, desarrolladores de sistemas o de infraestructura – no tienen clara la diferencia entre un dato personal y un dato personal sensible, ocasionando que se soliciten, almacenen y procesen los datos indistintamente. Está acción pone en riesgo la privacidad de los usuarios y es muy difícil su seguimiento para identificar que se cumpla la normatividad vigente [35], [36]. Esto tiene enorme relevancia considerando que contamos con rasgos biométricos limitados, y su exposición de manera pública pone en mayor riesgo al ciudadano. Por ejemplo, en México, cierto banco utiliza reconocimiento por voz para acceder a servicios específicos por medio de su call center, sin embargo, la frase es la misma por un largo periodo de tiempo y puede ser grabada por los delincuentes con la finalidad de reproducir la frase tantas veces sea necesario para suplantar la identidad de la víctima.

Otro problema asociado al uso de rasgos biométricos es la posibilidad que tiene una instancia de poder trazar las actividades de los ciudadanos [35], [36]. En este sentido, el gobierno tiene mayor control de seguimiento de sus ciudadanos al mantener una base de datos nacional, considerando un bien común o mayor en la pronta detección de posibles amenazas a la seguridad nacional; sin embargo, la misma posibilidad pueden tener instituciones financieras o cualquiera otra organización con fines y propósitos propios, invadiendo la privacidad de las personas.

Medidas para Prevenir el Robo de Identidad

En [4], [14], se hace mención que la responsabilidad para reducir el delito de robo de identidad recae en tres actores: a) personas, son quienes deben resguardar su información de identificación personal; b) instituciones, son las entidades que solicitan, almacenan y resguardan la información de identificación personal adoptando la legislación actual; y c) gobierno, crean las medidas legislativas y normatividad que las instituciones deben seguir para proteger a los ciudadanos y castigar a los infractores. En este sentido, las partes involucradas en el manejo y resguardo de la información de identificación personal conforman una cadena de seguridad que será tan fuerte como su eslabón más débil [15].

Con la intención de alertar a una persona, en México, contra el delito del robo de identidad, el buró de crédito (https://www.burodecredito.com.mx/) – empresa mexicana que mantiene el histórico de información crediticia que sirve para otorgar o negar un crédito – ofrece el servicio de alerta buro. El servicio de alerta buro debe ser contrato por el ciudadano para recibir notificaciones cada vez que una institución financiera o crediticia busca su histórico en las bases de datos del buro de crédito, proceso previo para otorgar un crédito o financiamiento. A través de este proceso, el ciudadano recibe una alerta y en caso de no haber autorizado la búsqueda en la base de datos puede tomar las acciones pertinentes para cancelar la solicitud.

Otras alternativas que existen en el mercado nacional son VeriDocID (Verificación de Documentos de Identidad en https://sumamexico.com/verificacion-de-identidad-biometrica/) y FAD (Firma Autógrafa Digital en https://hola.firmaautografa.com/promocion-

firma-digital) que capturan una imagen de la credencial para votar con la finalidad de revisar los elementos físicos de seguridad. Además, ambas aplicaciones consulta en tiempo real las bases de datos del INE para realizar un proceso de verificación a través del reconocimiento facial. VeriDocID sirve para verificar la validez de un documento de identidad personal para diversos escenarios. Por el contrario, FAD verifica el documento de identidad personal y permite grabar un video de la persona como evidencia de vida para abrir cuentas bancarias, en específico.

III. Materiales y Equipos

El proyecto se desarrolló en el laboratorio de seguridad y servicios electrónicos de la Universidad De La Salle Bajío utilizando cuatro laptops con procesador core i5, 8 GB de memoria RAM y disco duro de 1 TB. Se utilizaron dos switch catalyst 2960 y tres routers 2900 series para probar la conexión segura a través de una VPN. Se desarrollaron dos versiones utilizando los lenguajes de programación utilizados fueron JAVA y C#, y el gestor de base de datos fue Microsoft SQL server 2012. Es importante mencionar que, la configuración utilizada en los routers es conocida y se encuentra documentada por Cisco[1], por tal motivo, se omite la explicación de su configuración en el documento.

La metodología empleada en el desarrollo del proyecto se muestra en la Figura 1. El primer paso fue revisar la literatura relacionada al robo de identidad, considerando la revisión de artículos publicados en idioma español e inglés. Los artículos se buscaron a través del scholar.google.com y se consideraron artículos que describieran los tipos de robo de identidad y presentaran una definición. Posteriormente, se buscaron artículos que explicarán el impacto y consecuencias en las víctimas del delito para comprender la gravedad del ataque. Es importante mencionar que, se consultaron datos publicados por la CONDUSEF y notas periodísticas con la intención de sensibilizar a los estudiantes sobre los beneficios que puede tener el proyecto.

En el segundo paso, se definió la propuesta considerando la información obtenida de la credencial para votar, identificando que es el medio de identificación oficial en México, y que cuenta con varias medidas de seguridad. También se identificaron los datos que deberían ser consultados y validados por la propuesta, como son el nombre, edad actual y fotografía. En el tercer paso, se definieron los lenguajes de programación para desarrollar la aplicación y el gestor de base de datos. También se probaron dos modelos de lectores de código de barras para determinar la mejor opción y evitar teclear algún dato con la finalidad de reducir errores de dedo.

Una vez definida la propuesta y la tecnología a utilizar, se procedió con el desarrollo de la aplicación utilizando la metodología en cascada debido a ser la mejor opción para grupos de trabajo pequeños y poder probar los avances por módulos, permitiendo la identificación rápida de errores o áreas de oportunidad. La configuración de los equipos de red se realizó en dos días utilizando equipos de la marca Cisco®. Al finalizar la aplicación, se realizaron pruebas con diferentes modelos de credenciales para votar, y se consideraron casos donde se utilizaba una credencial para votar falsa, simulando un robo de identidad, y como la propuesta evidenciaba el ataque.

[1] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ikevpn/configuration/xe-3s/sec-ike-for-ipsec-vpns-xe-3s-book/sec-encrypt-preshare.html y https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/9221-quicktip.html

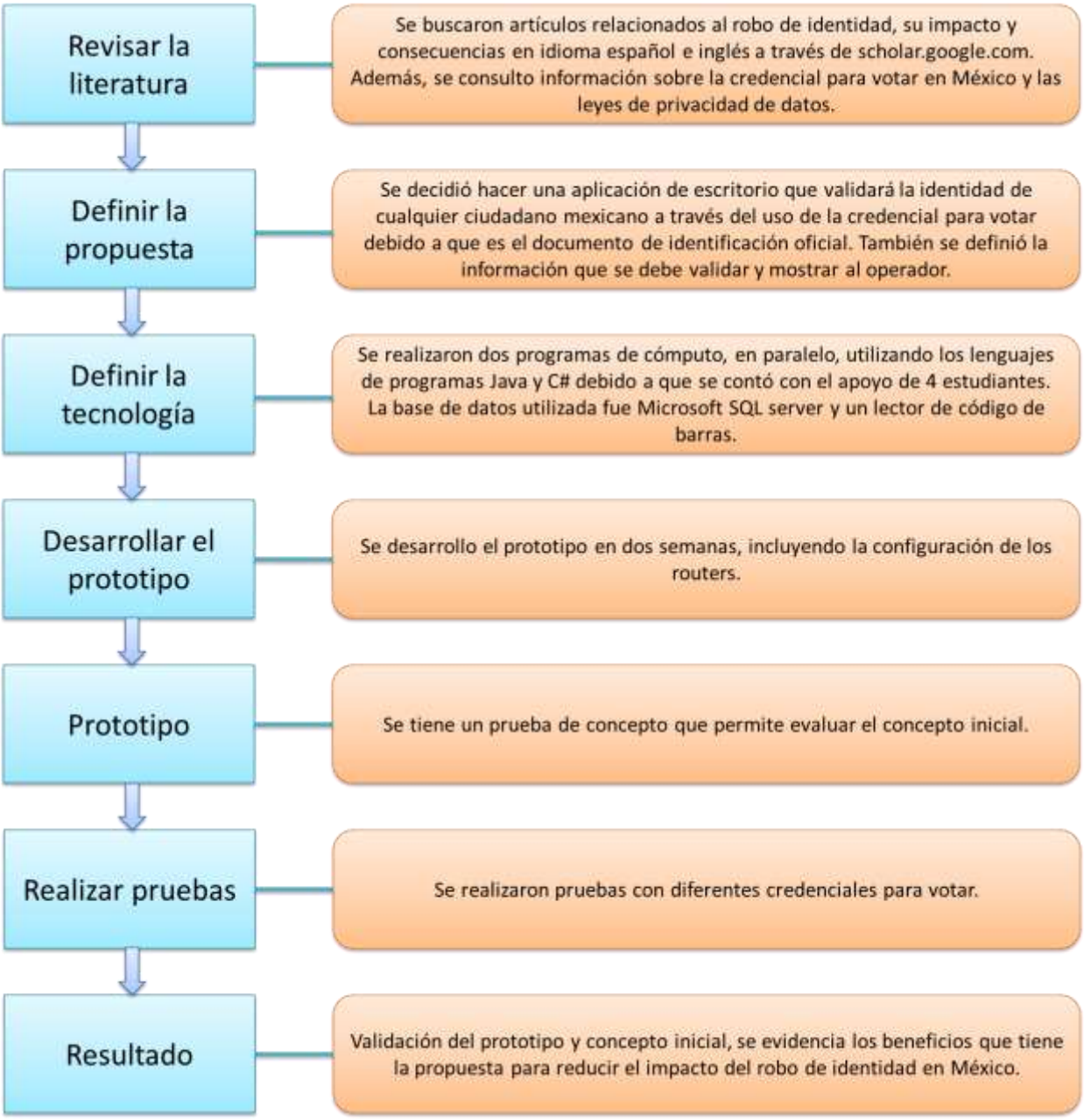


Figura 1. Metodología empleada para desarrollar el proyecto.

IV. Métodos Experimentales

Con la finalidad de reducir el impacto del ataque de robo de identidad, se propone el sistema de validación de información de identidad o SisVal. SisVal es un sistema que requiere de un servidor de base de datos, una aplicación de escritorio, un lector de código de barras, conexión a Internet, y un verificador que, en su conjunto permiten validar la información de identidad de cualquier ciudadano mexicano con credencial para votar vigente. SisVal se puede implementar en cualquier negocio o empresa donde se requiera verificar la información de identidad de una persona

durante un proceso, por ejemplo, contratación de personal, trámite de un crédito, reserva de una habitación, o control de acceso.

Supuestos

Se tienen contemplados los siguientes supuestos que hacen posible la realización del presente proyecto.

1. El INE es propietario de la infraestructura tecnológica (servidores de base de datos y servidores VPN) que da origen a SisVal.
2. El INE mantiene seguro el acceso al servidor de base de datos general – donde se encuentran los datos personales de todos los mexicanos – sin acceso a través de SisVal, protegiéndolos con corta fuegos y otras medidas de seguridad.
3. El INE crea y mantiene un servidor de base de datos particular – donde se encuentra la información que se puede consultar a través de SisVal – con acceso a través de una VPN.
4. El INE permite consultar el código de identificación de la credencial (CIC) para mostrar el nombre completo, fotografía y fecha de nacimiento de cada ciudadano a través de SisVal.
5. El INE tiene los procedimientos para permitir formar parte de SisVal que incluyen: contrato, reglamento, políticas de uso, políticas de privacidad, entre otros.
6. Las entidades o verificadores que utilizan SisVal cuentan con conexión a Internet y la capacidad para establecer un canal de comunicación seguro por VPN.
7. Las entidades o verificadores que utilizan SisVal tienen instalado SisVal en los equipos de cómputo necesarios.
8. Las entidades o verificadores que utilizan SisVal tienen un lector de código de barras para leer el CIC de la credencial para votar.
9. Las credenciales para votar a utilizar son de tipo D, E y F.

Entidades de SisVal

SisVal se encuentra conformado por las siguientes entidades:

- Aplicación de escritorio que permite capturar los datos de entrada y mostrar el resultado de la validación de identidad. La aplicación se encuentra desarrollada en visual.net.
- Lector de código de barras para leer el código de barras unidimensional de la credencial para votar tipo D, E y F.
- Servidor de base de datos INE particular que contiene el nombre completo, fotografía y fecha de nacimiento de cada ciudadano; además, se incluye el código de identificación de la credencial (CIC) para realizar la validación de identidad por medio de la credencial para votar tipo D, E y F.
- Servidor de base de datos INE general que contiene todos los datos personales de los ciudadanos mexicanos. Este servidor no se utiliza en SisVal pero es la fuente de datos desde donde se exportan los datos personales de los ciudadanos mexicanos al servidor de base de datos INE particular.
- Servidor VPN que permite establecer un canal de comunicación seguro con los diferentes usuarios o entidades.
- Entidades son los negocios o empresas que hacen uso de la aplicación de escritorio en sus procesos donde requieren validar la identidad de una persona.

- Verificador es el usuario final que utiliza SisVal para corroborar la identidad de otro ciudadano.

Arquitectura de SisVal

Las entidades y su interacción se presentan en la Figura 2. Es importante mencionar que, todos los servidores se contemplan propiedad del Instituto Nacional Electoral (INE), y las entidades o verificadores consumen el servicio.

Como se muestra en la Figura 2, el INE mantiene y administra los servidores de base de datos. En el presente proyecto, se simplifica la arquitectura considerando un servidor de base de datos general donde se almacenan los datos personales y sensibles de los ciudadanos mexicanos que son obtenidos a través del proceso para obtener la credencial para votar que todo ciudadano realiza al cumplir dieciocho años. El otro servidor de base de datos se ha nombrado particular, y es el servidor que consulta la aplicación.

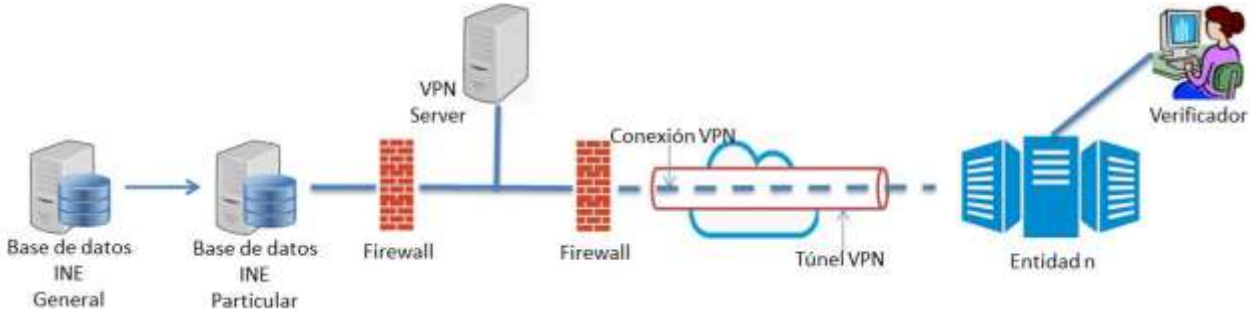


Figura 2. Arquitectura de SisVal.

Los cortafuegos o *firewalls* sirven para proteger el acceso desde Internet a la red local, manteniendo seguro el acceso a las bases de datos. El servidor VPN se encarga de realizar la autenticación de las entidades para establecer un canal de comunicación seguro, utilizando IPsec u otro protocolo. En este proyecto, se ha utilizado una configuración de autenticación nombrada "*pre-share*" utilizando equipo de la marca Cisco®. La comunicación entre las entidades y la base de datos particular se realiza a través de un canal de comunicación seguro con una VPN. Se utiliza una VPN porque se crea el túnel bajo demanda cuando se requiere verificar la identidad de una persona con SisVal. A través de la VPN viaja la solicitud de verificación del CIC, al ser el ID en la base de datos. El servidor de base de datos particular se encarga de entregar los datos relacionados a la clave primaria para que la aplicación de escritorio pueda calcular la edad del ciudadano y mostrar el resultado.

La Figura 2 muestra que cualquier entidad – privada o gubernamental – puede hacer uso de SisVal con una conexión a Internet. SisVal se ha diseñado para que cualquier entidad que requiere verificar la información de identidad de un ciudadano mexicano pueda hacerlo sin restricciones, con la única finalidad de reducir el impacto del robo y suplantación de identidad.

Proceso y Desarrollo de SisVal

SisVal ha sido diseñado para verificar la información de identidad de cualquier ciudadano mexicano que cuenten con una credencial para votar expedida por el INE, y

que se encuentre vigente. El proceso para obtener la credencial para votar se encuentra disponible en el siguiente enlace de Internet https://www.ine.mx/credencial/credencial-proceso/, y no se considera ningún cambio o modificación al respecto.

Las entidades o verificadores que deseen hacer uso de SisVal deberán solicitar ser miembros del sistema. En caso de cumplir con todo lo solicitado por el INE, se entregarán los parámetros necesarios para establecer una conexión segura y la aplicación de escritorio. La conexión segura se puede hacer por medio del protocolo IPsec. Posteriormente, se entregará la aplicación de escritorio que deberá ser instalada en los equipos de cómputo donde se verificará la identidad de los ciudadanos mexicanos. La adquisición de lector de código de barras es responsabilidad de cada entidad o verificador. En este punto, se tienen los elementos claves para hacer uso de SisVal.

SisVal cuenta con un servidor de base de datos nombrado INE particular que contiene dos tablas. La primera tabla almacena los datos personales de ciudadanos mexicanos. Los datos personales han sido copiados desde la base de datos INE general. La tabla de validación de identidad contiene los siguientes campos (ver Tabla 1): identificador que es único a través del uso del CIC, nombre completo del ciudadano, fecha de nacimiento, y la fotografía tomada el día que tramitó su credencial.

Tabla 1. Tabla de validación de identidad.

Campo	Tipo de dato	Tamaño	Descripción
ID	Numérico	10	Código Identificador de la Credencial
Nombre	Carácter	100	Nombre completo del ciudadano
Fnacimiento	Fecha	8	Fecha de nacimiento del ciudadano
Imagen	Carácter	255	Ruta de ubicación de la fotografía

La segunda tabla almacena las transacciones sobre validación de identidad que se realizan a través de SisVal. La tabla de transacciones sobre validación de identidad contiene los siguientes campos (ver Tabla 2): identificador de la transacción, el CIC utilizado, nombre completo del solicitante, fecha, y el estatus de la transacción.

Tabla 2. Tabla de transacciones sobre validación de identidad.

Campo	Tipo de dato	Tamaño	Descripción
IDTran	Numérico	10	Identificador de la transacción
ID	Carácter	10	Código Identificador de la Credencial
Nombre	Carácter	100	Nombre completo del ciudadano
Ftran	Carácter	60	Fecha de la transacción
Estatus	Carácter	8	Transacción aceptada o rechazada

En el momento que deban verificar la identidad de un ciudadano mexicano, se deberá solicitar la credencial para votar del tipo D, E o F. Con la credencial en manos del verificador, se procederá a leer el CIC que se muestra en la Figura 3 (A). Es importante mencionar que, el CIC se encuentra codificado en el código de barras que se encuentra dentro del rectángulo color rojo. Por lo tanto, el lector de código de barras es utilizado para introducir el CIC a SisVal. También se puede introducir el CIC de manera manual; sin embargo, con el lector de código de barras se pueden reducir errores. SisVal se encuentra conectado a la base de datos INE particular para traer los

datos relacionados con el CIC. Con los datos en la aplicación, se calcula la edad del ciudadano a partir de la fecha de nacimiento del ciudadano.

Se hace énfasis que SisVal consulta (lee) los datos almacenados en la base de datos INE particular, y en ningún momento se escriben o modifican datos. Con la información procesada, se muestra el resultado en la aplicación de escritorio de SisVal (ver Figura 3 (B)). La aplicación de escritorio muestra en pantalla el ID o CIC, nombre completo del ciudadano, su edad actual, y la fotografía que se encuentra almacenada en el servidor de base de datos del INE particular.



Figura 3. CIC impreso en la credencial y aplicación de escritorio SisVal.

Ejemplo de Utilidad de SisVal

Con la intención de ejemplificar el beneficio de SisVal, se presenta un escenario de utilidad genérico. Se asume que el banco X hace uso de SisVal, y en el proceso de cambio de cheque se debe corroborar la identidad del ciudadano que solicita el cambio de cheque.

El verificador (cajera o cajero) solicita al ciudadano su credencial para votar del INE. Con la credencial para votar en su mano, se procede a leer el CIC con el lector de código de barras, como se muestra en la Figura 4.



Figura 4. Lectura del CIC a una credencial para votar del INE.

Como se puede ver en la Figura 5 (A), SisVal muestra el resultado de la consulta, nombre completo, edad y fotografía del ciudadano, permitiendo al verificador determinar si se trata de la persona correcta o es un intento de robo de identidad. Además, se activan el botón aceptado

(*accepted*) o el botón rechazado (*rejected*). En caso que, los datos proporcionados por SisVal no coincidan con la apariencia física de la persona, el verificador determina que no se trata de la misma persona, y, por ende, no realiza el cambio de cheque. Adicionalmente, el verificador puede guardar evidencia de la transacción presionando el botón rechazar. En caso contrario, el verificador presiona el botón aceptar para guardar evidencia sobre la transacción de manera positiva (ver Figura 5 (B)).

En el caso que la credencial para votar sea falsa, SisVal muestra un mensaje de error y los datos del nombre, edad y fotografía aparecen en blanco, alertando al verificador sobre el intento de robo de identidad (ver Figura 5 (C)). En este caso, se habilita el botón rechazar para que el verificador guarde evidencia sobre el intento de robo de identidad (Figura 5 (D)).

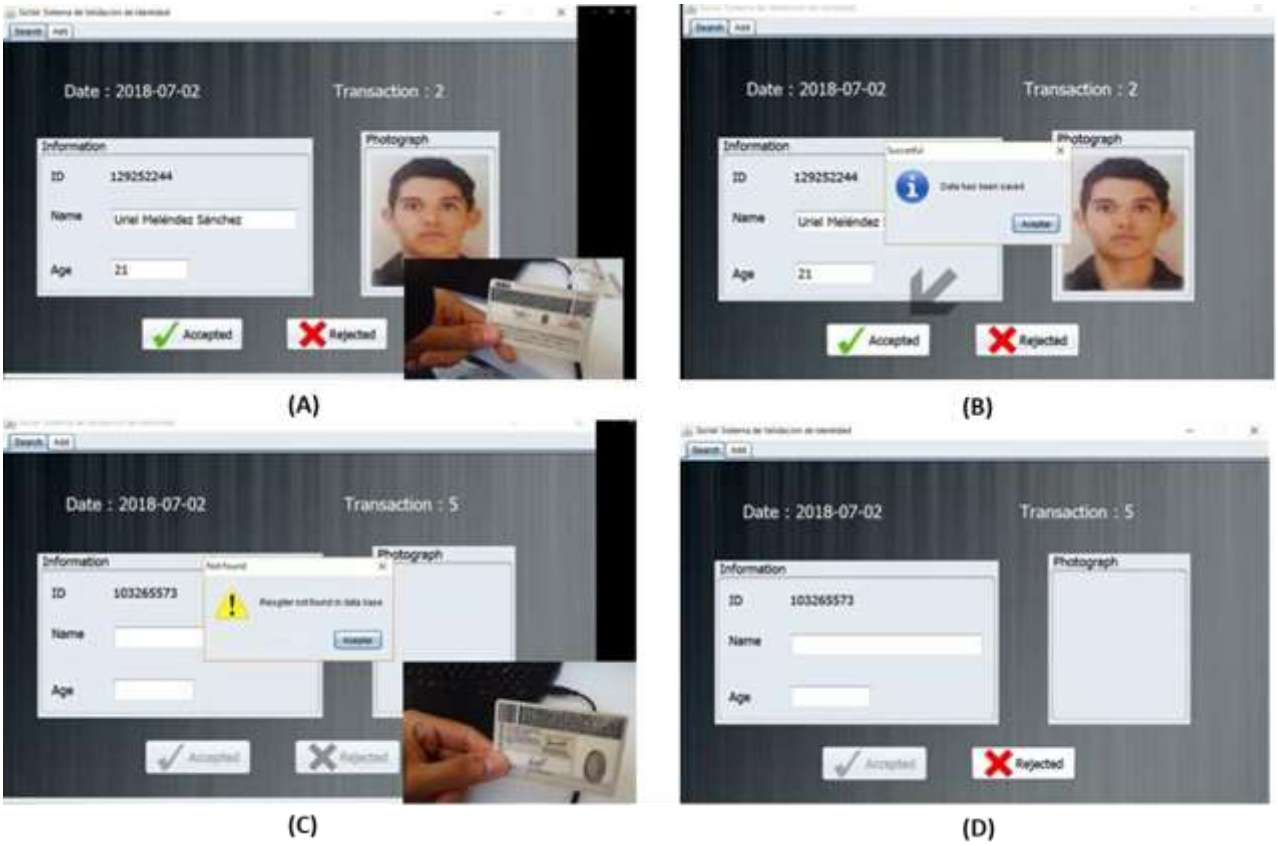


Figura 5. Resultado de verificación de identidad con SisVal.

V. Discusión de Resultados

SisVal es una herramienta que contribuye a combatir el robo y fraude de identidad mediante la validación de la información personal presentada en la credencial para votar; en consecuencia, se puede incrementar la seguridad y utilidad de la credencial a nivel nacional. Con la intención de presentar las ventajas que ofrece SisVal en comparación con la solución desarrollada por el INE y la CNBV, se realiza la siguiente comparativa.

Inicialmente, se hace mención que la solución del INE y CNBV requiere la

adquisición de lectores de huella dactilar, y, por ende, se utiliza un dato biométrico de los ciudadanos mexicanos, manteniendo el uso de la credencial para votar. Además, se hace uso de un dato sensible de acuerdo a la Ley Federal de Protección de Datos Personales del 2010, requiriendo mayor inversión en medidas de seguridad físicas y lógicas para reducir riesgos de seguridad. Por otra parte, la solución propuesta en este artículo hace uso exclusivo de la credencial para votar y un lector de código de barras, requiriendo menor inversión.

En la Tabla 3, se hace evidente que la adquisición de un lector de huella dactilar es más costosa que un lector de código de barras, requiriendo mayor inversión para las entidades. En cuanto al espacio que requiere, ambos dispositivos requieren un espacio reducido en el escritorio, permitiendo buena movilidad. El lector de huella dactilar es menos intrusivo que otros lectores biométricos; sin embargo, el lector de código de barras no realiza la lectura de ningún dato biométrico.

Tabla 3. Comparativa entre soluciones.

Características	Huella dactilar	Código de barras
Costo	$1,370.00	$600.00
Medidas	5.30 x 7.50 x 1.00 pulgadas	5.82 x 2.82 x 4.72 pulgadas
Intrusivo	Muy Baja	No aplica
Comodidad para el ciudadano	Media	Alta
Comodidad para el verificador	Media	Media
Tasa de error	.02 y 0.5 por ciento	1/5,000,000 por ciento

Otra característica considerada es la comodidad para el ciudadano. En este caso, el lector de huella dactilar ofrece una comodidad media para el ciudadano debido a que debe colocar el dedo en la posición correcta, tantas veces sea necesario, mientras que, con el uso del lector de código de barras la comodidad es alta debido a que el verificador es quien realiza la lectura.

En cuanto a la comodidad para el verificador, el lector de huella dactilar y el lector de código de barras ofrecen un nivel de comodidad media debido a que debe interactuar con el sistema en ambos casos.

Un punto clave, es la tasa de error que ambos lectores o técnicas presentan. Si bien es cierto que, la tasa de error de la huella dactilar es baja, entre 0.2 y 0.5 por ciento, la tasa de error del código de barras es de 1/5 millones por ciento; es decir, los falsos rechazos se producen más con el lector de huella dactilar que con el lector de código de barras. Además, el porcentaje de un falso rechazo depende en que los ciudadanos coloquen el dedo correctamente en el sensor, mientras que, con el lector de código de barras la exigencia de la posición es menos restrictiva.

Un componente clave en SisVal es la base de datos de transacciones sobre validación de identidad donde se pueden guardar las solicitudes no exitosas y rechazadas por el validador en base a: a) la credencial para votar es falsa al no encontrar su registro, b) no hay coincidencia entre la información visualizada por SisVal y la información contenida en la credencial para votar, y c) intento de suplantación de identidad. Con la información almacenada en la base de datos

de las transacciones sobre validación de identidad, se pueden identificar las credenciales que han sido reportadas como robadas o extraviadas, y se encuentran en uso por usuarios mal intencionados.

VI. Conclusiones

SisVal es una herramienta tecnológica que permite validar la identidad de cualquier ciudadano mexicano a través de verificar los datos personales contenidos en la credencial para votar, expedida por el INE, con la finalidad de reducir el impacto del robo y fraude de identidad en México.

Si bien es cierto que, se cuenta con una solución basada en el uso de datos biométricos, en específico la huella dactilar, su implementación en micro, pequeñas y medianas empresas puede llegar a ser costoso por la inversión inicial y las medidas de seguridad adicionales que se deben implementar. Además, se mantiene la solicitud de la credencial para votar como medio de identificación a lo largo y ancho del país, sin un mecanismo de validación. En este sentido, SisVal incrementa la seguridad en el uso de la credencial para votar, aumentando la certeza de quien realiza el trámite es quien dice ser, y se requiere una menor inversión inicial en la adquisición de los lectores de código de barras, ampliando sus posibilidades de uso.

VII. Agradecimientos

Se agradece a los miembros que integran el Honorable Consejo General, Honorable Consejo Técnico y Coordinación General del Programa Delfín, y a los Consejeros Técnicos de las instituciones participantes en el proyecto por haber impulsado la movilidad de sus estudiantes.

VIII. Referencias

[1] Barba Álvarez, R., El robo de identidad en México. Revista de investigación en Derecho, Criminología y Consultoría Jurídica, No. 22, 246-260, 2018.

[2] Sproule, S., Archer, N., Defining Identity Theft. Eight World Congress on the Management of eBusiness (WCMeB), 1-11, 2007. DOI: 10.1109/WCMEB.2007.5

[3] CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. Ley Federal de Protección de Datos Personales en posesión de los Particulares. [En línea] Disponible http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

[4] Leeper Piquero, N., Piquero A.R., Gies S., Green B., Bobnis, A., & Velasquez, E. Preventing Identity Theft: Perspectives on Technological Solutions from Industry Insiders. Victims & Offenders, 16(3), 444-463, 2021. DOI: 10.1080/15564886.2020.1826023

[5] GIACT Systems LLC, Infographic the growing costs of identity fraud. [En línea] Disponible https://www.giact.com/infographic-the-growing-costs-of-identity-fraud/.

[6] CONDUSEF, Reclamaciones imputables a un posible robo de identidad 2011-2015 (1er. semestre). [En línea] Disponible https://www.condusef.gob.mx/documentos/com71_reclamaciones-robo-identidad.pdf.

[7] ABM, Síntesis informativa. [En línea] Disponible https://www.abm.org.mx/sala-de-prensa/sintesis/historial/sintesis_2018_04_09.pdf.

[8] Hernández, A., Robo de identidad cuesta 2 mil 965 mdp. El Universal. [En línea]

Disponible https://www.eluniversal.com.mx/cartera/robo-de-identidad-cuesta-2-mil-965-mdp.

[9] Hernández, A., En 2020, por posibles fraudes, cliente reclamaron a los bancos 24 mil 870 mdp. El Universal. [En línez] Disponible https://www.eluniversal.com.mx/cartera/en-2020-por-posibles-fraudes-clientes-reclamaron-los-bancos-24-mil-870-mdp.

[10] Amigón, E., Robo de identidad, un delito en aumento. Primer plano, 20-23, 2015.

[11] Koops, B.J., Leenes, R., Identity Theft, Identity Fraud and/or Identity-related Crime. Datenschutz und Datensicherheit - DuD, 30(9), 553-556, 2006. https://doi.org/10.1007/s11623-006-0141-2

[12] National Fraud Authority, Fraud typologies and victims of fraud: Literature review. [En línea] Disponible https://researchportal.port.ac.uk/portal/files/1926122/NFA_report3_16.12.09.pdf.

[13] Abdullah, A.K., Protecting your good name: identity theft and its prevention. 1st annual conference on information security curriculum development (InfoSecCD), 102-106, 2004. https://doi.org/10.1145/1059524.1059547

[14] Burnes, D., DeLiema, M., Langton, L. Risk and protective factors of identity theft victimization in the United States. Preventive Medicine Reports, 17, 2020. https://doi.org/10.1016/j.pmedr.2020.101058

[15] Center for Victim Research. What we know about identity theft and fraud victims from research- and practice- based evidence. Research Report, 1-36, 2019.

[16] Martínez, F.R.C., Candelaria, A.D.H., Lozano, M.A.R., Zúñiga, A.R.R., Peláez, R.M., & Michel, J.R.P., Después de presionar el botón enviar, se pierde el control sobre la información personal y la privacidad: Un caso de estudio en México. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, No. 21, 115-128, 2017. http://dx.doi.org/10.17013/risti.21.115-128

[17] Federal Trade Commision, Identity Theft. [En línea] Disponible https://www.consumer.ftc.gov/articles/0005-identity-theft.

[18] Gordon, G.R., Willox, N.A., Identity Fraud: A critical national and global threat. Economic Crime Institute, 1-48, 2003.

[19] INE, INE colabora con instituciones bancarias para prevenir robo de identidad y fraudes a partir de la identificación de huellas dactilares. Central Electoral. [En línea] Disponible https://centralelectoral.ine.mx/2019/02/17/ine-colabora-instituciones-bancarias-prevenir-robo-identidad-los-fraudes-partir-la-identificacion-huellas-dactilares/.

[20] Golladay, K & Holtfreter, K., The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes. Victims & Offenders, 12(5), 741-760, 2017. DOI: 10.1080/15564886.2016.1177766

[21] Saunders, K.M. and Zucker, B., Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. Cornell Journal of Law and Public Policy. 8(3), 1999. https://doi.org/10.1080/13600869955134

[22] Harrell, E. Victims of identity theft, 2016. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. 2019.

[23] Green, B., Gies, S., Bobnis, A., Leeper Piquero, N., Piquero, A.R., & Velasquez, E., Exploring Identity-Based Crime Victimizations: Assessing Threats and Victim Services among a Sample of Professionals. Deviant Behavior, 2020. DOI: 10.1080/01639625.2020.1720938

[24] Liu, F., Does identity theft insurance undermine risk perceptions and increase risky behavioral intentions?. Asian economic and financial review, 9(8), 926-935, 2019.

[25] Maitlo, A., Ameen, N., Peikari, H.R. and Shah, M., Preventing identity theft: Identifying major barriers to knowledge-sharing in online retail organisations. Information Technology & People, 32(5), 1184-1214, 2019. https://doi.org/10.1108/ITP-05-2018-0255

[26] Li, Y., Yazdanmehr, A., Wang, J., Raghav Rao, H., Responding to identity theft: a victimization perspective. Decision Support Systems, 121, 13-24, 2019. https://doi.org/10.1016/j.dss.2019.04.002

[27] Wyre M., Lacey D., and Allan K., The identity theft response system. Trends & issues in crime and criminal justice no. 592. Canberra: Australian Institute of Criminology. 2020.

[28] Sovern, J., Stopping identity theft. The journal of consumer affairs, 38(2), 233-243, 2004. https://doi.org/10.1111/j.1745-6606.2004.tb00866.x

[29] Ruiz Saldaña, J.R., Un itinerario garantista: sobre la credencial para votar en México. Revista Derecho Electoral, No. 31, 253-259, 2021.

[30] INE, No todas las credenciales votan. [En línea] Disponible https://www.ine.mx/wp-content/uploads/2019/12/ABC_CREDENCIAL2020.pdf.

[31] Martinez-Peláez, R., Pomykała, J., Rico-Novella, F., and Satizabal, C., Using fingerprint biometric-based identification on tables of poker and blackjack to enhance the security in casinos., in: Metody biometryczne i kryptograficzne w zintegrowanych systemach bezpieczeństwa, Wyższa Szkoła Menedżerska, Warszawa 2011.

[32] Yellamma, P., Rajesh, P.S.S., Pradeep, V.V.S.M., and Manishankar, Y.B., Privacy preserving biometric authentication and identification in cloud computing. International Journal of Advanced Science and Technology, 29(6), 3087-3096, 2020.

[33] CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. Ley Federal de Protección de Datos Personales en posesión de los Particulares. [En línea] Disponible https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017.

[34] Villaverde Hidalgo, L.C., Análisis de cultura de seguridad informática. Tesis para obtener el título de Ingeniero en Tecnologías y Soluciones de Negocio. Universidad De La Salle Bajío, 2018.

[35] Kugler, M.B., From identification to identify theft: public perceptions of biometric privacy harms. UC Irvine Law Review, 10(1), 107-152, 2019.

[36] Bisztray, T., Gruschka, N., Mavroeidis, V., Fritsch, L., Data protection impact assessment in identity management with a focus on biometrics. In: Roßnagel, H., Schunck, C. H., Mödersheim, S. & Hühnlein, D. (Hrsg.), Open Identity Summit 2020. Bonn: Gesellschaft für Informatik e.V. (S. 185-192). DOI: 10.18420/ois2020_17

ANEXO A

A continuación, se muestra el código para leer el CIC de la credencial para votar del INE y el código para calcular la edad del ciudadano:

```
Private void LeerCodigo(object sender, KeyEventArgs e)
    {
      Try
      {
        if (e.KeyCode != Keys.ShiftKey && e.KeyCode != Keys.Return && e.KeyCode != Keys.OemOpenBrackets)
          mensaje += e.KeyCode.ToString()[e.KeyCode.ToString().Length - 1];

        if (e.KeyCode == Keys.Return)
        {
          lblError.Text = "";
          Conexion con = new Conexion();
          per = new Persona();
          per = con.GetAll(mensaje);

          lblEdad.Text = CalcularEdad(per.FechaNacimiento).ToString();
          lblId.Text = per.ine_id;
          lblNombre.Text = per.Nombre;
          imgFoto.Image = per.Imagen;
          per.ine_id = mensaje;

          mensaje = "";
        }
      }
      catch (Exception ex)
      {
        lblError.Text = "NOT FOUND\n SORRY :(";
        lblNombre.Text = "";
        lblEdad.Text = "";
        lblId.Text = "";
        imgFoto.Image = null;
        mensaje = "";
      }
    }
```