IDENTIFICACIÓN DIGITAL E INFRAESTRUCTURA PARA INCREMENTAR LA SEGURIDAD EN EL CIBERESPACIO

Francisco R. Cortes Martínez

Universidad Autónoma de Ciudad Juárez, División Multidisciplinaria de Ciudad Universitaria

al114359@alumnos.uacj.mx

Ángel D. Herrera Candelaria

Universidad Autónoma de Ciudad Juárez, División Multidisciplinaria de Ciudad Universitaria

al114847@alumnos.uacj.mx

Rafael Martínez Peláez

Universidad de la Salle Bajío, Facultad de Ingeniería en Computación y Electrónica

rmartinezp@delasalle.edu.mx

Yesica I. Saavedra Benítez

Instituto Tecnológico de Toluca, División de Estudios de Posgrado e Investigación

ysaavedrab@toluca.tecnm.mx

Pablo Velarde Alvarado

Universidad Autónoma de Nayarit, Área de Ciencias Básicas e Ingenierías

pvelarde@uan.edu.mx

Resumen

El número de usuarios de Internet crece día a día y el mecanismo utilizado para registrar nuevos usuarios continúa siendo el formulario de registro web. Las funciones del formulario de registro web son verificar el formato utilizado en cada campo y revisar que todos los campos se encuentren completados. Puesto que, el formulario de registro web no tiene la función de verificar la información capturada por el usuario, se puede utilizar información falsa o robada para crear cuentas de usuario. En consecuencia, usuarios maliciosos pueden crear cuentas falsas y realizar actividades ilegales, tales como acoso sexual, *bullying*, suplantación de identidad, trata de personas, entre otras. Por consiguiente, se propone una

identificación digital que contenga información del ciudadano y se pueda verificar su legitimidad. También, se presenta una propuesta de infraestructura que puede sustentar los procesos de registro, generación, expedición, y usabilidad de la identificación digital.

Palabra(s) Clave(s): Autenticación, delito, servicios electrónicos, sitio de redes sociales, suplantación de identidad.

1. Introducción

Un mecanismo de autenticación se compone de los procesos de identificación y validación [1]. El proceso de identificación permite al usuario presentar su credencial; mientras que, el proceso de validación permite a la autoridad verificar la legitimidad de dicha credencial. El resultado de una autenticación positiva otorgará permisos o privilegios al usuario dentro del sistema. En Internet, el mecanismo de autenticación más utilizado es la combinación de usuario-contraseña [1]. Sin embargo, un proceso clave para todo mecanismo de autenticación es el registro de los usuarios. El proceso de registro [1] de usuarios permite corroborar la información de un usuario antes de otorgarle su identificador dentro del sistema.

El registro de usuarios en Internet se realiza por medio del formulario de registro web. El formulario de registro web permite recolectar información personal de cada usuario para su almacenamiento posterior. Por medio del formulario de registro web, se puede validar el formato utilizado en cada campo o que todos los campos se encuentren completados [2]. Una vez concluido el llenado del formulario de registro web, se procede a enviar los datos personales al servidor remoto. Los datos personales son transmitidos a través de un canal de comunicación seguro, utilizando certificados digitales [3] y el protocolo *Secure Socket Layer* (SSL) [4] o *Transport Layer Security* (TLS) [5], en la mayoría de los casos. No obstante, el formulario de registro web no tiene la capacidad de corroborar la veracidad de los datos utilizados por los usuarios de Internet. Es decir, un usuario de Internet puede utilizar información falsa o robada para completar un formulario de registro web.

El hecho de la falta de un procedimiento o mecanismo que permita corroborar la veracidad de los datos utilizados para crear una cuenta de usuario y ser miembro de un sistema, ha permitido que usuarios maliciosos realicen acciones delictivas, como son: acoso sexual, operaciones comerciales fraudulentas, suplantación de identidad, trata de personas, entre otras. Lo anterior se ve reflejado en el número creciente de denuncias relacionadas con delitos realizados a través de sitios de redes sociales[1,2] o en el número de quejas por compras no reconocidas con tarjetas de crédito/debito[3,4].

El artículo se encuentra estructurado de la siguiente forma. En la sección 2, se describen tres ataques realizados para demostrar lo vulnerable que es el ciberespacio. En la sección 3, se introduce la identificación digital – sus componentes – y su infraestructura – centros y procesos. Se presenta un análisis de seguridad sobre el uso de la identificación digital en el ciberespacio, en la sección 4. Finalmente, se dan las conclusiones en la sección 5.

2. Ataques a sitio de red social y servicio electrónico

Para ilustrar el problema, se presenta brevemente una serie de ataques realizados al sitio de red social más popular en México y a uno de los servicios de correo electrónico más utilizados en Latinoamérica.

Primero, se decidió crear una identidad falsa a partir de nombres poco comunes. La identidad falsa tiene los siguientes datos: fecha de nacimiento, lugar de residencia, colegios, grados académicos, entre otros. Una vez creada la identidad falsa, se completó el formulario de registro web para crear una cuenta de correo electrónico, utilizando la identidad falsa. La cuenta de correo electrónico se generó sin ningún contratiempo. Posteriormente, se procedió a crear una cuenta de

[1] http://www.milenio.com/politica/Condusef-robo_de_identidad_0_707929207.html

[2] http://www.interpol.int/es/Criminalidad/Delitos-contra-menores/Delitos-contra-menores

[3] http://ntrzacatecas.com/2014/03/09/alerta-condusef-por-cargos-no-reconocidos-en-tarjetas-bancarias/

[4] http://www.razon.com.mx/spip.php?article174743

usuario en el sitio de red social con la misma identidad falsa y el correo electrónico. Al finalizar el procedimiento, se obtuvo una cuenta de usuario.

Para dar continuidad al ataque, se decidió enviar solicitudes de amistad a usuarios que tuvieran gustos en común con nuestro usuario falso. Al paso del tiempo, la cuenta de usuario continúa incrementando su número de amigos y es miembro de algunos grupos.

Las actividades se han realizado en diferentes lugares – cibercafés y redes inalámbricas abiertas –, se ha cambiado la dirección MAC del equipo, y se ha utilizado más de un equipo de cómputo para reducir la posibilidad de ser detectados. También, se pueden utilizar algunas herramientas para crear cuentas de usuario con información falsa o robada.

En conclusión, se ha demostrado lo fácil que es crear una cuenta de usuario debido a la falta de un procedimiento o mecanismo de verificación de identidad.

3. Identificación digital e infraestructura para crear cuentas de usuarios en el ciberespacio

A partir del análisis presentado en la sección anterior, se propone una identificación digital. La identificación digital tiene el objetivo de presentar información de cada ciudadano para reemplazar el uso del formulario de registro web. Se puede entender a la identificación digital como la representación electrónica de un documento de identificación, estructurado lógicamente con información de un ciudadano, para conocer su identidad en el proceso de creación de una cuenta de usuario en sitios de red social o servicios electrónicos, privados o públicos. La identificación digital se encuentra constituida por las siguientes categorías:

- La categoría de identidad del ciudadano contiene información personal de cada ciudadano para su identificación. El iris es el rasgo biométrico que hará único al ciudadano en el sistema. La foto será de color blanco y negro debido al bajo costo del tamaño en bytes.
- La categoría de domicilio del ciudadano presenta la dirección física del ciudadano que contiene la credencial para votar.

- La categoría de historial delictivo servirá para conocer los antecedentes penales de los ciudadanos y poder prevenir ataques.
- La categoría información del documento servirá para validar la veracidad de la identificación digital y evitar falsificaciones.

  En la tabla 1, se presentan los datos para la identificación digital de cada ciudadano.

Tabla 1 Estructura de la identificación digital.

Categoría	Componente	Tipo y Longitud	Requerido	Tamaño en Bytes
Identidad del ciudadano	Apellido P.	Alfabético (20)	SI	160
	Apellido M.	Alfabético (20)	SI	160
	Nombre	Alfabético (20)	SI	160
	Iris	N/A	SI	688
	Foto	JPG	SI	3747.84
	CURP	Alfanumérico (18)	SI	144
Domicilio del ciudadano	Calle	Alfanumérico (30)	SI	240
	Número exterior	Numérico (5)	SI	40
	Colonia	Alfanumérico (30)	SI	240
	Código Postal	Numérico (5)	SI	40
Historial delictivo	Antecedentes penales	Alfabético (2)	SI	16
	Fecha de solicitud	Alfanumérico (10)	SI	80
Información del documento	Expedición	Alfanumérico (10)	SI	80
	Vigencia	Alfanumérico (10)	SI	80
	ID del documento	Numérico (13)	SI	104
	Huella digital del emisor	Hexadecimal (32)	SI	256
Byte				6,235.84
KiloByte				**6.089**

Para poder hacer uso de la identificación digital, se ha definido la siguiente infraestructura. Se debe entender como infraestructura a cada componente necesario para utilizar la identificación digital. Los componentes principales que se han definido son:

- Centro de emisión: es la dependencia encargada de generar la identificación digital y entregar el documento al ciudadano.
- Centro de registro: es la dependencia encargada de recibir la documentación e información del ciudadano.

- Centro de validación: es la dependencia encargada de verificar la legitimidad de los documentos e información del ciudadano.
- Ciudadano: es el solicitante de la identificación digital y puede tener nacionalidad mexicana o extranjero con residencia legal en la República Mexicana.
- Terceros: dependencias gubernamentales o iniciativa privada que requiere información personal de ciudadanos mexicanos o extranjeros con residencia legal para crear una cuenta o vender un producto y/o servicio a través de un medio digital.
- Los componentes secundarios que se han definido son:
- Políticas: es el plan de acción para recibir, evaluar, dictaminar, y emitir la identificación digital de cada ciudadano. También, se incluyen las acciones a seguir para rechazar y cancelar una identificación digital. Adicionalmente, se presentan las acciones a seguir en caso de una incidencia. Se entiende por incidencia a toda aquella acción legal relacionada con la identificación digital.
- Leyes: son las normas jurídicas emitidas por el poder legislativo en México y son todas aquellas que se encuentren relacionadas con documentos o transacciones digitales. Por ejemplo, la ley de privacidad de datos personales en posesión de particulares [6].
- Host: es todo equipo de cómputo y software que se utilizará para recibir, evaluar, dictaminar, emitir, rechazar, y cancelar la identificación digital.
- Equipo de trabajo: son todas las personas que trabajarán para recibir, evaluar, dictaminar, emitir, rechazar, y cancelar la identificación digital.
- Red de comunicaciones: es todo el equipo de comunicaciones que se utilizará para interconectar a los Host hacia el interior y exterior.

A continuación, se explica cada uno de los componentes principales.

- Centro de emisión: es el encargado de generar y entregar la identificación digital al ciudadano. La generación involucra el proceso de la firma digital

que vincula los datos del ciudadano con el centro de emisión. El centro de emisión tendrá la siguiente jerarquía (figura 1).

- Principal: es el centro de emisión nacional que mantiene la información actualizada de los centros de emisión de segundo nivel.
- Segundo nivel: es el centro de emisión local que se encuentra accesible a los ciudadanos. Existirá un centro de emisión de segundo nivel por localidad. Su función es entregar la identificación digital a los ciudadanos.

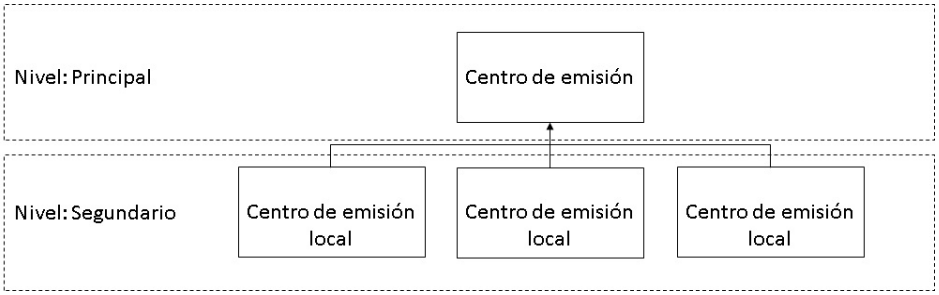

Figura 1 Jerarquía del centro de emisión.

- Centro de registro: se encuentra constituido por todas las oficinas del INE, y tienen por misión realizar las funciones de asistencia al centro de emisión local en los procedimientos y trámites relacionados con los ciudadanos para su identificación, registro, y validación de documentos para garantizar la correcta expedición de la identificación digital. En el supuesto que, una localidad no cuenta con oficinas del INE, se utilizara una unidad móvil para realizar la identificación, registro, y validación de documentos.

  En lo particular, los ciudadanos menores de edad que deseen obtener su identificación digital deberán realizar el procedimiento a través de la Secretaría de Educación Pública de su estado. La Secretaría de Educación Pública se limitará a validar la información y no emitirá bajo ninguna circunstancia la identificación digital.
- Centro de validación: tiene como función comprobar el estado e información de la identificación digital para ciudadanos mexicanos y extranjeros con documentos en regla. El protocolo para la validación de la información se

desarrollará posteriormente debido a que no es la finalidad del presente documento proponer un protocolo de intercambio de información. La función principal es garantizar que la información sea correcta y no afecte la reputación de un ciudadano, y en el caso de realizar actividades ilegales se procederá a proporcionar la información personal a las autoridades.

Se tiene contemplado tener varios centros de validación distribuidos en el interior de la República Mexicana para no saturar un servidor y balancear la carga de peticiones, incrementado la disponibilidad del servicio de consulta a terceros. La figura 2 presenta un escenario en donde un tercero desea validar la información de un ciudadano. El tercero tiene la opción de elegir entre tres centros de validación. En el caso que ocurra una falla con el primer centro de validación, se puede proceder con el segundo centro de validación, y así sucesivamente.

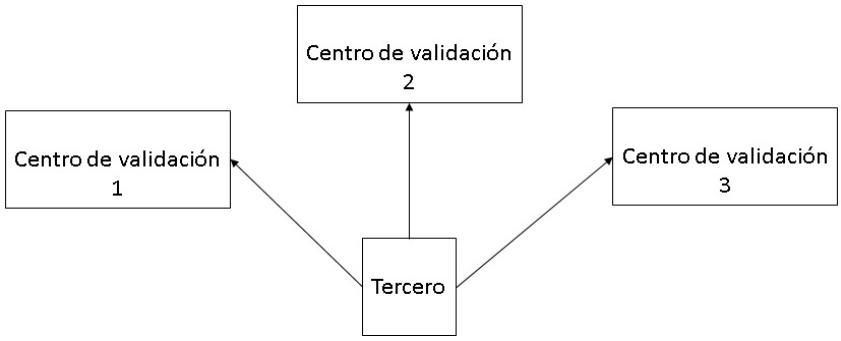

Figura 2 Escenario de validación de información por un tercero.

- Ciudadano: en el ámbito de la identificación digital, se entiende como ciudadano a toda persona física con nacionalidad mexicana o extranjero con residencia legal en México que por su propia voluntad solicita su identificación digital. El ciudadano debe mostrar documentos que lo relacionen con sus datos personales.

  En lo particular, los ciudadanos menores de edad deberán ir acompañados de un responsable legal y ambos deberán acudir por su propia voluntad para solicitar la identificación digital. Así mismo, se deberán presentar documentos personales de ambos.

- Terceros: en el ámbito de la identificación digital, se entiende como tercero a toda persona física o moral y dependencia gubernamental que solicita datos personales a ciudadanos mexicanos o extranjeros con residencia legal en México para crear una cuenta de usuario en un sistema web o móvil y/o para realizar una transacción comercial a través de medios digitales.

A continuación, se describen los procesos de registro y usabilidad de la identificación digital.

El proceso de registro sirve para que un ciudadano obtenga su identificación digital (figura 3).

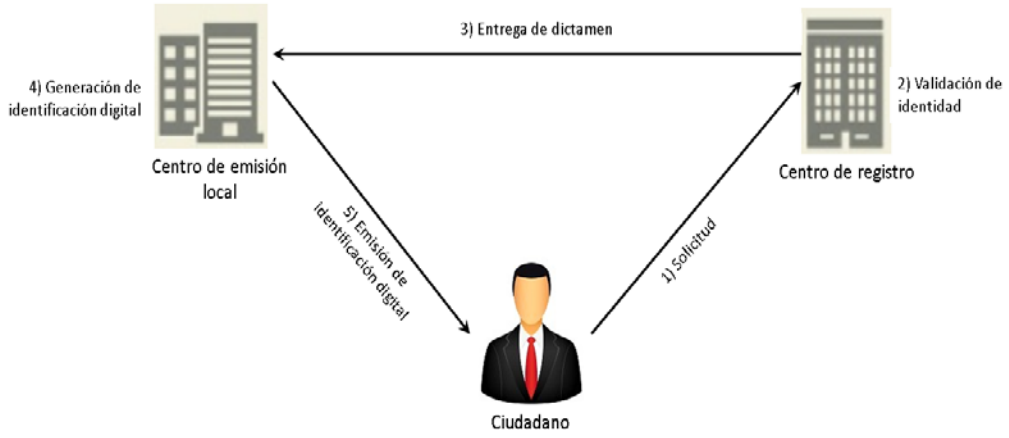

Figura 3 Proceso para obtener la identificación digital.

El ciudadano debe acudir físicamente al centro de registro más cercano a su domicilio con la documentación probatoria sobre su identidad (paso 1). El grupo de trabajo del centro de registro recibirá la documentación y procederá a validarla (paso 2). En caso que el proceso de validación sea positivo, se procederá a escanear el iris del ciudadano para generar la plantilla. Una vez generada la plantilla y verificada su funcionalidad, se procederá a emitir una solicitud de generación que será enviado al centro de emisión local (paso 3). El centro de emisión local se encargará de generar la identificación digital en base a la información proporcionada por el centro de registro (paso 4). Una vez concluida la generación de la identificación digital, se procederá a firmar digitalmente dicho

documento, y en caso de ser necesario, se procederá a cifrar la identificación digital con la clave pública del centro de evaluación. Finalmente, se entrega la identificación digital al ciudadano de manera física (paso 5).

Es importante mencionar que, se tiene contemplado agendar cita para asistir a solicitar y entregar la identificación digital.

El proceso propuesto para que un ciudadano pueda crear una cuenta de usuario en un sitio de red social o un sistema web, se presenta en la figura 4.

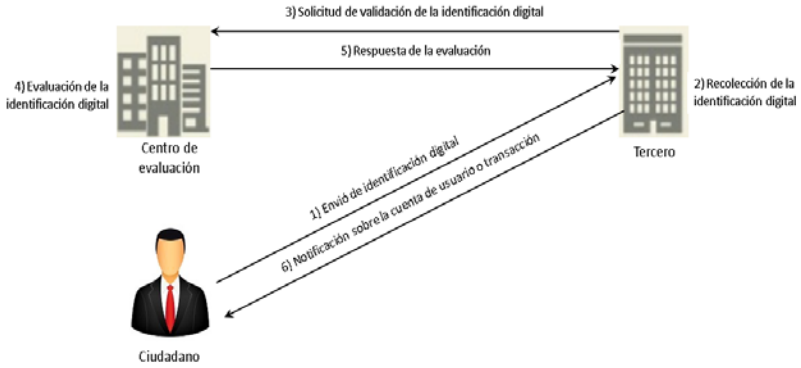

Figura 4 Proceso para crear una cuenta en una red social o en un sistema web.

El ciudadano debe utilizar un equipo de cómputo o un dispositivo móvil y conexión a Internet para crear una cuenta de usuario o realizar una transacción electrónica. En ese momento, el Tercero le solicitará su información personal para crear la cuenta de usuario o realizar la transacción comercial. El ciudadano enviará su identificación digital al tercero a través de un canal de comunicación seguro que se puede establecer utilizando el protocolo SSL y certificados digitales (paso 1). Una vez recibida la identificación digital, el tercero procederá a almacenar la identificación digital (paso 2). Una vez almacenada, se enviará la petición de validación al centro de validación a través de un canal de comunicación seguro (paso 3). El centro de validación tendrá que evaluar la validez de la identificación digital por medio de la verificación de la firma digital (paso 4). El resultado de la evaluación será enviado al tercero (paso 5). En caso de recibir un resultado positivo, el tercero generará la cuenta de usuario o continuará con la transacción comercial. Finalmente, el resultado será notificado al ciudadano (paso 6).

La seguridad de la identificación digital e infraestructura se encuentra dada por:

Protocolos criptográficos que permiten asegurar un canal de comunicación abierto, como es Internet, mantener la confidencialidad de información y evitar el repudio. Se tienen dos escenarios para establecer un canal de comunicación seguro. El primer escenario, se refiere al uso del chip criptográfico para almacenar la identificación digital y el canal de comunicación se debe establecer desde el chip criptográfico hasta el servidor web remoto [7]. El segundo escenario, se refiere al uso de la identificación digital en una memoria USB y el canal de comunicación se debe establecer desde el navegador web del usuario hasta el servidor web remoto.

La diferencia entre los escenarios se debe al uso del chip criptográfico. El chip criptográfico tiene la capacidad de calcular operaciones criptográficas y su acceso es restringido por un número de identificación personal (NIP). Por lo tanto, se puede calcular protocolos criptográficos como son Diffie-Hellman [8], RSA [9] y funciones hash [10], con sus recursos propios, incrementando la seguridad. Por el contrario, la memoria USB carece de dichas características, y por lo tanto, se debe utilizar los recursos de la computadora y del navegador Web.

El canal de comunicación se puede establecer por medio de un protocolo Diffie-Hellman o SSL. En donde, se establece una clave de sesión para cifrar los paquetes.

También, se recuerda que en el escenario de la memoria USB, la identificación digital deberá estar cifrada con RSA 2048 bits. El resultado es mantener la confidencialidad de la información del ciudadano en caso de robo o extravío.

La representación sería:

$$C = (Identidad\ Digital)^e (mod\ n)$$

Donde *C* es la identificación digital cifrada, *e* y *n* es la dupla que conforma la clave pública del centro de emisión

En el supuesto que, el ciudadano pierda su memoria USB y otro ciudadano desee conocer la información almacenada en la identificación digital, se verá frustrado debido a no poder descifrar *C* sin conocer la clave privada (*d*) del emisor.

También, se utiliza la firma digital en la identificación digital para verificar su originalidad y validez. La firma digital permite verificar la validez de los datos

almacenados en la identificación digital, debido a que, se realiza por el centro de emisión.

La representación está dada por la ecuación 1.

$$FD = \left(H(Identificación\ Digital)\right)^{d}(mod\ n) \tag{1}$$

Donde:

- *H* Resumen de la identificación digital a través de una función hash SHA-2 o MD5
- *FD* Firma digital de la identificación digital
- *d y n* Dupla que conforma la clave privada del centro de emisión

A través de la firma digital, el centro de validación podrá verificar que la información personal del ciudadano es válida. En caso de que algún usuario malicioso decida realizar el ataque de robo de identidad y generar su propia identificación digital, el centro de validación podrá reconocer el ataque cuando realice la verificación de la firma digital. El resultado será el rechazo de la identificación digital, y por consiguiente, la petición de crear una cuenta o realizar una transacción comercial será rechazada.

4. Evaluación de seguridad

Con la intención de explicar la seguridad de la infraestructura propuesta, se presenta una evaluación de seguridad.

La comunicación entre el ciudadano y el centro de registro se realizará de manera personal y con la documentación en regla. La documentación será verificada por el equipo de trabajo. En caso de encontrar alguna inconsistencia se rechazará la solicitud.

El rasgo biométrico permitirá identificar a un ciudadano con una taza de error menor que con la huella dactilar. La plantilla del rasgo biométrico será incluida en la identificación digital para poder verificar la identidad del ciudadano en cualquier momento. Además, la inclusión de un rasgo biométrico reducirá ataques de suplantación y robo de identidad. También, se espera reducir el préstamo de la

identificación digital a un atacante o para hacer acciones maliciosas debido a que la plantilla servirá para identificar al propietario de la identificación digital.

El registro y emisión de la identificación digital ha sido dividido en dos dependencias diferentes para evitar coacción y coerción para beneficiar a un ciudadano o grupo de ciudadanos; es decir, se busca reducir la corrupción.

El centro de emisión local se encarga de generar la identificación digital y el equipo de trabajo del centro de registro no conocerá, ni tendrá acceso a los host y/o políticas de seguridad. Se espera tener independencia entre ambos centros y reducir ataques desde el interior.

La identificación digital será almacenada en un chip criptográfico para proteger su integridad. También, se ha considerado el caso en donde la identificación digital se almacena en una memoria USB para su traslado y uso. La identificación digital será cifrada utilizando el algoritmo RSA con 2048 bits de longitud de clave.

La identificación digital será enviada a través de un canal de comunicación seguro establecido por el protocolo SSL o Diffie-Hellman.

La verificación de los datos almacenados en la identificación digital se realizará por medio del centro de validación. Esto significa que, el tercero no tendrá la responsabilidad de verificar los datos y se delegará la responsabilidad a un centro de validación. La validación se realizará utilizando la firma digital.

Los centros de validación serán distribuidos para que cada tercero puedo decidir con cual centro de validación confiar y establecer la comunicación. De esta manera, se podrá dar la oportunidad a los terceros de elegir el o los centros de validación más cercanos o de mayor confianza.

5. Conclusiones

La suplantación de identidad es un problema que puede afectar a cualquier ciudadano, y por lo tanto, nadie se encuentra exento. Inicialmente, el problema se extendió del mundo real al mundo virtual debido a la facilidad que se tiene para crear una cuenta de usuario y poder realizar diferentes acciones. Sin embargo, se ha detectado que la información personal proporcionada en los sitios de redes sociales es suficiente para robar su identidad y suplantar a una persona.

Con la intención de proponer una solución al problema, se ha introducido la primera identificación digital cuya finalidad es contener información verificable de un ciudadano mexicano. Además, se han definido los componentes de una infraestructura que pueda soportar el uso de la identificación digital a través del ciberespacio. La infraestructura cuenta con tres centros entre el que se encuentra el centro de validación. El centro de validación es el encargado de verificar la validez de la identificación digital y del contenido. Por medio de la identificación digital, se pueden crear cuentas de usuario con información real, incrementado la seguridad en sitios de redes sociales y en transacciones electrónicas.

6. Bibliografía y Referencias

[1] L. Rebollo Delgado, M. M. Serrano Pérez, Introducción a la protección de datos. 2008. DYKINSON, S.L. Madrid.

[2] A. Ramos Martín, M. J. Ramos Martín, Aplicaciones Web. 2014. Ediciones Paraninfo, S.A. Madrid.

[3] ITU-T, The Directory: Public-key and attribute certificate frameworks. IETF. 2005.

[4] A. Freier, P. Karlton, P. Kocher, The Secure Sockets Layer (SSL) Protocol Version 3.0. IETF. 2011.

[5] T. Dierks, C. Allen, The TLS Protocol Version 1.0. IETF. 1999.

[6] Cámara De Diputados Del H. Congreso De La Unión, Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación. 2010.

[7] A. Ali, K. Lu, M. Montgomery, “Network Smart Card - A new paradigm of secure online transactions”. 20th International Information Security Conference. 2005.

[8] W. Diffie, M. Hellman, “New directions in cryptography”. IEEE Transactions on Information Theory. Vol. 22. No 6. 1976. Pp. 644-654.

[9] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM. Vol. 21. Vo 2. 1978. Pp. 120-126.

[10] R. Rivest, The MD5 Message-Digest Algorithm. IETF. 1992.

7. Autores

Francisco Roger Cortes Martínez es egresado de la ingeniería de software de la Universidad Autónoma de Ciudad Juárez. Sus áreas de interés son desarrollo de software y seguridad informática.

Ángel Daniel Herrera Candelaria es egresado de la ingeniería de software de la Universidad Autónoma de Ciudad Juárez. Sus áreas de interés son desarrollo de software y seguridad informática.

Rafael Martínez Peláez es doctor por la Universidad Politécnica de Cataluña e ingeniero en sistemas computacionales por la Universidad del Valle de México en 2010 y 2003, respectivamente. Actualmente, es profesor investigador de tiempo completo en la Universidad de la Salle Bajío y miembro del Sistema Nacional de Investigadores (SNI.) con el nombramiento de candidato. Sus áreas de interés son autenticación, seguridad en servicios electrónicos, y privacidad en redes sociales.

Yesica Imelda Saavedra Benítez es doctora por la Universidad de Versalles e ingeniera en computación por el Instituto Tecnológico de Toluca en 2013 y 1997, respectivamente. Actualmente, es profesora de tiempo completo en el Instituto Tecnológico de Toluca y directora del laboratorio de investigación. Es miembro del Sistema Nacional de Investigadores (SNI) con el nombramiento de candidato. Sus áreas de interés son redes inalámbricas ad-hoc, redes de sensores y seguridad en redes inalámbricas.

Pablo Velarde Alvarado es doctor y maestro en ciencias por el Centro de Investigación y de Estudios Avanzado del IPN e ingeniero en electrónica por la Universidad Autónoma de Guadalajara en 2009, 2001 y 1993, respectivamente. Actualmente, es profesor investigador de tiempo completo en la Universidad Autónoma de Nayarit y miembro del cuerpo académico de nuevas tecnologías aplicadas a la educación. Es miembro del Sistema Nacional de Investigadores con el nombramiento de nivel I. Sus áreas de interés son sistemas de detección de intrusiones, entropía y seguridad en redes.