UNIVERSIDAD JUAN AGUSTÍN MAZA
FACULTAD DE CIENCIAS EMPRESARIALES
LICENCIATURA EN INFORMÁTICA

VOTO ELECTRÓNICO POR INTERNET

Autor: Fabio Escudero
Tutor disciplinar: Prof. Pablo Leiva
Tutora metodológica: Mgter. Cecilia Raschio

Mendoza, diciembre de 2013

A mi familia, que siempre confió en mí y me apoyó en todo momento

A todos los que hicieron posible este sueño

Gracias

RESUMEN

Antiguamente era impensado que el uso de la tecnología pudiera suplantar a procesos manuales como sucedió con el uso del correo electrónico o el reemplazo de los cajeros humanos por cajeros electrónicos. Pensamos que al igual que sucedió con estos procesos, llegará el momento en que el voto electrónico sea un opción habitual de emisión del sufragio.

En el marco de este trabajo analizamos los diferentes esquemas de seguridad utilizados en ámbitos de procesamiento remotos, como así también hacemos un recorrido por las experiencias realizadas en el mundo entero respecto de la votación electrónica.

Por otra parte se analiza el impacto de Internet en el mundo y en particular en Argentina que impulsa la realización de nuevos desarrollos basados en esta herramienta.

En este trabajo se propone un sistema de votación remota por Internet que satisface los requerimientos propios del proceso electoral y que a la vez hace uso de la tecnología disponible actualmente, la cual se utiliza en otros ámbitos como el bancario, para darle un marco de confiabilidad, transparencia y seguridad, garantizando además la libertad y privacidad de los votantes.

INDICE

INTRODUCCIÓN

Situación problemática

Los procesos de votación datan de hace más de 2500 años y han sido parte fundamental en los procesos democráticos de las sociedades, y constituye un derecho de los ciudadanos y en nuestro país también una obligación.

Por otra parte, en los últimos años hemos vivido la introducción cada vez más importante de las tecnologías de la información y las comunicaciones (TICs) en muchos ámbitos de nuestra vida, las cuales han afectado la vida social, familiar, las relaciones humanas, la educación, en resumen, cada espacio de nuestra cotidianeidad.

En este marco, Internet ha tenido un crecimiento exponencial y ha comenzado a participar cada vez más de actividades que normalmente se realizaban en forma personal: compras, pago de impuestos, trámites, transacciones comerciales, entre otras.

Sin embargo todavía, existe cierta desconfianza en el ciudadano común sobre la seguridad e integridad de la información transmitida por Internet debido a actividades como el hacking o los virus informáticos. Esto es una preocupación para los profesionales del área quienes continuamente investigan mecanismos que le brinden a la sociedad el grado de seguridad necesario dentro de un marco confiable.

En resumen, si disponemos de medios eficaces para realizar transacciones comerciales a través de Internet, las cuales involucran el movimiento de algo tan sensible como es el dinero, como no vamos a poder transpolar estas tecnologías para aplicarlas a la emisión y recuento de votos dentro de un sistema electoral digital.

En un sentido amplio, cuando hablamos de voto electrónico nos estamos refiriendo a la incorporación de recursos informáticos a cualquier parte del proceso electoral, pero a los fines de este trabajo vamos a considerar estrictamente dos áreas del mismo: la emisión del voto en sí misma y el recuento de dichos votos. Nos circunscribiremos a estos aspectos ya que

son los ámbitos donde Internet y las TICs en general pueden llegar a tener un impacto más significativo y donde se pueden percibir sus verdaderas ventajas.

El planteo es que dicho sistema no substituiría al actual proceso electoral, sino que lo complementaría ya que los votantes con acceso a la tecnología dispondrían de la posibilidad de realizar su voto en forma electrónica durante un período determinado (anterior a la fecha de la elección) y el día del comicio se realizaría normalmente en forma presencial para todo aquel que no haya podido realizarlo en forma virtual. De esta forma se contaría con las mejoras de la tecnología, pero sin excluir a aquellas personas que no tengan acceso a la misma o que su utilización resulte demasiado compleja.

Una de las principales ventajas de este proceso es que se podría realizar desde cualquier equipo conectado a Internet, independiente de la tecnología del dispositivo utilizado (PCs, notebooks, tablets, teléfonos inteligentes, entre otros) y de la plataforma utilizada (Windows, Linux, iOS, Mac OS, Android).

Desde el punto de vista legal será necesario analizar las leyes que rigen el proceso electoral en Argentina para determinar si se cumple con los requerimientos determinados en las mismas y las alternativas para conciliar el actual desarrollo del proceso con la inclusión de estas nuevas tecnologías.

Para que una democracia sea tal, los resultados de una elección deben representar la voluntad del pueblo, es por ello que aspectos como la precisión y la confiabilidad serán líneas rectoras de este trabajo.

Ahora bien, para automatizar un proceso tan importante y sensible es necesario contar con un proceso confiable de trabajo que brinde las garantías necesarias, por ello nos plantearemos una serie de preguntas de investigación y de objetivos.

Pregunta de investigación

El interrogante que guía la presente tesina es el siguiente:

¿Cómo implementar un sistema de voto electrónico por Internet que responda al marco legal argentino, que sea seguro y exacto y logre la aceptación de la gente?

Subpreguntas

¿Hay forma de ofrecer al votante la seguridad de que el voto se ha registrado tal cual ha sido emitido, o que el recuento es el correcto?

¿Se puede ofrecer un sistema que permita la fiscalización por parte de los partidos políticos tal como se realiza con la votación tradicional?

¿Se pueden implementar elementos de auditoría sin poner en riesgo la confidencialidad de los votos registrados?

¿Se puede transpolar un esquema de seguridad similar al utilizado en transacciones bancarias al de votación por Internet que le brinde la misma tranquilidad al votante que la conseguida por el mismo?

¿Se pueden disminuir las posibilidades de error a la hora de emitir el sufragio con un sistema de voto asistido gracias a un sistema informático?

¿Se puede facilitar la emisión del voto a personas con discapacidades gracias a la descentralización del proceso de votación?

Objetivo general

Desarrollar un sistema que permita emitir el voto por Internet, ajustado a los requerimientos del marco legal argentino y que garantice la seguridad y exactitud de los resultados para la sociedad en general.

Objetivos específicos

- Entender las implicaciones sociales, culturales y políticas del voto electrónico por Internet.

- Estudiar y comprender el marco cívico-legal de los comicios.
- Establecer los medios necesarios para que el sistema de votación planteado cumpla con los principios de universalidad, igualdad, libertad y secreto requeridos en todo proceso democrático.
- Lograr que el sistema aporte velocidad y facilite el proceso electoral.
- Desarrollar los parámetros de seguridad básicos que garanticen la transparencia del proceso, tanto en la emisión como en el recuento final de los votos.
- Plantear elementos de auditoría que permitan tanto al votante como a los agentes fiscalizadores poder comprobar la confiabilidad del sistema en cualquier momento del proceso.

Justificación de la investigación

Este trabajo se enmarca en la búsqueda de una plataforma teórica que permita la construcción de un sistema de votación por Internet, lo cual se trasparentaría en ventajas tangibles como: rapidez en la votación y en el escrutinio de los votos, accesibilidad para votantes con discapacidades físicas, prevención de errores en el sufragio, menores costos de implementación del proceso electoral y la conveniencia para el votante de no tener que desplazarse al lugar de votación.

La concepción de este proyecto no tiene como objetivo reemplazar al actual sistema de votación, sino complementarlo, obteniendo así las fortalezas del mismo, pero sin discriminar a aquellas personas que no tengan la posibilidad o los conocimientos necesarios para realizar dicho proceso a través de una computadora.

Es intención de esta tesina, sentar las bases para futuros desarrollos informáticos que permitan el proceso de voto electrónico por Internet, bajo la premisa de enmarcarlo en una metodología de código abierto, es decir que sea accesible a expertos que validen y realicen sus aportes logrando un sistema confiable, sólido y eficiente acorde a la importancia que tiene el proceso en todas las sociedades democráticas.

Estructura del trabajo

El trabajo está organizado en 5 capítulos, de los cuales los 4 primeros conforman el marco teórico y el restante corresponde al desarrollo de la propuesta.

En el primer capítulo, se realiza una breve reseña del surgimiento de Internet, su evolución hasta la situación actual y además, se analiza el contexto de Internet en Argentina.

En el segundo capítulo, se hace un análisis del sistema electoral en Argentina haciendo un repaso por su historia y el marco legal que lo regula, además se analiza el proceso electoral propiamente dicho y los pasos llevados a cabo en una elección típica.

En el tercer capítulo se hace un repaso de las experiencias llevadas a cabo en votación electrónica a través del mundo para luego llegar a analizar las experiencias en nuestro país.

En el cuarto capítulo se hace un análisis de la seguridad en Internet, teniendo en cuenta los tipos de ataques que se pueden sufrir en una comunicación a través de esta red de redes y de las formas de prever y solucionar dichos inconvenientes para darle confiabilidad a la misma. Se plantea además en este capítulo las bases que fundamentarán el esquema de seguridad que le da un marco de confianza al sistema propuesto.

Por último en el capítulo quinto se desarrolla el sistema propuesto, teniendo en cuenta primeramente los requisitos a cumplir por el mismo para luego verificar que los mismos se cumplan, luego se describe el sistema en detalle, el esquema de seguridad aplicado y las auditorías que se le pueden realizar al mismo para poder determinar la confiabilidad y exactitud del mismo. Por último se hace un repaso por las ventajas y desventajas de este sistema propuesto en comparación con el actual sistema de voto manual con boletas impresas.

MARCO TEÓRICO

CAPÍTULO I: INTERNET

I.a Historia y evolución

Hoy en día nos parece imposible prescindir de Internet y la usamos a diario, pero ¿qué es Internet? Según el diccionario de la Real Academia Española:

"*Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación.*"

También podemos citar una definición más técnica:

"*Internet es una red de computadoras que interconecta cientos de millones de dispositivos informáticos a lo largo de todo el mundo…Los sistemas terminales se conectan entre sí mediante una red de enlaces de comunicaciones y dispositivos de conmutación de paquetes.*" (Kurose & Ross, 2010)

Ahora, ¿qué es para una persona común? Básicamente es algo que vino a hacernos la vida más fácil, para ayudar a comunicarnos, para aprender, para expresarnos, para comprar y vender, para trabajar, y un largo etcétera. Cada día participa más de nuestra vida personal, familiar, social y laboral, proveyéndonos de grandes beneficios y a la vez presentándonos nuevos retos que nos obligan día a día a actualizarnos para poder acceder a los privilegios que esta otorga.

Originalmente nació para permitir la conexión entre universidades de Estados Unidos como respuesta a la necesidad de buscar maneras de optimizar el uso de las computadoras, ya que eran recursos muy escasos y costosos. De esta manera investigadores, científicos, profesores y estudiantes se vieron beneficiados de este nuevo medio de comunicación y de la posibilidad de hacer pública la información generada en sus actividades.

Hacia finales de 1969 estaba disponible la red precursora de Internet, llamada ARPAnet, formada por cuatro nodos. Hacia 1972 esta red había

crecido hasta 15 nodos y la primera demostración pública fue realizada por Robert Kahan en la International Conference on Computer Communications.

El número de dispositivos fue creciendo y llegó el momento de desarrollar una arquitectura que permitiera estandarizar la interconexión de estos elementos, así se acuñó el término interneting (interredes o interconexión de redes).

A finales de la década de 1970, había unos doscientos dispositivos conectados a la red ARPAnet. A finales de la década de 1980, este número llegaría a los cien mil. La década de 1980 fue una época de enorme crecimiento.

El 1 de enero de 1983 se llevó a cabo el lanzamiento oficial de TCP/IP como el nuevo protocolo estándar para ARPAnet.

La década de 1990 estuvo marcada por una serie de acontecimientos que simbolizaron la evolución y la llegada de la comercialización de Internet.

"*El principal acontecimiento de la década de 1990 fue la aparición de la Word Wide Web, que llevaría Internet a los hogares y negocios de millones de personas de todo el mundo. La Web sirvió como plataforma para posibilitar e implantar cientos de nuevas aplicaciones, que hoy damos por sentadas.*" (Kurose & Ross, 2010)

Hacia finales de 1993 estaban operativos aproximadamente doscientos servidores web, los cuales serían un presagio de lo que estaba por venir. Al mismo tiempo había varios investigadores que desarrollaron navegadores web que los estudiantes universitarios utilizaban diariamente, como Mosaic y Netscape. En 1996, Microsoft empezó a desarrollar navegadores y comenzaría la guerra con Netscape que ganaría unos pocos años después.

En el período comprendido entre 1995 y 2001 se produjeron varios altibajos para Internet en los mercados financieros. Antes que fueran incluso rentables, cientos de nuevas empresas de Internet fueron vendidas en el mercado bursátil valoradas en millones de dólares sin tener ingresos significativos. Las acciones de Internet se hundieron en 2001 y muchas de

estas empresas cerraron. No obstante, algunas de ellas emergieron como las grandes ganadoras en el espacio Internet, entre las que se incluyen Microsoft, Cisco, Yahoo, eBay, Google y Amazon.

Según un informe de AT&T Labs:

"*Durante la década de 1990, se estimó que el tráfico en la Internet pública creció un 100 por ciento por año, mientras que el crecimiento medio anual en el número de usuarios de Internet se pensaba que era entre 20% y 50%*"

Según cálculos de la Internet World Stats tomados al 31 de diciembre de 2011, se calcula que existen 2.267 billones de usuarios de Internet (32,7% de la población mundial). En el caso de Argentina, se calculan 28 millones de usuarios (que representan nada menos que el 67% de la población total).

Se suma a esto el hecho que cada vez tenemos más terminales para acceder a Internet, como televisores, teléfonos móviles, consolas de juegos, automóviles, dispositivos de seguridad, incluso electrodomésticos, lo que hace que se acerque cada día más a la vida cotidiana de las personas.

Con respecto a la información que circula por este medio de comunicación, según un artículo publicado en la revista Science en febrero de 2011 por Martin Hilbert y Priscila López, nos dice:

"*Se estima que en 1993 Internet transportaba sólo el 1% de la información que fluía a través de las telecomunicaciones, en el año 2000 esta cifra había aumentado a 51%, y en 2007 más del 97% de toda la información telecomunicada se transportó por Internet.*" (Science Magazine)

Se estima que en 1993 llevó a la Internet sólo el 1% de la información que fluye a través de las telecomunicaciones en ambos sentidos, en el año 2000 esta cifra había aumentado a 51%, y en 2007 más del 97% de toda la información telecomunicada se llevó a través de Internet según la Internet World Stats.

Es innegable el crecimiento de Internet y que es una tecnología inagotable, de la cual no se vislumbra un límite previsible, lo cual representa un espacio

muy propicio para la incorporación de nuevos servicios que estarán disponibles para toda persona que tenga un dispositivo con capacidad de conectarse a Internet.

I.b Tecnología de Internet

Para poder comunicar dos dispositivos a través de Internet es necesario que se establezcan normas comunes que permitan dicho diálogo, a dichas normas se las conoce con el nombre de protocolos.

“Básicamente, un protocolo es un acuerdo entre las partes en comunicación sobre cómo se debe llevar a cabo la misma.” (Tanenbaum, 2003)

“El protocolo define el formato y el orden de los mensajes intercambiados entre dos o más entidades que se comunican, así como las acciones tomadas en la transmisión y/o la recepción de un mensaje u otro suceso” (Kurose & Ross, 2010)

Entonces, un protocolo lo podríamos definir como un conjunto de reglas y mensajes que regulan el intercambio de información entre dos sistemas informáticos. Estos protocolos son la base de la infraestructura que permite el intercambio de información independiente de los sistemas en que ésta se encuentra almacenada.

Para reducir la complejidad de su diseño, la mayoría de las redes está organizada como una pila de capas o niveles. El número de capas, así como el nombre y función de cada una de ellas difieren de red a red.

Cada capa le pasa la información a la capa inmediatamente inferior, hasta que se alcanza la capa más baja. La última capa el medio físico a través del cual se produce la comunicación real.

El conjunto de protocolos que se utilizan en Internet se denomina TCP/IP en referencia a los dos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que son los más importantes.

Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra HTTP (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, el ARP (Address Resolution Protocol) para la resolución de direcciones, el FTP (File Transfer Protocol) para transferencia de archivos, y el SMTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol) para correo electrónico, TELNET para acceder a equipos remotos, entre otros.

El protocolo TCP/IP tiene cuatro capas de abstracción según se define en el Request for Comments 1122:

- Capa de aplicación: es donde residen las aplicaciones e incluye varios protocolos como los nombrados anteriormente (HTTP, FTP, POP, etc.).
- Capa de transporte (TCP): permite que la información generada en una máquina se entregue sin errores a cualquier otra conectada a la red.
- Capa de red (IP): se encarga de encaminar los datos hacia su destino eligiendo la ruta más efectiva.
- Capa de enlace: Controla el flujo de los datos, la sincronización y los errores que puedan producirse.

  Al conjunto de capas y protocolos se lo conoce como arquitectura de red.

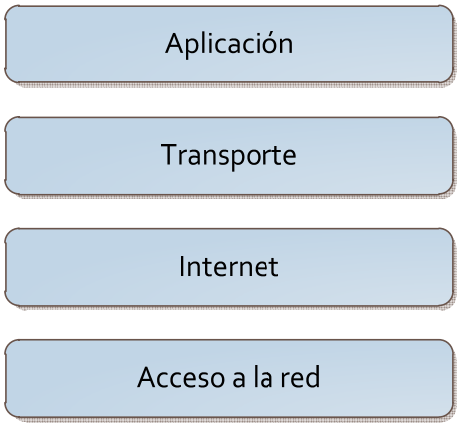


Figura 1: Capas de protocolo TCP/IP

Fuente: Tanenbaum, 2003

A principios de 1990 apareció una nueva aplicación en escena: la World Wide Web, que fue la primera aplicación de Internet que atrajo la atención del público en general.

Gran parte de su crecimiento durante la década de 1990 estuvo alimentado por empresas llamadas ISPs (proveedores de servicios de Internet) que ofrecen la capacidad de conectarse a Internet. Estas compañías suscribieron contratos con decenas de millones de usuarios nuevos por año durante el final de la década de 1990, cambiando por completo el carácter de la red de ser un campo para académicos y militares a uno de utilidad pública.

"Cambió de manera dramática, y continúa cambiando la forma en que las personas interactúan dentro y fuera de sus entornos de trabajo." (Kurose & Ross, 2010)

El protocolo de la capa de aplicación que se utiliza en la Web es el HTTP (HyperText Transfer Protocol) y se implementa en dos programas: uno cliente y otro servidor, como se determina en los documentos RFC 1945 y RFC 2616.

I.c Situación actual

El éxito actual de Web se debe por una parte a la facilidad con que se accede a la información y, por otra, a que cualquiera que esté conectado a Internet puede ser no sólo consumidor de información, sino que también puede convertirse en proveedor de la misma.

"Quizá lo que atrae a la mayoría de los usuarios es que la Web opera bajo demanda. Los usuarios reciben lo que desean y cuando lo desean." (Kurose & Ross, 2010)

Esto marcó una diferencia muy grande con respecto a los medios de comunicación del momento (radio, televisión, periódicos), ya que en los mismos el usuario sólo puede acceder a su contenido cuando el proveedor lo pone a disposición, además en dichos casos la comunicación es de una

sola vía ya que los usuarios no tienen más poder de decisión sobre los mismos que el que les da el hecho de poder cambiar de canal, de frecuencia o dejar de leer en el caso de los periódicos.

A medida que los usuarios se fueron involucrando cada vez más, permitieron el surgimiento de un nuevo paradigma en la navegación Web, esto es la Web 2.0.

El término Web 2.0 está ligado a la participación activa de los usuarios en la elaboración del contenido. Este término fue acuñado en el año 2004 en una tormenta de ideas llevada a cabo en la empresa O'Reilly Media.

“Una de las lecciones clave de la era de la Web 2.0 es la siguiente: Los usuarios añaden valor, se construyen sistemas que mejoran cuanta más gente los use.” (O'Reilly, 2005)

Otro gran avance que permitió esta nueva tecnología fue el aprovechamiento de la inteligencia colectiva tras un fin común, cuyo principal exponente es la enciclopedia libre y políglota: Wikipedia, que no solo se ganó su lugar en Internet sino que además dejó fuera de juego otros proyectos como la enciclopedia de Microsoft Encarta que se dejó de producir en octubre de 2009 como cita el portal ARS Technica en su página titulada “Microsoft to kill Encarta later this year.”

(http://arstechnica.com/microsoft/news/2009/03/microsoft-to-kill-encarta-later-this-year.ars, vista el 04/10/2012).

Anteriormente Internet era unidireccional, es decir, la información era más bien de corte informativo y no permitía la interacción directa con y entre los usuarios. Con la 2.0, se ha convertido en bidireccional y permite la interacción de todo tipo de contenido.

El uso de Internet genera muchos beneficios, ya que las personas pueden utilizar esta fuente de información para aprender, comunicarse y participar. Así como hace algunos años la televisión logró imponerse, hoy con Internet sucede lo mismo, y aunque su expansión no ha llegado a todos los hogares,

muchas personas tienen acceso a Internet desde distintos lugares como su casa, el trabajo, un cibercafé o la propia escuela.

El uso de Internet ofrece muchas ventajas, entre las cuales podemos citar:

- Facilita y expande las posibilidades de búsqueda de información.
- Establece una comunicación fluida y rápida con cualquier persona en cualquier lugar.
- Conecta a personas con los mismos intereses (a través de las redes sociales).
- Favorece el intercambio multicultural.
- Estimula la creatividad y promueve la investigación.
- Genera nuevos espacios de diálogo e intercambio.

Con respecto a la comunicación a través de Internet, podemos decir que sus características principales -y a su vez las que le brindan su mayor potencial- son:

- Multinivel: permite la comunicación interpersonal, grupal y masiva
- Multicrónica: permite la comunicación en tiempo real y diferido
- Desterritorializado: se rompen los vínculos territoriales, ya que las comunicaciones se producen a nivel mundial
- Hipertextual: el contenido tiene referencias cruzadas automáticas que permiten dirigirse a otra parte del documento o a un nuevo documento
- Hipermedial: los documentos no solamente están formados por texto, sino que pueden incluir video, audio, imágenes, animaciones u otros medios

Hoy en día los usos de esta red de redes son prácticamente ilimitados, y los avances se logran segundo a segundo, nombraremos algunos principales:

Correo electrónico: se puede redactar, enviar y recibir correo en cualquier momento y desde diversos dispositivos.

Acceso a la información: se puede acceder a información de todo tipo, desde noticias, capacitación, enciclopedias hasta música, películas y libros completos

Redes sociales: es una estructura social compuesta por un conjunto de individuos u organizaciones que están conectados teniendo en cuenta intereses comunes.

Transferencia de archivos: los usuarios pueden copiar y compartir archivos entre máquinas conectadas a Internet.

Teletrabajo: permite trabajar en forma no presencial, desde un lugar diferente a la oficina.

Trámites: muchas empresas y organismos públicos disponen de páginas desde donde ofrecen servicios que permiten la autogestión en diferentes tipos de gestiones

Con respecto a este último punto, vamos a hacer hincapié en el mismo ya que es un punto de partida para el tema a tratar en este estudio.

Las ventajas de realizar trámites a través de Internet son múltiples y variadas, entre las que podemos ver las siguientes:

- Se pueden realizar las 24 horas del día, los 365 días del año
- Permiten un ahorro de tiempo para los usuarios
- Promueven la transparencia, permitiendo a los usuarios conocer el estado de su trámite en todo momento a través de Internet
- Facilitan la rapidez de los trámites, ya que permite el pasaje rápido de los documentos entre las personas que deben trabajar sobre ellos
- Permiten un ahorro de dinero para las empresas que de esta forma prescinden del personal que debería realizar la recepción de dichos trámites
- Se suprimen las colas y la burocracia en las gestiones
- Se pueden realizar desde cualquier lugar del mundo

- Tienen cobertura legal, lo cual ha supuesto un paso muy importante en miras del presente trabajo
- Son seguros, incluso más que el papel ya que no es posible que se modifique o elimine información sin que quede un registro de quién realizó dicha transacción y cuándo la hizo, además de los medios de garantía de no alteración como puede ser la firma electrónica

En los últimos años han sido muchos los organismos estatales y privados que, preocupados por mejorar en eficiencia, optaron por implantar el trámite electrónico en su administración.

I.d Internet en Argentina

Las primeras computadoras se instalaron en Argentina a partir de 1960 y la primera carrera de grado, la de Computación Científica, comenzó a dictarse en 1963 en la Facultad de Ciencias Exactas y Naturales de la UBA (http://www-2.dc.uba.ar/futuros_estudiantes/contenidos.php?idi=8, vista el 02/11/12).

Pero recién en el año 1987, a través de la Cancillería, se realizan las primeras conexiones argentinas con Internet. En esa época no existían las interfaces gráficas ni siquiera la navegación en formato de texto.

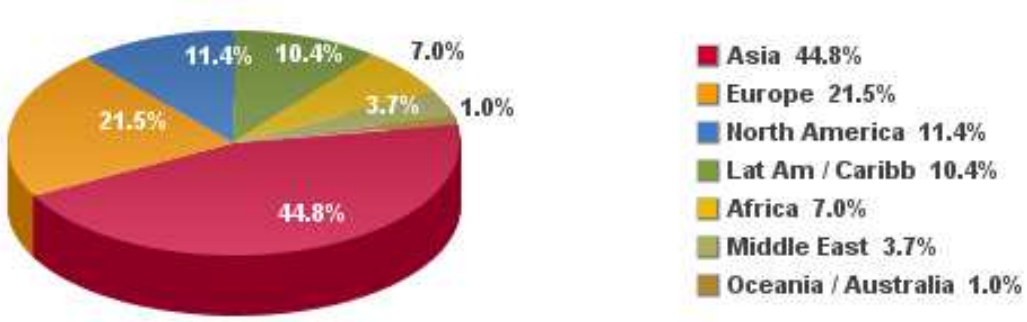
En 1988, la Secretaria de Ciencia y Técnica firma con ENTel un convenio por el cual la empresa de teléfonos cede el uso de un canal de datos para que las Universidades tuvieran correo electrónico. En ese momento, la Red Académica Nacional tenía más de 10,000 usuarios.

A principios de los 90, las Universidades de Buenos Aires, Córdoba y La Plata agregan enlaces propios en Internet, que se suman al que ya tenía la Secretaria de Ciencia y Técnica y el de Cancillería. Además se venden las primeras conexiones comerciales a Internet en Argentina. En pocos meses, miles de usuarios particulares y empresas argentinas navegan por una red que a nivel mundial reunía ya a 30 millones de personas.

Según la Internet World Stats (web que recopila estadísticas de uso de Internet a nivel mundial, incluyendo el número de usuarios en Internet para más de 265 países), el grado de penetración de Internet y tecnologías relacionadas a la fecha es la siguiente:

A nivel mundial:

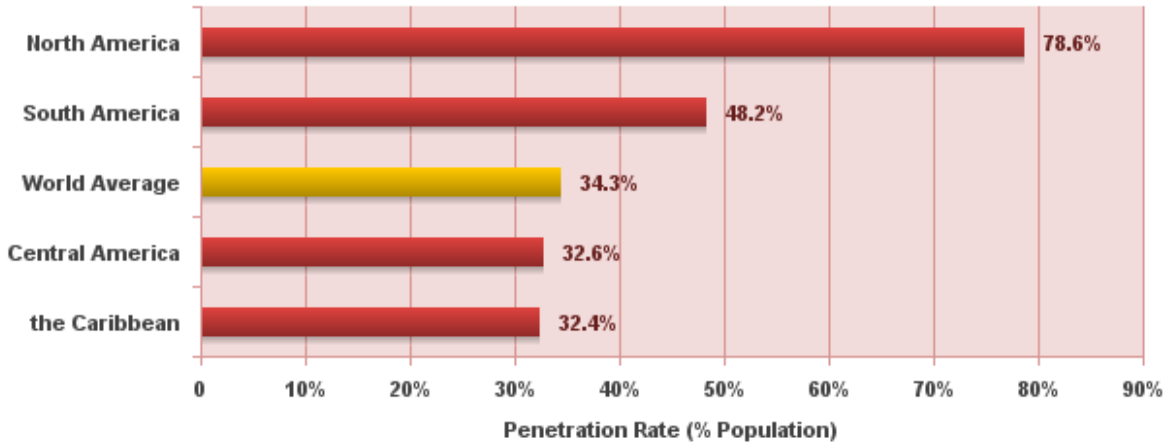
Gráfico N°1: Uso de Internet en el Mundo



Fuente: Internet World Stats, 2012

Las mismas estadísticas, pero en América:

Gráfico N°2: tasa de penetración de Internet en América



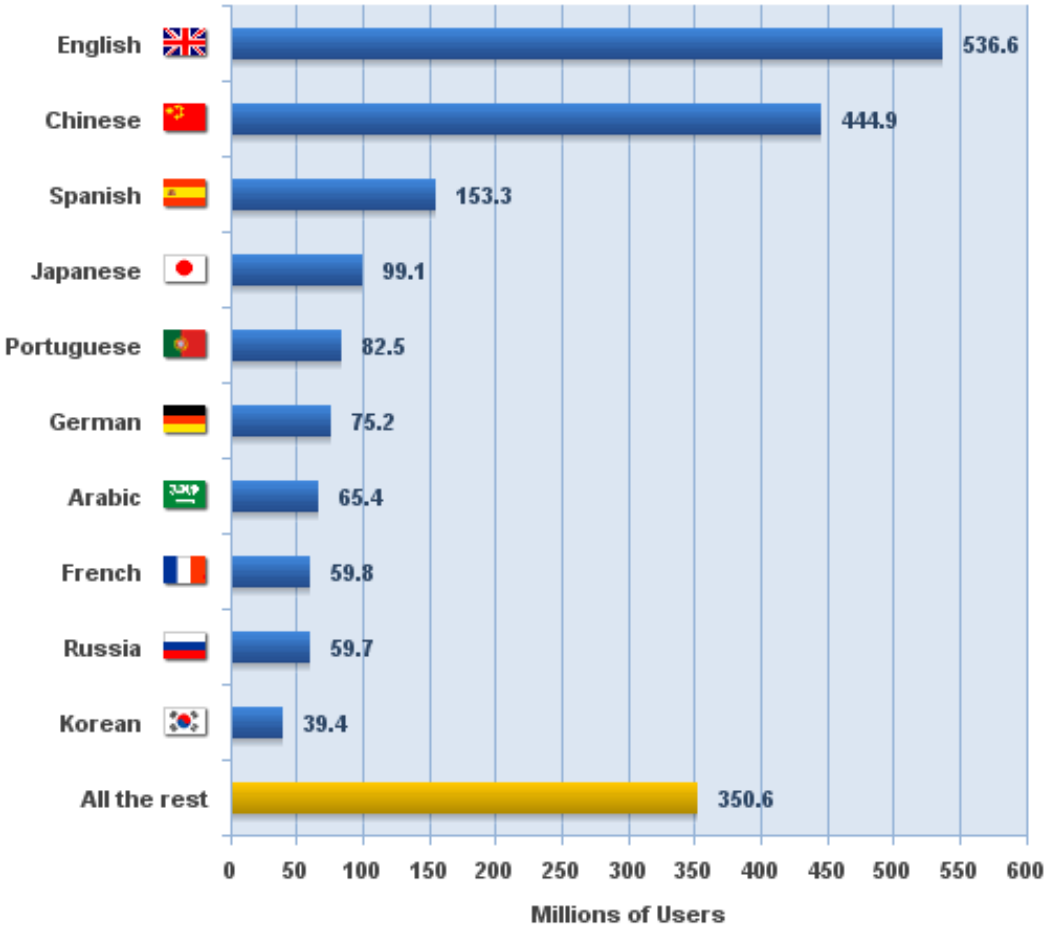
Fuente: Internet World Stats, 2012

Con respecto a América Latina, Argentina ocupa el tercer lugar en cuanto a cantidad de usuarios por habitantes, luego de Brasil y México. Con datos relevados a diciembre de 2011, se observa que en Argentina, tomando la

base de 42.192.494 habitantes, la penetración de Internet es del 67% (28.000.000 usuarios), con respecto a cantidad de celulares tenemos 137,2% (57.300.000 celulares subscriptos), y finalmente si vemos la cantidad de usuarios de Facebook veremos que estos representan un 45,1% (19.037.240 usuarios).

También es interesante destacar el grado de uso del lenguaje español en Internet, el cual ocupa el tercer lugar luego del inglés y el chino, con más de 153 millones de usuarios.

Gráfico N°3: Los 10 lenguajes más utilizados en Internet



Fuente: Internet World Stats, 2012

Si tenemos en cuenta los datos proporcionados por un organismo argentino y público como es el INDEC (Instituto Nacional de Estadística y Censos),

vemos que el 74% de las personas residentes en hogares urbanos del país utilizan celular, 58% emplean computadora y 54% usan Internet.

Además podemos ver que el 87% de las personas que asisten a un establecimiento educativo en el país utilizan una computadora y 83% de las mismas emplean Internet.

CAPÍTULO II: EL SISTEMA ELECTORAL

II.a Historia y evolución

Nuestro país, es uno de los primeros de América Latina en adoptar la modalidad del sufragio universal. Desde 1821, estaban habilitados a sufragar todos los ciudadanos de sexo masculino y mayores de veinte años de edad.

Actualmente las condiciones jurídicas del sufragio están constituidas por su universalidad, la igualdad, la obligatoriedad y el secreto. No obstante, para llegar a este punto, los condicionamientos y las formas de votar fueron modificándose a través de la historia Argentina, variando en función de la evolución de la vida democrática y de los sucesos en general de los acontecimientos mundiales en relación a la práctica democrática, en particular, de aquellos que conciernen a las prácticas democráticas de los países que se consideran, popularmente, evolucionados o del primer mundo.

Luego de dictada la Constitución Nacional, se sancionó el 16 de septiembre de 1857 la primera Ley Nacional de electores bajo el Nº 140. Como requisito para sufragar, los ciudadanos debían inscribirse en las “Juntas Calificadoras”, constituidas por funcionarios o en su defecto, por el párroco, o por una comisión de “vecinos notables”. La inscripción era obligatoria, pero no existió sanción formal de este requisito, hasta el año 1902, cuando es sancionada la ley 4161.

Para emitir el voto había que ser mayor de veintiún años, impidiendo la emisión del voto a todo aquel ciudadano que fuese sordo mudo y a los funcionarios eclesiásticos.

El elector votaba por una lista de candidatos y el mismo podía emitirse en forma verbal o por escrito y el acto duraba tres días.

Esta ley fue modificada por la ley Nº 207 del 1º de julio de 1859, que estableció en el país el sistema de lista completa y el voto público, pero no

obligatorio. Luego fue nuevamente modificada en el año 1863, donde se redujo el acto eleccionario a un sólo día y la edad mínima a 18 años.

Las elecciones se realizaban en sitios abiertos y públicos, donde la gente, reunida por los comités electorales arribaba por grupos, y el voto no era secreto. Luego apareció la modalidad de la compra de votos.

Todas estas maniobras ocurrieron entre 1874 y 1912, época durante la cual, el partido oficialista llamado Partido Autonomista Nacional (P.A.N) deseoso de mantenerse en el poder, lo lograba, mediante el fraude electoral.

En el año 1910 se produce un hecho muy importante para la historia electoral de la Argentina, se impone la fórmula presidencial de Roque Sáenz Peña, quien en su juramento frente al Congreso Nacional dice las siguientes palabras:

“Opino que debemos levantar un nuevo padrón electoral, para llamar a la acción a todos los ciudadanos, procurando que todos los partidos fiscalicen la legalidad de la inscripción. El padrón existente lo juzgo legal, pero no satisface a los partidos, ni guarda proporción con la población. Me será grato proponer al Congreso el proyecto que contenga la nueva inscripción y la reforma de la ley electoral”

Bajo la presidencia de Roque Sáenz Peña se dictó la ley 8871, conocida como Ley Sáenz Peña que impuso el voto secreto y obligatorio, para impedir el fraude y posibilitar que los electores votaran individualmente en un cuarto oscuro. Esta ley fue sancionada el 12 de febrero de 1912 y promulgada el 13 de febrero del mismo año.

Se consagró así el sistema de sufragio universal, aunque dentro de este sistema no se incluyó a las mujeres, quienes recién el 9 de septiembre de 1947, con la Ley 13010, lograron los mismos derechos políticos y las mismas obligaciones que los varones argentinos.

Se estableció que regiría para ellas la misma ley electoral que para el hombre y se previó que el Poder Ejecutivo de la Nación procedería a su empadronamiento y se les haría entrega de su libreta cívica como

documento de identidad indispensable para todos los actos cívicos y electorales.

II.b Marco legal actual

El sufragio comprende el derecho de elegir (sufragio activo) y el de ser elegido (sufragio pasivo). Este derecho, y la función pública de votar se encuentran contemplados en la Constitución Nacional (art. 37) y su ejercicio está reglamentado por el Código Electoral Nacional.

La autoridad responsable de los comicios nacionales es la Justicia Nacional Electoral, que integra el Poder Judicial de la Nación. También ejerce sus atribuciones respecto de las elecciones provinciales y municipales cuando se realizan en forma simultánea con aquéllos.

La reglamentación del proceso electoral está regido por la Ley 19.945 con modificaciones introducidas por las leyes n° 20.175, 22.838, 22.864, 23.247, 23.476, 24.012, 24.444, 24.904, 25.610, 25.658, 25.858, 25.983 y 26.215.

La Ley 19.945 está dividida en 8 capítulos, que enumeraremos a continuación:

I. Del Cuerpo Electoral
II. Divisiones Territoriales. Agrupación de Electores. Jueces y Juntas Electorales
III. De los actos preelectorales
IV. El acto electoral
V. Escrutinio
VI. Violación de la Ley Electoral: Penas y Régimen Procesal
VII. Sistema Electoral Nacional
VIII. Disposiciones Generales y Transitorias

A los fines de esta tesis ahondaremos en los capítulos I, IV y V, los cuales veremos en forma resumida a continuación.

En la primer parte analizamos el Título I de la ley, donde se aborda lo relativo a los electores, quiénes están incluidos en el padrón electoral y por lo tanto tienen la responsabilidad legal de emitir el sufragio (con la excepción de los que tengan 16 y 17 años, para los cuales el voto es optativo).

Además se declara aquí la característica del secreto del voto como así también la confección de los padrones electorales con la fecha de cierre de los mismos.

A continuación vemos los artículos más importantes de dicho capítulo.

TITULO I - Del cuerpo electoral

Art. 1º- Electores. Son electores nacionales los ciudadanos de ambos sexos, nativos, por opción y naturalizados, desde los dieciocho años cumplidos de edad, que no tengan ninguna de las inhabilitaciones previstas en esta ley.

(Nota: Por la Ley 26.774 promulgada en noviembre de 2012, los jóvenes de 16 y 17 años también podrán votar. A pesar de que se estableció la obligatoriedad del voto para los mismos, aquellos que no emitan su sufragio no sufrirán sanción alguna.)

Art. 2º- Prueba de esa condición. La calidad del elector se prueba, a los fines del sufragio, exclusivamente por su inclusión en el registro electoral.

Art. 10º Amparo del elector. El elector que se considere afectado en sus inmunidades, libertades o seguridad, o privado del ejercicio del sufragio podrá solicitar amparo por sí, o por intermedio de cualquier persona en su nombre, por escrito o verbalmente, denunciando el hecho al juez electoral o al magistrado más próximo o a cualquier funcionario nacional o provincial, quienes estarán obligados a adoptar urgentemente las medidas conducentes para hacer cesar el impedimento, si fuere ilegal o arbitrario.

Art. 13.- Secreto del voto. El elector tiene derecho a guardar el secreto del voto.

Art. 15.- Ficheros. A los fines de la formación y fiscalización del registro electoral, se organizarán y mantendrán al día permanentemente los siguientes ficheros:

1. *De electores de distrito;*
2. *Nacional de electores; y*
3. *De electores inhabilitados y excluidos.*

Art. 29.- Padrón definitivo. Las listas de electores depuradas constituirán el padrón electoral, que tendrá que hallarse impreso treinta días antes de la fecha de la elección de acuerdo con las reglas fijadas en el artículo 31.

A continuación analizaremos el Título IV de la ley, donde se detalla el procedimiento de constitución de las mesas electorales, la emisión del sufragio por los votantes habilitados y el cierre de dicho proceso.

También se hace hincapié en el secreto del voto durante todo el desarrollo del acto electoral y se detalla el proceso desde que la persona se acerca a la mesa a votar, hasta que emite el sufragio y se le da la constancia del mismo.

Por último se determina en qué momento y cómo se cierra el proceso eleccionario.

A continuación vemos los artículos más importantes de dicho capítulo.

TITULO IV – El acto electoral

Art. 77. Ubicación de las mesas. Los jueces electorales designarán con más de treinta días de anticipación a la fecha del comicio los lugares donde funcionarán las mesas. Para ubicarlas podrán habilitar dependencias ofíciales, locales de entidades de bien público, salas de espectáculos y otros que reúnan las condiciones indispensables.

Art. 81.- Constitución de las mesas el día del comicio. El día señalado para la elección por la convocatoria respectiva deberán encontrarse a las siete y

cuarenta y cinco horas, en el local en que haya de funcionar la mesa, el presidente y sus suplentes, el empleado de correos con los documentos y útiles que menciona el artículo 66 y los agentes de policía que las autoridades locales pondrán a las órdenes de las autoridades de comicio.

Art. 83. - Apertura del acto. Adoptadas todas estas medidas, a la hora ocho en punto el presidente declarará abierto el acto electoral y labrará el acta pertinente llenando los claros del formulario impreso en los padrones correspondientes a la mesa.

Art. 84. Procedimiento. Una vez abierto el acto los electores se apersonarán al presidente, por orden de llegada, exhibiendo su documento cívico.

1. *El presidente y sus suplentes, así como los fiscales acreditados ante la mesa y que estén inscriptos en la misma, serán, en su orden, los primeros en emitir el voto.*

2. *Si el presidente o sus suplentes no se hallan inscriptos en la mesa en que actúan, se agregará el nombre del votante en la hoja del registro haciéndolo constar, así como la mesa en que está registrado.*

3. *Los fiscales o autoridades de mesa que no estuviesen presentes al abrirse el acto sufragarán a medida que se incorporen a la misma.*

Art. 85. Carácter del voto, El secreto del voto es obligatorio durante todo el desarrollo del acto electoral, Ningún elector puede comparecer al recinto de la mesa exhibiendo de modo alguno la boleta del sufragio, ni formulando cualquier manifestación que importe violar tal secreto.

Art 86.- Dónde y cómo pueden votar los electores. Los electores podrán votar únicamente en la mesa receptora de votos en cuya lista figuren asentados y con el documento cívico habilitante. El presidente verificará si el ciudadano a quien pertenece el documento cívico figura en el padrón electoral de la mesa.

Art. 89. Verificación de la identidad del elector. Comprobado que el documento cívico presentado pertenece al mismo ciudadano que aparece

registrado como elector, el presidente procederá a verificar la identidad del compareciente con las indicaciones respectivas de dicho documento, oyendo sobre el punto a los fiscales de los partidos.

Art. 93. Entrega del sobre al elector. Si la identidad no es impugnada el presidente entregará al elector un sobre abierto y vacío, firmado en el acto de su puño y letra, y lo invitará a pasar al cuarto oscuro a encerrar su voto en aquél.

Art. 94. Emisión del voto. Introducido en el cuarto oscuro y cerrada exteriormente la puerta, el elector colocará en el sobre su boleta de sufragio y volverá inmediatamente a la mesa. El sobre cerrado será depositado por el elector en la urna.

Art. 95. Constancia de la emisión del voto. Acto continuo el presidente procederá a anotar en el padrón de electores de la mesa, a la vista de los fiscales y del elector mismo, la palabra "votó" en la columna respectiva del nombre del sufragante, La misma anotación fechada, sellada y firmada, se hará en su documento cívico, en el lugar expresamente destinado a ese efecto.

Art. 100. - Clausura de/ acto. El acto eleccionario finalizará a las dieciocho horas, en cuyo momento el presidente ordenará se clausure el acceso al comicio, pero continuará recibiendo el voto de los electores presentes que aguardan turno.

Por último analizaremos el Título V de la ley que se refiere a los procedimientos llevados a cabo una vez que concluyó el proceso electoral.

Se detalla principalmente la forma de realizar el recuento de los votos, y la elaboración de un acta de cierre una vez terminado dicho proceso.

Determina además el tiempo y forma de realizar reclamos sobre problemas que puedan haberse detectados tanto en la constitución como en el funcionamiento de las mesas electorales.

Se detalla además el esquema de seguridad que se lleva a cabo para brindarle confiabilidad al proceso.

A continuación vemos los artículos más importantes de dicho capítulo.

TITULO V – Escrutinio

Art. 101. Procedimiento. Calificación de los sufragios. Acto seguido el presidente del comicio, auxiliado por los suplentes, con vigilancia policial o militar en el acceso y ante la sola presencia de los fiscales acreditados, apoderados y candidatos que lo soliciten hará el escrutinio.

Art. 102.- Acta de escrutinio. Concluida la tarea del escrutinio se consignará, en acta impresa al dorso del padrón (artículo 83 "acta de cierre").

Art. 103. Guarda de boletas y documentos. Una vez suscripta el acta referida en el artículo anterior y los certificados de escrutinio que correspondan, se depositarán dentro de la urna: las boletas compiladas y ordenadas de acuerdo a los partidos a que pertenecen las mismas, los sobres utilizados y un "certificado de escrutinio".

Art. 104. Cierre de la urna y sobre especial. Seguidamente se procederá a cerrar la urna, colocándose una faja especial que tapará su boca o ranura, cubriéndose totalmente la tapa, frente y parte posterior, que asegurarán y firmarán el presidente, los suplentes y los fiscales que lo deseen.

Art. 110.- Reclamos y protestas. Plazo. Durante las cuarenta y ocho horas siguientes a la elección la Junta recibirá las protestas y reclamaciones que versaren sobre vicios en la constitución y funcionamiento de las mesas, Transcurrido ese lapso no se admitirá reclamación alguna.

Artículo 112. Procedimiento del escrutinio. Vencido el plazo del artículo 110, la Junta Electoral Nacional realizara el escrutinio definitivo, el que deberá quedar concluido en el menor tiempo posible.

II.c Principales procedimientos realizados en las votaciones

Un sistema electoral, es un conjunto de mecanismos, reglas y procedimientos mediante los cuales -a través de los votos de los ciudadanos- se determinan las preferencias políticas de los mismos y se establece la adjudicación de puestos legislativos o ejecutivos. Dentro de este proceso podemos destacar cuatro pasos fundamentales presentes en todo sistema electoral: la confección de padrones electorales, la oficialización de los candidatos, el proceso de votación propiamente dicho y el recuento final de votos.

Confección de los padrones electorales

El padrón electoral se conforma con las listas de electores registradas en las oficinas de Registro Civil de todo el país con las personas que cumplan 18 años de edad hasta el mismo día del comicio y deberá estar impreso 30 días antes de la fecha de la elección. Los ciudadanos podrán pedir, hasta 20 días antes del acto comicial, que se subsanen los errores y omisiones existentes en el padrón.

Las mesas electorales podrán contener hasta 450 electores inscriptos y con un mínimo de sesenta. Los fiscales podrán votar en las mesas en que actúen aunque no estén inscriptos en ellas, siempre que estén en la sección a que ellos pertenecen. En ese caso se agregará el nombre del votante en la hoja del Registro, haciendo constar dicha circunstancia y la mesa en que está inscripto. La designación del fiscal será comunicada hasta 24 horas antes del acto eleccionario.

Los presidentes y suplentes a quienes corresponda votar en una mesa diferente a aquella en que ejercen sus funciones podrán hacerlo en la que tienen a su cargo.

Oficialización de los candidatos

Desde la publicación de la convocatoria y hasta 50 días anteriores a la elección, los partidos registrarán ante el Juez Electoral la lista de los candidatos públicamente proclamados, quienes deberán reunir las

condiciones propias del cargo para la cual se postulan y no estar comprendidos en alguna de las inhabilidades legales.

En caso de muerte o renuncia de cualquiera de los candidatos de la fórmula a Presidente y Vicepresidente de la Nación, los partidos políticos o alianzas a los que pertenezcan, podrán registrar a otros en su lugar en el término de 7 días corridos.

Treinta días antes de la elección, los partidos políticos que hayan proclamado candidatos, deberán someter a aprobación los modelos exactos de las boletas de sufragio destinadas a ser utilizadas en los comicios.

Procedimiento de votación

El presidente de mesa procederá a recibir la urna, los registros, útiles y demás elementos que le entregue el empleado de correo. A las 8 en punto el presidente declarará abierto el acto electoral y labrará el acta pertinente llenando los claros en el formulario impreso en los padrones correspondientes a la mesa. Los electores podrán votar únicamente en la mesa receptora de votos en cuya lista figuren asentados y con el documento cívico habilitante. El presidente verificará si el ciudadano a quien pertenece el documento cívico figura en el padrón electoral de la mesa y que posea un documento igual o más nuevo del que aparece en el padrón.

Todo aquel que figure en el padrón electoral y exhiba su documento cívico tiene derecho a votar y nadie podrá cuestionarlo en el acto de sufragio. Los presidentes no aceptarán impugnación alguna que se funde en la inhabilidad del ciudadano para figurar en el padrón electoral. Se podrá impugnar la identidad del elector cuando a juicio de las personas éste hubiere falseado su identidad.

Finalizada la elección del ciudadano, el presidente de mesa procederá a anotar en el padrón de electores de la mesa, a la vista de los fiscales y del elector mismo, la palabra ”votó” en la columna respectiva del nombre del sufragante. La misma anotación, fechada, firmada y sellada, se hará en su documento cívico en el lugar expresamente destinado a ese efecto.

El acto eleccionario finalizará a las 18 horas, en cuyo caso el presidente ordenará que se clausure el acceso pero continuará recibiendo los votos de

los electores presentes que aguardan turno. Concluida la recepción de estos sufragios, tachará del padrón los nombres de los electores que no hayan comparecido y hará constar al pie el número de los sufragantes y las protestas que hubieren formulado los fiscales.

La iniciación de las tareas de escrutinio de mesa no podrá tener lugar, bajo ningún pretexto, antes de las 18 horas, aun cuando hubiera sufragado la totalidad de los electores.

Concluida la tarea del escrutinio se consignará en acta impresa la hora de cierre, el número de sufragios emitidos, cantidad de votos impugnados, diferencia entre las cifras de votos escrutados y los votantes señalados en el registro de electores. Cantidad de los sufragios logrados por cada uno de los respectivos partidos y en cada una de las categorías de cargos. El número de votos nulos, recurridos y en blanco, el nombre del presidente, los suplentes y fiscales que actuaron en la mesa.

Contabilización de los votos

El recuento de votos (o escrutinio) es un proceso manual que se realiza con el objetivo de determinar los votos totales contabilizados por cada candidato. Este proceso se divide a su vez en tres etapas sucesivas:

- Conteo voto por voto de cada urna en la mesa
- Escrutinio provisorio de los telegramas
- Escrutinio definitivo

Conteo en cada mesa

Finalizada la elección, la mesa electoral se cierra y el presidente de la misma y los fiscales de cada partido que controlan la mesa, se reúnen a solas para proceder al conteo de cada voto.

En este recuento la única autoridad es el presidente de mesa, que es quien decide si algún voto debe ser declarado nulo o en blanco. Los fiscales no pueden tomar decisiones, y sólo pueden impugnar ciertos votos o recurrir decisiones del presidente de mesa, sobre votos concretos.

Finalizado el conteo de todos los votos, los resultados se colocan en un acta, que firma el presidente de la mesa y los fiscales de los partidos

políticos presentes. Debido a que la firma del fiscal implica la aceptación por parte del partido político del contenido del acta, en adelante no se podrán cuestionar ni impugnar votos o cuestiones que no hayan sido planteadas por los fiscales en cada mesa.

Las papeletas se colocan en la urna con una copia del acta, la urna se cierra con una faja firmada por el presidente y los fiscales, y se envían, la urna y el acta, al centro de cómputos para que se proceda al escrutinio definitivo.

La urna es usualmente trasladada por autoridades públicas neutrales acompañadas por fiscales de los partidos, con el fin de controlar que las mismas no sean reemplazadas o afectadas en ningún sentido.

Simultáneamente el presidente de mesa realiza un telegrama con los resultados volcados en el acta, el que es enviado inmediatamente al centro de cómputos para que se proceda al escrutinio provisorio.

Escrutinio provisorio

Debido a la demora que implica enviar todas las urnas y actas originales a un único centro de cómputos para que se proceda a al conteo, usualmente se realiza un escrutinio provisorio, que consiste en efectuar el conteo con los telegramas con los resultados de cada urna enviados por los presidentes de mesa.

El escrutinio provisorio no computa como votos positivos, ni a los votos impugnados ni a los votos recurridos, cuya validez recién va a ser decidida en el escrutinio definitivo.

El escrutinio provisorio carece de valor legal y prácticamente nunca coincide exactamente con el resultado final establecido por el escrutinio definitivo.

Escrutinio definitivo

El escrutinio definitivo es el único que tiene validez legal y se realiza bajo la autoridad de un juez electoral neutral. Comienza a realizarse usualmente algunos días después de finalizado el escrutinio provisorio y puede durar días o semanas, según la complejidad de la elección que se escruta.

En principio el escrutinio definitivo consiste en contar todos los resultados volcados en todas las actas confeccionadas en las mesas electorales. Sin

embargo, también corresponde al escrutinio definitivo verificar si las propias actas son válidas, y resolver sobre los votos impugnados y recurridos que los diferentes partidos políticos puedan haber realizado en cada mesa y que consten en las actas.

En caso de que las actas no sean consideradas válidas o existan impugnaciones por parte de algún partido político, el juez electoral puede ordenar que la urna correspondiente sea abierta, para resolver la cuestión. En casos extremos puede también ordenar una elección complementaria limitada a los ciudadanos incluidos en la mesa invalidada.

Las decisiones del juez electoral, pueden ser apeladas por los partidos políticos que se sienten afectados, como en cualquier otro caso del sistema judicial.

Una vez realizado el escrutinio definitivo y agotadas todas las apelaciones que pudieran haber realizado los partidos políticos, se confecciona el resultado definitivo, único legalmente válido, y la atribución de los cargos a los candidatos victoriosos.

CAPÍTULO III: EXPERIENCIAS EN VOTACIÓN ELECTRÓNICA

III.a Antecedentes a nivel mundial

Hoy día es común que en las noticias sobre el desarrollo de procesos electorales aparezca el término voto electrónico. El uso de este término se remonta a 1964 cuando, por primera vez, se emplearon computadoras en EEUU para realizar ciertas funciones ligadas al proceso electoral. Desde entonces, este término viene empleándose para identificar sistemas de votación de naturaleza muy diversa. A continuación se mencionan algunas de las experiencias de voto más recientes o relevantes que han empleado computadoras en alguna fase del proceso electoral.

Estados Unidos

EEUU es uno de los países que más experiencia ha acumulado en torno al voto electrónico. El caso de este país, por su extensión y organización federal, es significativo por la gran variedad de métodos electrónicos que existen (registro electrónico directo, máquinas de palanca de votar, tarjetas perforadas, lectores ópticos, etc.) y por las numerosas irregularidades producidas y los problemas detectados en los sistemas electrónicos fabricados por algunas empresas.

En el año 1975 el Congreso de los Estados Unidos crea la Comisión Electoral Federal (FEC) compuesta por un grupo de expertos que debía emitir regularmente una serie de documentos con instrucciones y criterios para implementar y seleccionar los dispositivos electrónicos (Voting System Standards). De tal manera se establece un marco general que deben seguir los diferentes Estados al elegir los instrumentos de votación electrónica.

En este país hay una gran multiplicidad de medios para el recuento automático de votos. En las elecciones presidenciales de 2000 solamente el 1,5% de los electores votaron con las boletas habituales. El 12,5% lo hizo con el registro electrónico directo (DRE); el 29,5% usó lectores ópticos; el 17% usó las máquinas con palancas de votar y el 31% tarjetas perforadas, el resto utilizó otro sistema de votación.

En 2005 se presentó en el Congreso de los Estados Unidos una nueva ley de votación denominada “Voting Integrity and Verification Act” (VIVA) que pretendía hacer obligatoria la impresión de un comprobante del voto para permitir a los electores que votaran con máquinas electrónicas pudieran verificar e incluso corregir, si fuera necesario, su voto, de forma que el mismo quedara en poder de las autoridades para posibles recuentos manuales

En octubre de 2008, los ciudadanos americanos residentes en el extranjero pudieron votar por Internet para elegir al presidente de Estados Unidos. Esta fue la primera vez que los votantes ausentes registrados en el estado de Florida y que residían en Alemania, Reino Unido y Japón pudieron ejercer su derecho al voto a través de este medio. Estas personas no fueron las únicas, los astronautas estadounidenses votaron también desde el espacio, a través de un novedoso sistema de votos electrónicos y autorizados por una ley aprobada en el Parlamento de Texas en 1997.

En las elecciones presidenciales de Estados Unidos de 2012, en varios estados (Alabama, Arkansas, Misuri, Nueva York, Alaska y Virginia Occidental) se pudo ejercer el derecho al voto por internet, a través de la empresa española SCYTL.

Bélgica

Bélgica es el país pionero en la aplicación de sistemas de voto electrónico en Europa. La justificación de la utilización de este tipo de sistemas residía en los días de retraso que se producían tras el escrutinio manual en el complejo sistema de votación belga.

El método utilizado y regulado por ley del 11 de Abril de 1994 es el presencial con la utilización de una papeleta electrónica con banda magnética, en la que los datos se graban a través de una pantalla en la que aparecen las opciones y un lápiz óptico para su selección. Posteriormente, el votante introduce la tarjeta en una urna electrónica que computa automáticamente los resultados.

Este mecanismo se fue trasladando al territorio belga de manera progresiva principalmente debido a los costos que suponía la sustitución en todo el estado del sistema tradicional por el electrónico.

En las elecciones europeas y regionales de junio de 2009, se utilizó el sistema de voto electrónico en 200 municipios, lo que supone un 44% del número total de votantes.

Holanda

La utilización del voto electrónico en Holanda se remite a la legislación de votación de 1965, que permite el uso de un sistema de tablero electrónico con pantalla no táctil para la realización del proceso de voto.

Desde entonces, han tenido lugar numerosas experiencias entre las que destacan las elecciones de 2002, en las que el 95% de los municipios holandeses disponían de máquinas de voto electrónico, y las elecciones europeas de 2004, en las que los ciudadanos en el extranjero en el día de votación pudieron ejercer el voto a través de Internet o por teléfono celular.

En el año 2006 se realiza un estudio llevado adelante por un grupo de investigadores que determinó graves fallos de seguridad en el método empleado. Como consecuencia del mismo en mayo de 2008 el Gobierno holandés anunció oficialmente el abandono del sistema de voto electrónico, ya que no se daban las condiciones mínimas de seguridad, anonimato y fiabilidad esperadas y necesarias, volviendo nuevamente el sistema de tradicional.

Francia

En mayo de 2005 Francia pone en marcha un proyecto piloto de votación electrónica a través de un sistema de pantalla táctil. La experiencia tuvo lugar en 13 municipios franceses, que fueron equipados con máquinas electrónicas y que recibieron una subvención el gobierno para su compra o alquiler.

Posteriormente, en las elecciones presidenciales de 2007, el 3% del total de los votantes franceses participó en una prueba piloto de voto electrónico. La implementación de este sistema se produjo en 82 municipios, todos ellos de más de 3.500 habitantes. Dotadas de doce botones, uno por cada candidato a la presidencia, más uno destinado al voto en blanco, los sistemas de registro contabilizaron los votos sin que quedase ninguna constancia física de los mismos.

La actuación suscitó polémica ya que la mayoría de los partidos políticos se opusieron a su utilización al considerarlo un riesgo innecesario.

Estonia

Estonia es otro de los países pioneros del sufragio por Internet. En 2005, se probó por primera vez el voto por Internet en las elecciones municipales y posteriormente se utilizó en las elecciones Parlamentarias de 2007, convirtiéndose así en el primer país del mundo en permitir esta modalidad de voto online.

Para el voto por Internet, los votantes disponen de una tarjeta de identificación (similar al DNI electrónico) que insertan en un lector conectado a su computadora accediendo a un portal web seguro, donde realizan su elección tras introducir dos contraseñas.

En 2008, después de modificar la ley electoral, implantaron el voto por Internet a través del teléfono celular. Para votar a través del mismo, la tarjeta SIM sirve para identificarse y se necesita activar la identificación móvil en la web de la Policía de Estonia.

Inglaterra

En el año 2002 el gobierno británico realiza pruebas piloto en 17 municipios durante las elecciones locales, y el año siguiente hizo una nueva apuesta y para llevar adelante los comicios se permitió utilizar Internet, televisión interactiva y SMS. Este sistema fue probado en más de 30 distritos. Los

resultados de estas experiencias mostraron que cuanto más fácil es la utilización de los sistemas implementados, los ciudadanos participan más a gusto y en mayor proporción; aunque persisten las preocupaciones vinculadas a cuestiones tales como la seguridad y vulnerabilidad del sistema.

Brasil

Este país aprobó en octubre de 1995 la Ley Electoral que marca las directrices del voto electrónico con la intención de eliminar el fraude electoral y reducir el tiempo de escrutinio. El proceso de votación se lleva a cabo a través de una especie de cajero automático, dotado de un monitor, en el que van apareciendo los candidatos y donde los votantes pueden realizar su selección oprimiendo un botón. Al finalizar la jornada electoral, se bloquea la urna mediante una clave y automáticamente se imprime una copia de los resultados, a la vez que se obtiene una copia digital que se lleva de inmediato a un Centro de Recuento para su cómputo. La urna electrónica fue el único método de votación en las elecciones a presidente en octubre de 2002, donde 115 millones de votantes lo emplearon.

De acuerdo con la evaluación realizada por el Juez José Paulo Sepúlveda Pertence, presidente del Tribunal Superior Electoral de Brasil, “La experiencia brasileña ha sido altamente positiva”. Se mantuvieron dos elecciones con la totalidad del electorado usando urnas electrónicas (las municipales del año 2000 y las federales y estatales de 2002). En los últimos comicios, dice Sepúlveda Pertence, se obtuvieron resultados absolutamente confiables, y se notó una disminución del 50% de los votos nulos, con un aumento de la asistencia electoral y sin ninguna impugnación consistente. Lo mismo sucedió en los comicios municipales: se votó en 5.600 municipios y “los resultados fueron magníficos, muchas veces decididos por una docena de votos de diferencia”.

En las elecciones municipales de octubre de 2008, se utilizaron urnas biométricas en algunas ciudades, con lo que los electores no necesitaron de

ningún documento de identidad ya que la verificación de identidad se realizó mediante la huella digital.

Venezuela

Este país ha incluido en su Reglamento General Electoral las instrucciones para que el proceso de votación y publicación de resultados del proceso se realicen en forma automática. A diferencia del caso de Brasil este Reglamento no especifica el funcionamiento de ninguna máquina de voto en particular.

En las Elecciones Municipales del año 2000 se confió a una empresa española la automatización del proceso de votación. Con este sistema, el elector emite el voto en la urna electrónica y automáticamente se acumula para su recuento y difusión sin intervención humana. Este proceso tiene como característica singular que es auditable por empresas y organizaciones externas al proceso electoral. Sin embargo, las primeras implantaciones de voto electrónico en los procesos electorales venezolanos no han sido muy afortunadas y se han presentado muchos problemas, básicamente motivados por la desconfianza hacia los resultados obtenidos.

En las elecciones del año 2004, se utilizaron máquinas con pantalla touchscreen que imprimen el voto en un papel térmico, lo que permitiría auditar el proceso de votación.

El ticket impreso posee un código seguridad además de los principales datos del evento: tipo de elecciones, código que corresponde al centro de votación, mesa y tomo. El código de seguridad es esencial para evitar la falsificación del voto. Esta impresión es colocada por el elector en una urna. Una vez finalizado el día electoral el presidente de mesa cierra la misma y la maquina imprimirá el acta de dicha mesa.

Luego de esta impresión, la información final acumulada por cada máquina se transmite vía telefónica o en forma satelital encriptada con clave pública y privada de 128 bits al centro de consolidación de datos.

Paraguay

Con la reforma constitucional acaecida en Paraguay en 1992, se creó un Tribunal Superior Electoral que tuvo la facultad de introducir –de manera gradual- la votación electrónica. Según explica el doctor José María Cabral, decano de la Facultad de Derecho de la Universidad Católica de Asunción este proceso se realizó de manera progresiva, primero en elecciones municipales, de manera parcial, y luego en elecciones generales, donde usaron tecnologías de voto electrónico prácticamente la mitad del electorado.

Esta implementación se hizo gracias a acuerdos de cooperación firmados con Brasil (que proveyó las urnas) y la OEA (que se encargó de la asistencia técnica y las auditorias). También intervino EE.UU. financiando parte del proyecto.

El uso más amplio fue en las elecciones presidenciales de abril del 2003. En las mismas se habilitaron 3.780 mesas con urnas electrónicas, donde votaron 748.020 personas. Al considerarse las cifras de votantes habilitados se determina que la participación en las mesas electrónicas llegó al 67,86%, mientras que en las mesas comunes fue del 64,28%.

III.b Experiencias Argentinas

Tierra del Fuego

Según explica el doctor Horacio Maffei, Juez Electoral y de Registro de la provincia de Tierra del Fuego el primer paso se dio en 1994, cuando se decide digitalizar el padrón provincial. Este fue generado sobre la base del padrón federal pero luego continuó su actualización de manera independiente.

El segundo paso se dio en las elecciones de 1999, cuando en cada centro de votación se instaló una PC en red, conectada al centro de cómputos. A través de estas, y mediante un programa desarrollado por los profesionales del Centro de Informática del Poder Judicial de la Provincia, una vez terminado el escrutinio provisorio y antes de cerrar el acta, se volcaban los

resultados en la PC que realizaba una verificación de la coherencia inicial de las sumas. Si ésta era correcta, la misma emitía un ticket que luego se enviaba junto con las actas y los votos, para el escrutinio definitivo. Según Maffei, este sistema de transmisión contribuyó muchísimo a evitar los problemas y errores que plagaban la tradicional opción manual.

Finalmente, se implementó el voto electrónico en la elección provincial municipal, realizada en la ciudad de Ushuaia en el año 2003. El sistema fue provisto por la empresa española Indra (www.indracompany.com, visto el 11/07/2013). Vale destacar que del padrón provincial de 72.500 electores, en esa oportunidad votó cerca del 68%.

Se utilizaron 105 urnas electrónicas y 25 impresoras. Si bien el proyecto original no contemplaba el uso de impresoras, se tuvieron que incorporar debido a los reclamos públicos para que hubiera algún tipo de comprobante en papel. Se decidió utilizar el ticket que emite la urna, pero siempre cuidando que no fuera posible relacionar un voto concreto con determinado votante, para respetar el principio del secreto del voto.

Es importante destacar que cuando se realizaron las verificaciones en estas urnas “control” contra los correspondientes votos en papel, se vio que los resultados eran absolutamente fieles, y los veedores de los partidos políticos participantes decidieron -de común acuerdo- dar por válida la verificación.

Para evitar eventuales fraudes, los equipos técnicos del juzgado con competencia electoral tuvieron acceso al software que usa el sistema de Indra, incluso se puso a disposición el código para cualquier experto propuesto por los partidos políticos interesados en revisarlo (hecho que fue efectivamente realizado).

Como parte de los preparativos de esta votación, una semana antes de los comicios se realizó un simulacro completo, con los apoderados partidarios presentes. Y el día anterior a la contienda electoral se hizo una nueva prueba piloto con 10 máquinas e impresoras elegidas al azar.

Entre las conclusiones de esta experiencia Maffei destaca que “la gente pide seguir votando así, especialmente las personas mayores que vieron facilitado su voto porque la urna mostraba fotos de los candidatos y sólo tenía que usar el dedo para elegirlos”.

Por otra parte, la velocidad de la obtención de resultados también fue buena: en una hora se logró cerrar el escrutinio provisorio, y tener todos los resultados.

De acuerdo con la experiencia recogida por Horacio Maffei, los argumentos de quienes estaban en contra de la prueba (básicamente los partidos políticos) se resumían en los siguientes:

- No se había probado previamente en el país el sistema a utilizar.
- Los opositores preferían hacer pequeñas pruebas pilotos antes de realizar una experiencia general.
- Imaginaban que la gente más humilde iba a tener problemas con el uso del sistema.
- Lo mismo para la gente mayor.

Para contrarrestar estos inconvenientes y alcanzar una buena implementación del voto electrónico los organizadores de los comicios realizaron campañas de divulgación a través de todos los medios de comunicación (diarios, radio y televisión).

A esto se le sumó un equipo que llevó las urnas electrónicas a diferentes lugares de alta concentración de público (Shoppings, hospitales, Casa de Gobierno, etc.) y allí se realizaron demostraciones completas. Esto incluyó trasladar los equipos a centros de jubilados y otros lugares relacionados con los adultos mayores.

Buenos Aires

La provincia de Buenos Aires comenzó a manejar el proyecto de voto electrónico a principios de marzo del 2003, a partir de un convenio firmado con el gobierno de Brasil. “Este país aportó su know-how y sus urnas para

poder armar la experiencia piloto que se realizó empleando la solución brasileña", según explicó el licenciado Vicente Fasano, responsable de Informática de la Junta Electoral de la Provincia de Buenos Aires. Luego de un puñado de meses de desarrollo, se implementó una prueba piloto durante las elecciones realizadas en septiembre de ese año. La misma tuvo lugar en la 7ma sección electoral, que se ubica geográficamente en el centro de la provincia. Para su realización se tuvo que modificar la Ley Electoral de la Provincia.

Finalmente la experiencia se concretó incluyendo sólo a los electores extranjeros de dicha sección. El total considerado era de unos 5.000 electores, de los cuales terminaron votando cerca de 1.000. Vale destacar que se votaron cargos reales y los votos electrónicamente emitidos fueron debidamente contabilizados.

La decisión de optar por la 7ma sección fue simple, según Fasano y es útil tomar en cuenta los argumentos a la hora de considerar las posibles locaciones de futuras pruebas piloto: se trata de una sección compuesta por pocos distritos, y que no registran una violenta disputa electoral, tal como suele ocurrir en las secciones mayores.

Para transmitir los datos de cada urna electrónica al centro de consolidación de datos, asegurando la integridad de la información y disminuyendo la posibilidad de hackeos, se utilizaron líneas conmutadas punto a punto, pero sólo se identificaron los números a utilizar 24 horas antes de los comicios. De todos modos, la información viajaba por las redes públicas de manera encriptada y se realizaba a su llegada una verificación de integridad por medio de una firma digital.

Se utilizaron 36 urnas electrónicas de origen brasileño y la evaluación final resultó más que satisfactoria. Según Fasano, apenas 17 minutos después del cierre del acto eleccionario ya se contaba con resultados de un distrito ubicado a 200 kilómetros de la ciudad de La Plata. Y a 38 minutos de la conclusión, se tenía lista la información completa de la sección electoral.

Otras característica que resaltó esta experiencia es que la urna electrónica facilitó el corte de boleta, lo que –en definitiva- debería ayudar a mejorar la calidad de la representatividad política. Aunque las boletas tenían 4 cuerpos, las evaluaciones estadísticas mostraron que el elector tardaba entre 30 segundos y dos minutos en emitir su voto (con un promedio general de un minuto treinta segundos por elector). Vale considerar que los participantes eran extranjeros y el 60% mayores de 50 años.

Salta

En las elecciones legislativas de 2013 Salta será la primera provincia en aplicar el voto electrónico para el 100% del padrón electoral. El proceso gradual comenzó en 2009 cuando se sufragó con el sistema electrónico en 36 mesas de Capital y de la ciudad de San Lorenzo. El uso de este sistema se profundizó en las elecciones provinciales de 2011, cuando el 33% del padrón usó esta modalidad.

Para concretar este objetivo se puso en marcha el Plan Provincial de Reforma Electoral y 100% voto electrónico, que se aplicará hasta mediados de 2013 para difundir las características del sistema y preparar a todos sus actores.

La boleta única electrónica es una síntesis de los sistemas electorales que se están aplicando en el país. Se trata de un sistema que brinda seguridad e inmediatez para el procesamiento de los resultados. Las boletas fueron evolucionando y mejorando gracias a que el sistema que se utiliza en Salta no es cerrado, sino que permite introducir las modificaciones que se crean necesarias para el elector, el universo político y el concepto de transparencia.

La primera vez se que se usó fue en una interna del PJ, en julio de 2009. Luego en el referéndum en Nazareno que se realizó el domingo 8 de agosto de 2010. En este caso hubo 585 votantes.

La tercera implementación se realizó en las internas de la juventud peronista que se hicieron en noviembre de 2010, en 12 mesas habilitadas en Capital,

San Lorenzo, San José de Metán, Cafayate y San Ramón de la Nueva Orán.

Además en las últimas elecciones generales de abril de 2011, este sistema fue empleado por el 33% del padrón electoral de la provincia. Se habilitaron 725 mesas de las cuales 430 fueron en Capital y San Lorenzo. El resto en el interior, en Orán, Metán, La Caldera y Cafayate.

El sistema también fue empleado en la última elección de la Junta de Calificadora de Méritos y Disciplina.

El proceso se realizó en conjunto con el Tribunal Electoral, siempre con miras a la meta de que en octubre y noviembre de 2013 se pueda implementar el voto electrónico al 100% del padrón salteño.

Mendoza

En el año 2005 la provincia de Mendoza llevó a cabo dos experiencias piloto de votación electrónica. El motivo principal de estos ensayos fue generar pruebas, establecer contactos con proveedores y provocar un efecto demostrativo “para acercar esta tecnología a la gente y que los electores le vayan tomando confianza a los sistemas eVoto”, sostuvo Claudio Romano, secretario Administrativo, Legal y Técnico de la Gobernación. Para ambos sondeos se eligió hacer una elección abierta y de participación voluntaria.

La primera prueba se hizo en el mes de marzo, durante la Fiesta de la Vendimia y la segunda durante junio, para la elección de la Reina de la Nieve. En la experiencia de la Vendimia el proveedor fue la cooperativa Telpin (Cooperativa Telefónica de Pinamar) y en la votación participaron 1.732 personas.

Para esta primera consulta electrónica a los mendocinos se les mostraban en la pantalla fotos de cada participante.

Se utilizaron diez mesas conectadas por medio de una red inalámbrica (ocho fijas y dos móviles), ubicadas en diferentes puntos de la ciudad y durante tres días los ciudadanos votaron sin dificultades.

En el informe final, elaborado por el proveedor, puede leerse que el 70% de los votantes no solicitó ayuda y se desempeñó sin problemas. El 96% valoró el sistema como “fácil”, el 3% como “medianamente fácil” y sólo un 1% lo consideró “difícil”.

Los jóvenes se manifestaron más familiarizados con la tecnología, aunque hubo excelente predisposición de los mayores para aprender y participar. El 29% de los votantes tenían entre 18 y 30 años; el 49%, entre 31 y 50 años, y el 22%, más de 50 años.

Un 20% evaluó al sistema opinando que era fácil de usar, práctico, ordenado o seguro. Un 6% lo catalogó como más rápido, ágil y menos burocrático que el sistema tradicional. En tanto que el 6% del total declararon que no les gustó la experiencia, tuvieron algún tipo de problema o solicitaron mayor información.

Esta información está disponible en la web del proveedor de dicha tecnología: www.telpin.com.ar/interneteducativa/webeleccion/mendoza.htm, visto el 16/07/2013.

En la segunda práctica la participación fue mayor, llegando a 5.022 electores y el responsable técnico fue la empresa española Indra.

En este ensayo se colocaron urnas electrónicas en prácticamente todos los departamentos que integran la provincia, y se tomó especial cuidado en analizar lo que ocurría en regiones en las que los potenciales votantes no hubieran tenido contacto previo con tecnologías informáticas.

En ambas oportunidades los sistemas probados contemplaron los diferentes tipos de discapacidades físicas, que no constituyeron un problema ya que prevén respuestas específicas. De todos modos, al igual que ahora ocurre con el sistema tradicional de papeles, una autoridad de mesa puede orientar al elector discapacitado.

También se definió que los proveedores interesados en participar de esta experiencia deberían aportar previamente el código del software a utilizar para que fuera revisado por parte de los técnicos de la provincia.

Según Élida Rodríguez (licenciada en Educación, coordinadora de la Unidad de Reforma y Modernización del Estado de Gobierno de la provincia y responsable del diseño e implementación del Plan Provincial "Hacia el Gobierno Digital"), luego de las pruebas el equipo técnico hizo encuestas de satisfacción y evaluación. En ambos casos se preguntó al elector si el sistema le parecía fácil o difícil de usar. Y el 99% lo calificó como “fácil”.

Otra pregunta fue ¿Preferiría usted usar sistemas de voto electrónico en las próximas elecciones políticas? Nuevamente un 97% respondió que sí.

El 17 de julio de 2013 el gobernador de la provincia de Salta, Juan Manuel Urtubey presentó el sistema de voto electrónico en la localidad de Maipú, junto a su par Francisco Pérez. El mandatario salteño indicó que Salta será la primer provincia en la que la totalidad del padrón votará en forma electrónica este año. Destacó, además, la fiabilidad, transparencia y rapidez del sistema.

“Lo que se está buscando con este nuevo sistema es romper con el proceso de manipulación, avanzar en la confianza, rapidez, transparencia, igualdad y la inclusión de generación en generación; eso para nosotros es uno de los temas centrales”, explicó Urtubey.

Los encargados de cumplir con la experiencia mendocina destacan algunos hechos que brindan detalles importantes a tomar en cuenta a la hora de diagramar futuras experiencias exitosas:

“Nosotros detectamos una barrera que tiene que ver con la `contaminación´ de la idea del voto electrónico”, resume Romano. “Paradójicamente, a la hora de usar estos instrumentos, quienes están más lejos de las TICs demuestran menos desconfianza y prejuicios que los propios profesionales dedicados a la informática”. Esa resistencia cultural no tiene tanto que ver con niveles socioeconómicos sino con las deformaciones profesionales.

Por otra parte, concluye que tomando en cuenta el descontento que los ciudadanos expresan hoy contra su sistema político, parecería una necesidad –tal vez temporal- que sea cual sea el tipo de voto electrónico a

implementar en lo inmediato cuente con algún tipo de respaldo en papel que permita auditorias posteriores.

Y un último aporte de la experiencia mendocina reconoce que los procesos de implementación de votación electrónica suelen estar desorganizados. Y por lo tanto “es una muy buena idea empezar usando las TICs con los subprocesos de la elección, como por ejemplo digitalizar el padrón, cuidar la logística, estudiar la capacitación previa de las autoridades de mesa, entre otros aspectos".

CAPÍTULO IV: SEGURIDAD EN INTERNET

IV.a Requisitos de seguridad y tipos de ataques

Como indica William Stallings al referirse a este tema, para entender los tipos de amenazas a la seguridad que existen, necesitamos partir de una definición de los requisitos de seguridad. La seguridad en computadoras y en redes implica cuatro requisitos:

- Privacidad: se requiere que sólo entidades autorizadas puedan tener un acceso a la información.
- Integridad: se requiere que los datos sean modificados solamente por partes autorizadas.
- Disponibilidad: se requiere que los datos estén disponibles para las partes autorizadas.
- Autenticidad: se requiere que una computadora o servicio sea capaz de verificar la identidad de un usuario.

A su vez, Tanenbaum hace referencia a los problemas que nos podemos encontrar cuando nos referimos a la seguridad en las redes, y los divide -en términos generales- en cuatro áreas interrelacionadas: confidencialidad, autenticación, no repudio y control de integridad.

- Confidencialidad: consiste en mantener la información fuera de las manos de usuarios no autorizados.
- Autenticación: se encarga de determinar con quién se está hablando antes de revelar información delicada.
- El no repudio: se encarga de las firmas de los mensajes y de que el emisor del mismo no pueda negar haber enviado un dato habiéndolo hecho o que el receptor no niegue haberlo recibido.
- Control de integridad: hace referencia a la forma de asegurar el mensaje enviado para que nadie lo modificó en el camino

Una forma útil de clasificar los ataques a la seguridad se especifican en el RFC 2828 (http://www.ietf.org/rfc/rfc2828.txt, visto el 20/07/2013) que los divide en términos de ataques pasivos y ataques activos. Un ataque pasivo intenta averiguar o hacer uso de información del sistema, pero sin afectar a los recursos del mismo. Un ataque activo intenta alterar los recursos del sistema o influir en su funcionamiento.

Ataque pasivo: Los ataques pasivos consisten en escuchas o monitorizaciones de las transmisiones. La divulgación del contenido de un mensaje y el análisis de tráfico constituyen dos tipos de ataques pasivos. Los ataques pasivos son muy difíciles de detectar, ya que no suponen la alteración de los datos. Normalmente, el tráfico de mensajes es enviado y recibido de forma aparentemente normal y ni el emisor ni el receptor son conscientes de que un tercero haya leído los mensajes u observado el tráfico de información.

Ataque activo: Los ataques activos suponen alguna modificación del flujo de datos o la creación de flujos falsos. Los podemos clasificar en 4 categorías:

- Enmascaramiento: tiene lugar cuando una entidad pretende ser otra entidad diferente.
- Retransmisión: supone la captura de datos y su retransmisión posterior para producir un efecto no autorizado.
- Modificación de mensajes: algún fragmento de un mensaje legítimo se modifica, se retrasa o se reordena para producir un efecto no autorizado.
- Denegación de servicio: se impide o inhibe el normal uso o gestión de los servicios de comunicación. Puede suprimir todos los mensajes dirigidos a un destino concreto o logar la interrupción de un servidor o de toda una red, bien deshabilitando el mismo o sobrecargándolo con mensajes con objeto de degradar su rendimiento.

IV.b Tipos de ataques más comunes

En los primeros años los ataques involucraban poca sofisticación técnica, generalmente eran empleados disconformes de las organizaciones que utilizaban sus permisos para alterar archivos o registros, o personas que atacaban desde fuera de la ubicación física de la organización, pero simplemente se introducían a la red averiguando alguna contraseña válida.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataques para aprovecharse de debilidades de diseño, configuración y operación de los sistemas informáticos. Esto permitió a los atacantes tomar el control de sistemas completos, produciendo verdaderos inconvenientes en las organizaciones.

A continuación se detallarán los tipos de ataques más comunes que podemos encontrar en sistemas comunicados a través de redes, como es el caso de Internet.

Packet sniffing

Hace referencia a la captura pasiva del tráfico de red, que se realiza gracias a programas llamados sniffers que monitorizan la información que circula por la red. Esto puede ser realizado por un usuario con legítimo acceso o por un intruso que ha ingresado por alguna vía. Este método es muy utilizado para capturar nombres de usuario y contraseñas que viajen sin cifrar a través de la red. También son utilizados para capturar números de tarjetas de crédito, direcciones de email o cualquier información importante.

Tampering o data diddling

Se refiere a la modificación no autorizada a los datos, o al software instalado en un sistema, incluyendo el borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador, con la capacidad de ejecutar cualquier comando y poder alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. El administrador del sistema posiblemente necesite dar de

baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Spoofing

Esta técnica es utilizada para actuar en nombre de otros usuarios. Una forma común es conseguir el nombre y contraseña de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él. El envío de falsos e-mails es otra forma de spoofing que podemos encontrar. Aquí el atacante envía a nombre de otra persona e-mails con algún objetivo malintencionado.

Flooding

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla. Otra acción común es la de enviar miles de e-mails en forma continua, saturando los distintos servidores.

Bombas lógicas

Este suele ser el procedimiento de sabotaje más comúnmente utilizado dentro de las organizaciones por empleados descontentos. Consiste en introducir un programa que en una fecha determinada puede destruir, modificar la información o provocar una falla de los sistemas.

Ingeniería Social

Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Básicamente se trata de convencer a la gente de que haga lo que en realidad no debería. El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil". En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet se usa, adicionalmente, el envío de

solicitudes de renovación de permisos de acceso a páginas web o emails falsos que solicitan respuestas, llevando así a revelar información sensible, o a violar las políticas de seguridad típicas.

Obtención de contraseñas

Con este método (usualmente denominado cracking) se trata de obtener aquellas claves que permiten ingresar a servidores, aplicaciones o cuentas de usuarios. Muchas contraseñas de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca lo cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos con la ayuda de programas especiales que prueban millones de posibles claves hasta encontrar la correcta.

IV.c Criptografía

Criptografía viene del griego y significa “escritura secreta”. Tiene una larga historia que se remonta a miles de años. Tanenbaum hace una distinción entre cifrados y códigos. Un cifrado hace referencia a una transformación carácter por carácter o bit por bit, sin importar la estructura del mensaje. En contraste, un código reemplaza una palabra con otra palabra o símbolo, estos últimos ya no se utilizan.

Hasta la llegada de las computadoras, una de las principales restricciones de la criptografía había sido la capacidad de la persona encargada de la codificación para realizar las transformaciones necesarias. Una restricción adicional ha sido la dificultad de cambiar rápidamente de un método de criptografía a otro, debido a que esto implica volver a capacitar a una gran cantidad de personas.

Los mensajes por encriptar se conocen como texto llano o texto plano, son transformados por una función parametrizada por una clave. El resultado del proceso de encriptación, conocido como texto cifrado, se transmite a continuación por algún canal de transmisión. Suponemos que una persona

malintencionada puede llegar a escuchar y copiar con exactitud todo el texto cifrado. Sin embargo, a diferencia del destinatario original, el intruso no conoce la clave de desencriptación y no puede obtener con facilidad el texto cifrado.

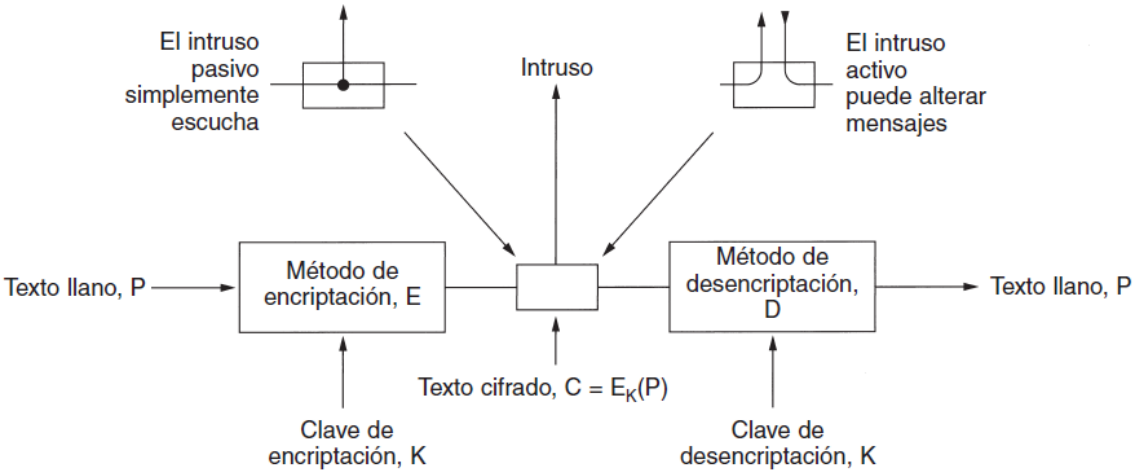


Figura 2: El modelo de encriptación

Fuente: Tanenbaum, 2003

A menudo resulta útil tener una notación para relacionar el texto llano, el texto cifrado y las claves, para ello utilizaremos $C = E_K (P)$ para indicar que la encriptación del texto llano P usando la clave K produce el texto cifrado C. Del mismo modo, $P = D_K (C)$ representa la desencriptación de C para obtener el texto llano nuevamente. Por lo tanto,

$$\mathbf{D_k (E_k (P)) = P}$$

D y E son funciones matemáticas que utilizan una clave k para encriptar y desencriptar el mensaje, si aplicamos ambas funciones al mensaje original, obtenemos la misma información.

El modelo básico es un método general estable y conocido públicamente pero parametrizado por una clave secreta y que puede cambiarse con facilidad. La idea que se conozcan los algoritmos y que la naturaleza secreta se base principalmente en las claves se conoce como principio de Kerckhoff, que debe su nombre al criptógrafo militar holandés Auguste Kerckhoff, que estableció dicho principio en el año 1883

Puesto que la parte secreta debe ser la clave, la longitud de ésta es un aspecto importante del diseño. Una longitud de clave de dos dígitos significa que hay 100 combinaciones, una clave de tres dígitos significa que hay 1.000 posibilidades y una clave de seis dígitos de longitud significa un millón de posibles combinaciones.

Los métodos básicos de cifrado son:

- Cifrado por sustitución: consiste en sustituir cada caracter o bloque de datos por otro de acuerdo a un algoritmo determinado, basado en algún tipo de clave, los ejemplos más sencillos son:
    - Aplicación de máscaras XOR: se le aplica la operación lógica XOR entre los datos a transmitir y la clave, y para obtener luego el mensaje original basta con volver a aplicar la misma operación con la clave utilizada.
    - Utilización de tablas de traducción: se trata de tablas que asignan a cada dato otro diferente que es el que se transmite. El receptor deberá tener la misma tabla para obtener el dato real representado por los datos recibidos.
- Cifrado por transposición: consiste en tomar bloques de datos y cambiar el orden de los mismos. Haciendo la transposición inversa se consigue recuperar el mensaje original.

Criptografía con cifrado simétrico

El cifrado simétrico, también denominado cifrado convencional o de clave única, era el único tipo de cifrado en uso antes de la introducción del cifrado de clave pública a finales de la década de los setenta. Básicamente los algoritmos de clave simétrica utilizan la misma clave para encriptar y desencriptar la información original.

Si denominamos M a la información a transmitir aún sin cifrar, K a la clave utilizada y ES() a la función de cifrado simétrico, en la criptografía simétrica el mensaje que se transmite es ES(K,M), resultado de cifrar M con la clave

K. El mensaje original se recupera aplicando el mismo algoritmo de cifrado con la misma clave, es decir, M = ES(K,ES(K,M)).

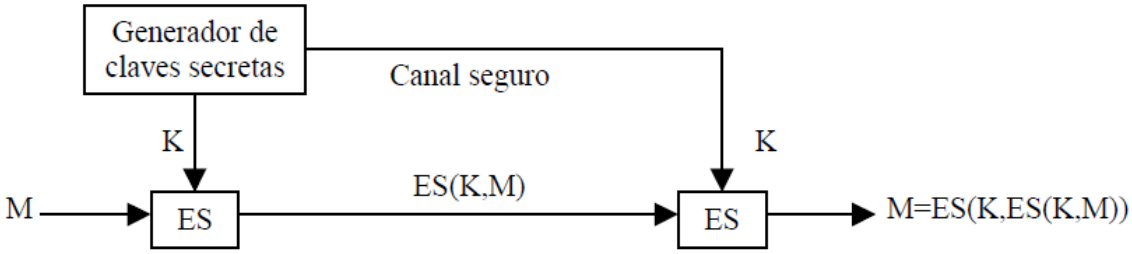


Figura 3: Modelo de cifrado simétrico

Fuente: Enguita González, 2012

Existen dos requisitos para la utilización segura del cifrado simétrico:

1. Se necesita un algoritmo de cifrado robusto. Como mínimo, es deseable que el algoritmo cumpla con el hecho de que aunque un oponente conozca el algoritmo y tenga acceso a uno o más textos cifrados, sea incapaz de descifrar el texto o averiguar la clave.
2. El emisor y el receptor tienen que haber obtenido las copias de la clave secreta de una forma segura y deben mantenerla en secreto. Si alguien puede descubrir la clave y conoce el algoritmo, toda comunicación que utilice esta clave puede ser leída.

Un ejemplo de criptografía simétrica es el Data Encryiption Standard (DES), desarrollado por el US National Burean of Standards e IBM y utiliza claves de 64 bits. Se puede aplicar de dos modos diferentes:

- En modo bloque: a partir de un bloque de información de 64 bits se genera otro bloque igual pero cifrado, siendo el resultado equivalente a una sustitución.
- En modo stream: el algoritmo se puede aplicar a un flujo de datos sin esperar a tener un bloque completo de 64 bits y resulta más difícil de romper por que la codificación de una parte de la información depende de la anterior.

Cifrado	Autor	Longitud de clave	Comentarios
Blowfish	Bruce Schneier	1–448 bits	Antiguo y lento
DES	IBM	56 bits	Muy débil para utilizarlo en la actualidad
IDEA	Massey y Xuejia	128 bits	Bueno, pero patentado
RC4	Ronald Rivest	1–2048 bits	Precaución: algunas claves son débiles
RC5	Ronald Rivest	128–256 bits	Bueno, pero patentado
Rijndael	Daemen y Rijmen	128–256 bits	La mejor opción
Serpent	Anderson, Biham, Knudsen	128–256 bits	Muy robusto
Triple DES	IBM	168 bits	Segunda mejor opción
Twofish	Bruce Schneier	128–256 bits	Muy robusto; ampliamente utilizado

Figura 4: Algoritmos comunes de clave simétrica

Fuente: Tanenbaum, 2003

Criptografía con cifrado asimétrico y claves públicas

Históricamente el problema de distribución de claves siempre ha sido la parte débil de la mayoría de los criptosistemas, como indica Tanenbaum. Sin importar lo robusto que sea un criptosistema, si un intruso puede robar la clave, el sistema no vale nada. Los criptólogos siempre daban por hecho que las claves de encriptación y desencriptación eran la misma y esta tenía que distribuirse a todos los usuarios del sistema. Por lo tanto, parecía haber un problema inherente: las claves se tenían que proteger contra robo, pero también se tenían que distribuir.

Para solucionar este inconveniente surgieron los métodos de criptografía asimétrica, donde se utilizan dos claves distintas, una para cifrar y otra para descifrar el mensaje.

Si denominamos M a la información a transmitir aún sin cifrar, Ks a la clave secreta para el descifrado, Kp a la clave pública para el cifrado y EA() a la función de cifrado asimétrico, el mensaje que se transmite es EA (Kp,M), resultado de cifrar M con la clave Kp.

El mensaje original se recupera aplicando el mismo algoritmo de cifrado pero con la clave secreta, es decir, M = EA (Ks, EA (Kp,M)).

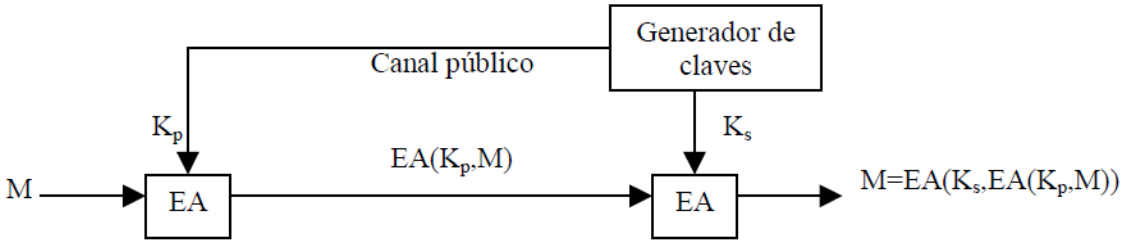


Figura 3: Modelo de cifrado asimétrico

Fuente: Enguita González, 2012

Para que un método de clave pública sea funcional se han de cumplir dos requisitos:

a) Debe ser muy difícil averiguar Ks a partir de Kp.

b) Debe ser muy difícil obtener la información que contiene el mensaje cifrado si no se dispone de Ks.

El cifrado de clave pública, propuesto públicamente por primera vez por Diffie y Hellman en su publicación "Multiuser Cryptographic Techniques" del año 1976 es el primer avance realmente revolucionario en cuanto algoritmos de cifrado en muchos años debido a que el algoritmo de clave pública se basa en funciones matemáticas en lugar de en operaciones simples sobre patrones de bits.

Un buen método fue descubierto por un grupo del M.I.T.en el año 1978 y es conocido por las iniciales de sus tres descubridores (Rivest, Shamir, Adleman): **RSA**.

Este método ha sobrevivido a muchos intentos por romperlo y se lo considera muy robusto, incluso mucha de la seguridad práctica de hoy en día se basa en él. Su mayor desventaja es que requiere claves de por lo menos 1024 bits para una buena seguridad (en comparación con los 128 bits de los algoritmos de clave simétrica), por lo cual es muy lento en su funcionamiento.

IV.d Firmas digitales

La autenticidad de muchos documentos legales, financieros y de otros tipos se determina por la presencia de una firma manuscrita autorizada. Para que los sistemas de mensajes computarizados reemplacen el transporte físico de papel y tinta se debía encontrar un método para que la firma de los documentos sea infalsificable.

El problema de idear un reemplazo para las firmas manuscritas requiere un sistema mediante el cual una parte pueda enviar un mensaje “firmado” a otra parte de modo que:

1. El receptor pueda verificar la identidad del transmisor.
2. El emisor no pueda negar después el contenido del mensaje.
3. El receptor no haya podido elaborar el mensaje él mismo.

Una de las aplicaciones del cifrado asimétrico es comprobar la autenticidad de los mensajes, es decir, la confirmación para el receptor de que el mensaje recibido ha sido emitido realmente por quien dice ser su emisor y que el mismo no ha sido alterado. Para ello el algoritmo de cifrado asimétrico ha de cumplir las siguiente propiedades:

$$M = EA (Ks, EA (Kp,M))$$

$$M = EA (Kp, EA (Ks,M))$$

Es decir que la función de encriptación asimétrica EA debe funcionar en ambos sentidos, tanto si encriptamos con la clave pública y luego desencriptamos con la clave privada, como si realizamos el procedimiento en forma inversa, es decir encriptamos con la clave privada y luego desencriptamos con la clave pública.

Un usuario A, emisor del mensaje M, lo firmará cifrándolo con su clave secreta KsA. Si se transmitiese así el mensaje EA(KsA, M), cualquier usuario que conozca la clave pública de A (KpA) podría descifrarlo.

El aplicar dos veces consecutivas un cifrado asimétrico a un mensaje completo puede ser muy costoso en tiempo de computación por lo que

generalmente no se firma todo el mensaje sino un código reducido que lo represente.

En el caso de Argentina, la firma digital se encuentra reconocida en la ley 25.506 sancionada en el año 2011.

La ley define a la firma digital (Art. 2) como el "...resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma".

Una gran ventaja del esquema de firma digital es que combina dos funciones a la vez: autenticación y confidencialidad.

Funciones Hash y MD5

Una función hash, también llamada digest, es una función cuyo resultado se obtiene a través de un algoritmo que tiene como entrada un conjunto de elementos (que suelen ser cadenas de caracteres), y los convierte en un valor de salida de longitud fija. Normalmente la cadena de entrada tiene una longitud más elevada que la de salida, por eso se las llama también funciones de resumen. La idea básica de un valor hash es que sirva como una representación compacta de la cadena de entrada.

Un efecto no deseado en las funciones hash son las colisiones, que se producen cuando, para dos valores distintos de entrada, tenemos el mismo valor hash de salida. Es matemáticamente imposible que una función de hash carezca de colisiones, ya que el número potencial de posibles entradas es mayor que el número de salidas que puede producir un hash, pero en ciertas aplicaciones especializadas con un número de entradas relativamente pequeño que son conocidas de antemano es posible construir una función de hash perfecta, que asegure que todas las entradas tengan una salida diferente.

Un algoritmo muy conocido para generar una firma digital para un conjunto de datos utilizando una función hash es el **MD5** (Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5). MD5 es un algoritmo que implementa una función hash para generar una firma de 128 bits a partir de un texto conocido.

El algoritmo está orientado a producir firmas para mensajes largos antes de su cifrado. MD5 fue desarrollado por el profesor Ronald Rivest del MIT (Massachusetts Institute of Technology, Instituto Tecnológico de Massachusetts) en el año 1991 y su funcionamiento se detalla en el RFC 1231 (http://tools.ietf.org/html/rfc1321, visto el 23/07/2013).

En la siguiente figura se muestra un ejemplo de funcionamiento de la firma digital de un mensaje utilizando el algoritmo MD5.

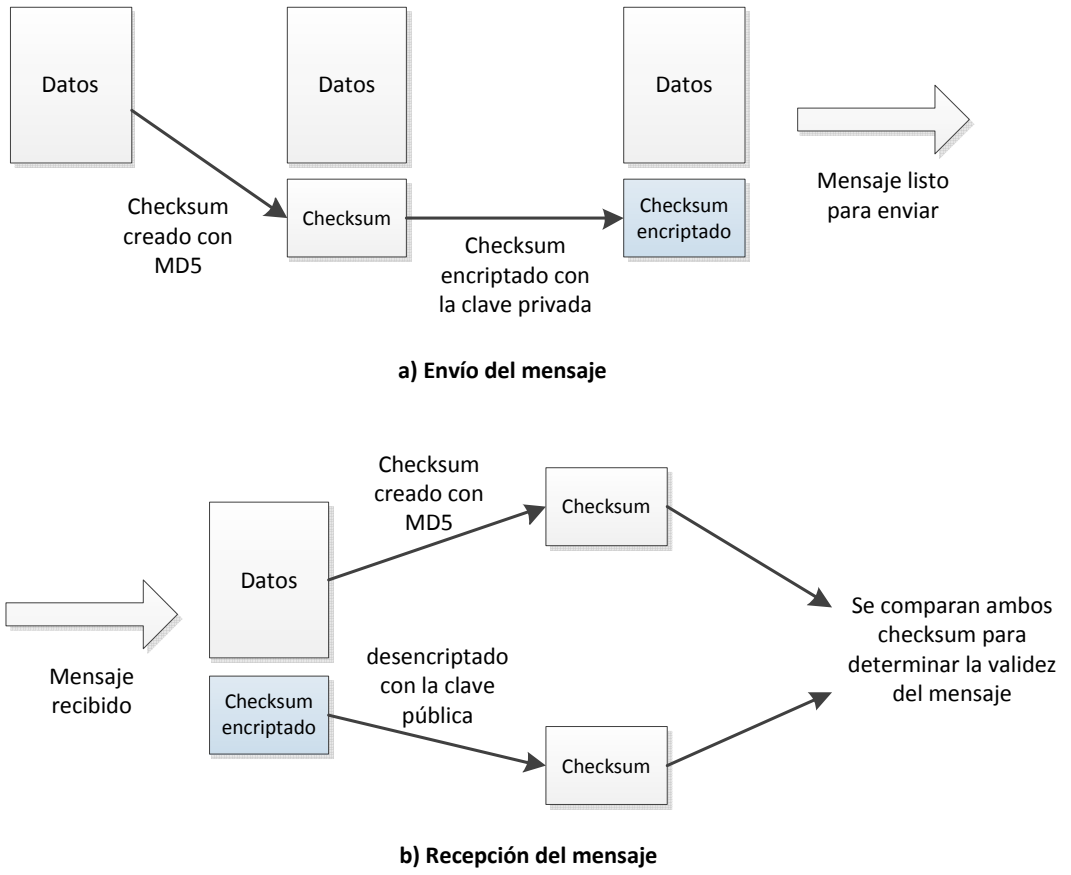


Figura 4: Esquema de funcionamiento de firma digital con MD5

Fuente: elaboración propia

Un checksum o suma de verificación es una función hash que tienen como propósito principal detectar cambios en una secuencia de datos para proteger la integridad de estos, verificando que no haya discrepancias entre los valores obtenidos al hacer una comprobación inicial y otra final tras la transmisión.

Autoridades certificadoras

Para que los métodos de clave secreta funcionen es vital que las claves se distribuyan de forma segura. En el caso de los de clave pública, el problema es más sutil. ¿Cómo se sabe que la clave pública que distribuye un usuario A que se incorpora a una comunidad es realmente distribuida por dicho usuario A y no por alguien que lo suplanta?

Un sistema de comunicaciones seguro debe disponer de una autoridad certificadora encargada de gestionar las claves secretas y/o públicas y de asegurar su pertenencia exclusiva a un usuario agilizando así el intercambio de claves en forma segura.

Dos situaciones pueden comprometer la seguridad del sistema:

1. La autoridad certificadora tiene que ser un sistema seguro ya que cualquier fallo en su seguridad comprometería la seguridad de todo el sistema que se fía de su integridad.
2. Cada usuario que se incorpora ha de establecer un enlace seguro con la autoridad certificadora mediante algún sistema que asegure la identidad de ambas partes y en la que se realice el intercambio de las claves secretas o públicas que se utilizarán en el enlace seguro.

Si se salvan con éxito estas dos situaciones, los usuarios podrán intercambiar información a través de la red cifrada mediante claves secretas y claves públicas y actualizarlas cuantas veces se quiera de forma segura a través de la red.

La autoridad certificadora verifica la identidad del solicitante de un certificado antes de su expedición. Los certificados son documentos que

recogen ciertos datos de su titular y su clave pública y están firmados electrónicamente por la Autoridad de Certificación utilizando su propia clave privada.

Una de las formas por las que se establece la confianza en una autoridad certificadora para un usuario consiste en la instalación en la computadora del mismo del certificado autofirmado de la entidad certificadora.

Una vez instalado dicho certificado de confianza, el navegador de Internet podrá validar cualquier certificado firmado por dicha entidad certificadora, ya que se dispone de la clave pública con la que verificar la firma que lleva dicho certificado.

En Argentina los certificados digitales están incluídos en la ley 25.506 (www.infoleg.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm, visto el 25/07/2013) sancionada en el año 2011, que en el Art. 14 determina lo siguiente:

Los certificados digitales para ser válidos deben:

a) *Ser emitidos por un certificador licenciado por el ente licenciante;*
b) *Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:*

    1. *Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;*

    2. *Ser susceptible de verificación respecto de su estado de revocación;*

    3. *Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;*

    4. *Contemplar la información necesaria para la verificación de la firma;*

    5. *Identificar la política de certificación bajo la cual fue emitido.*

IV.e Seguridad en la comunicación

Además de los métodos existentes para proteger la información transmitida y la autenticidad del emisor surge también la necesidad de proteger el canal de transmisión por el cual viaja la información que queremos proteger.

Cuando hablamos de protección del canal de comunicación hacemos referencia a la forma de mantener los bits enviados de manera secreta y sin modificación desde el origen hasta el destino y cómo mantener fuera a los bits no deseados.

Los problemas de seguridad que podemos encontrar se plantean en tres áreas principales:

1. La seguridad del perímetro: es la protección frente a ataques del exterior, generalmente está basada en firewalls o cortafuegos.
2. La seguridad del canal: donde se trata de proteger el canal donde viaja la información, por ejemplo a través de redes privadas virtuales (VPN) o de Secure Sockets Layer (SSL).
3. La seguridad de acceso: donde se contemplan tres aspectos, la identificación del usuario, la autorización del mismo (operaciones permitidas) y la auditoría de las operaciones realizadas.

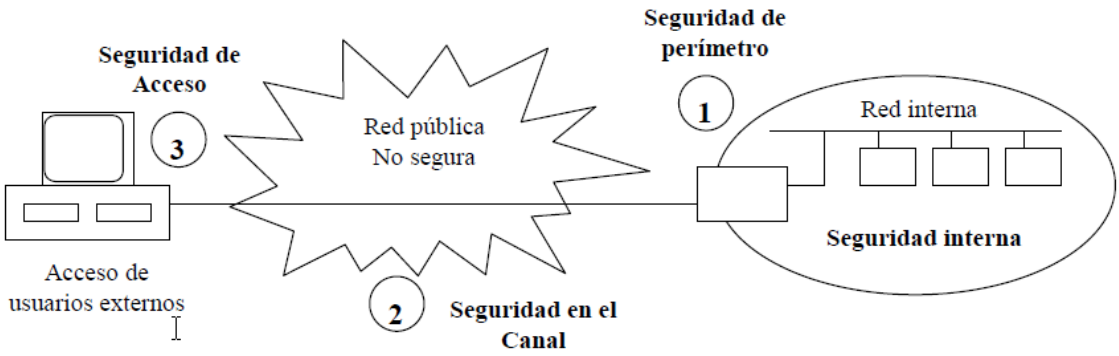


Figura 5: Áreas de seguridad en Internet

Fuente: Enguita González, 2012

Firewalls

Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo las comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos se utilizan para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet. Todos los mensajes que entren o salgan pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Hay dos políticas básicas en la configuración de un cortafuegos:

- Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar la empresas y organismos gubernamentales.
- Política permisiva: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a Internet.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

Redes privadas virtuales

Como se especifica en la página de Cisco, SSL VPN Security (http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html, visto el 25/07/2013), una red privada virtual, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo un conexión virtual punto a punto mediante el uso de conexiones dedicadas, con la encriptación de la información o la combinación de ambos métodos.

La conexión VPN a través de Internet se le presenta al usuario como si fuera un enlace privado, de ahí la designación de "red privada virtual".

Secure Sockets Layer

Secure Sockets Layer (SSL o capa de conexión segura) es un protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet.

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

SSL implica una serie de pasos:

1. Negociar entre las partes el algoritmo que se usará en la comunicación.
2. Intercambio de claves públicas y autenticación basada en certificados digitales.
3. Cifrado del tráfico basado en cifrado simétrico.

El detalle de este protocolo de comunicaciones está descripto en el Request for Comments 6101 (http://tools.ietf.org/html/rfc6101, visto el 25/07/2013).

Cuando el protocolo de transferencia de Internet, Hypertext Transfer Protocol (o HTTP) se utiliza sobre SSL, se conoce como HTTPS (HTTP Seguro).

Este protocolo, HTTPS es utilizado principalmente por entidades bancarias, comercio en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

Autentificación de usuarios

La autenticación o autentificación es el proceso de verificación de la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente que está siendo autenticado puede ser una persona que usa una computadora, una computadora por sí misma o un programa. Es un modo de asegurar que los usuarios son quién ellos dicen que son.

Los métodos de autenticación están en función de lo que utilizan para la verificación y estos se dividen en tres categorías:

1. Sistemas basados en algo conocido, por ejemplo una contraseña.
2. Sistemas basados en algo poseído, por ejemplo una tarjeta de identidad o un dispositivo usb tipo token, entre otros.
3. Sistemas basados en una característica física del usuario, por ejemplo las huellas dactilares, la verificación de patrones oculares o la verificación de la voz.

La mayor parte de los sistemas informáticos y redes mantienen una relación de identidades personales asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable que quien se está conectando es quien dice ser para que luego las acciones que se ejecuten en el sistema

puedan ser referidas a esa identidad y aplicar los mecanismos de autorización y/o auditoría oportunos.

El proceso general de autenticación consta de los siguientes pasos:

1. El usuario solicita acceso a un sistema.
2. El sistema solicita al usuario que se autentique.
3. El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.
4. El sistema valida según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no.

MARCO METODOLÓGICO

CAPÍTULO V: SISTEMA DE VOTACIÓN PROPUESTO

V.a Requisitos a cumplir por el sistema de votación propuesto

Es importante hacer notar que el sistema de voto electrónico por Internet propuesto debe satisfacer al menos los mismos requisitos de seguridad propios de los sistemas de voto convencional basado en papel. Diversos autores se han ocupado de estos requisitos de seguridad, para este trabajo tomamos como base el trabajo de Ed Gerk publicado en la revista electrónica The Bell, del año 2001, y a partir del mismo podemos determinar cuáles serán esos requerimientos a cumplir.

Estos requisitos serán los siguientes:

• **Legitimidad del votante:** En un proceso de elección, solamente pueden participar votantes autorizados y además sólo se puede tomar en cuenta un voto por votante. En el caso de los procesos de elección convencionales, este requisito se cumple cuando el participante muestra una identificación que lo acredite como votante autorizado. La autoridad de la elección comprueba la legitimidad del mismo verificando que su registro se encuentra en los padrones electorales.

• **Privacidad:** La relación entre votante y voto no debe ser conocida ni debe existir la posibilidad de que la misma pueda ser deducida. En un proceso de voto convencional se logra ocultar fácilmente la opción elegida por un votante, ya que una vez que el votante ha sido identificado como legítimo para votar, éste emite su voto de manera privada y lo deposita en una urna sellada.

• **Precisión:** El resultado de la elección debe proceder exactamente de los votos emitidos de manera legítima. Es decir, solamente los votos válidos provenientes de votantes legítimos deben ser tomados en cuenta. Por lo tanto, los votos duplicados o no válidos deben ser excluidos del escrutinio. Además, debe prevenirse cualquier alteración de los votos. Cualquier intento de quebrantar la integridad de los resultados de la elección debe ser detectado oportunamente.

• **Equidad:** No se deben conocer resultados parciales durante la fase de votación, de lo contrario dicho conocimiento podría influir en la decisión de los votantes que aún no han emitido su voto.

• **Verificación individual:** En un sistema de voto electrónico, cada votante debería poder verificar que su voto ha sido recibido correctamente (verificación de registro correcto) y que su voto ha sido incluido correctamente en el escrutinio (verificación de escrutinio correcto).

• **Verificación universal:** Un elemento importante para dar fiabilidad a un sistema de voto electrónico remoto es que este sea públicamente verificable, de tal manera que un observador autorizado pueda verificar la integridad de los resultados.

• **Incoercibilidad:** Un votante no debería tener la posibilidad de probar a un tercero la opción o candidato que ha elegido en una elección, ya que el poder probarlo facilitaría la coerción o venta de votos.

• **Robustez:** Un sistema de voto electrónico remoto debería ser tolerante a fallos tecnológicos, así como prevenir ataques de denegación de servicio. Por otro lado, un sistema de voto electrónico remoto debería ser resistente a ataques derivados de confabulaciones de autoridades deshonestas que intenten llevar a cabo un ataque contra el sistema de votación, por ejemplo violar la privacidad de los votantes o alterar los resultados de la elección.

V.b Descripción general del sistema de votación por Internet

En el sistema de votación clásico podemos diferenciar las siguientes etapas:

- Pre-elección
    - confección de los padrones electorales
    - registración de los candidatos
- Elección
    - autentificación del votante
    - emisión del voto
    - fiscalización del proceso electoral

- Post-elección
    - o contabilización de los votos emitidos por cada registro electoral
    - o consolidación y envío al centro de recuento principal
    - o escrutinio general definitivo
    - o publicación de los resultados
    - o auditoría general del proceso electoral

Básicamente este trabajo estará enfocado a la etapa de elección, ya que es dicha fase la más importante y la de mayor relevancia a la hora de hablar de un sistema de votación electrónica remota, y se hará referencia también al recuento de votos y la auditoría del sistema.

La siguiente figura ilustra el alcance general del sistema de voto electrónico y sus parámetros de entrada y salida:

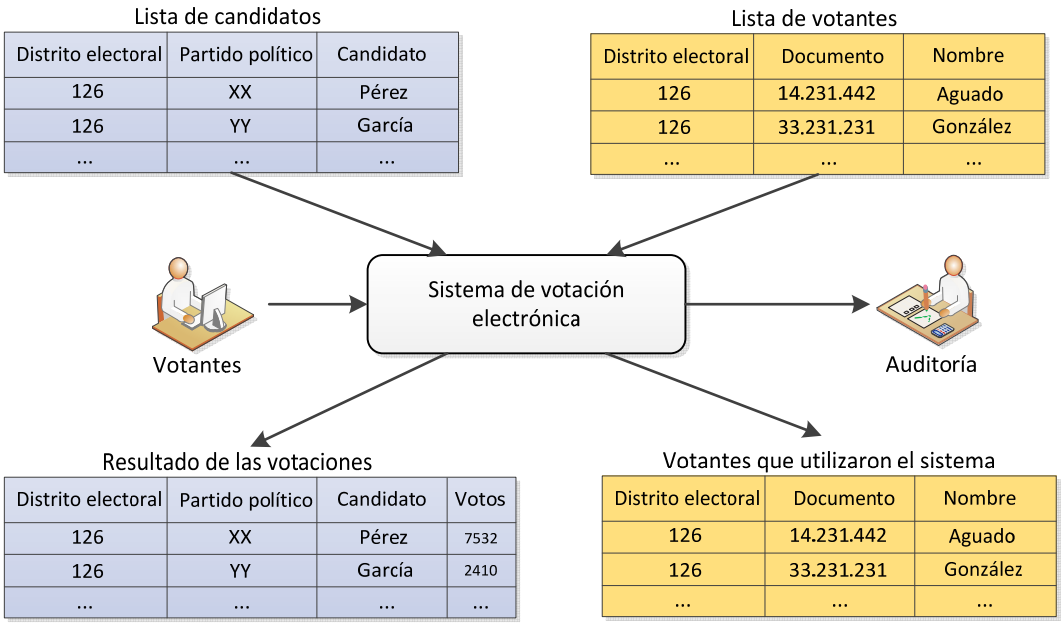


Figura 6: Esquema de votación propuesto

Fuente: elaboración propia

El sistema de votación propuesto presupone que ya se cuenta con:

a) las listas de votantes en un formato adecuado
b) las listas de candidatos en un formato adecuado

Y desde una perspectiva macro, las salidas que brindará el sistema serán:

a) la lista de votantes que utilizaron el sistema de voto electrónico
b) el resultado de la votación con los totales obtenidos por cada candidato

También es importante destacar la presencia de elementos de auditoría que permitirán darle confiabilidad al sistema y cuyo desarrollo veremos más adelante.

Implementación del proceso de votación electrónica

Para la implementación de esta propuesta se plantea que el sistema electrónico de votación no reemplace el actual sistema de votación manual, sino que lo complemente, y que el mismo esté disponible unos días antes del manual y que aquellas personas que utilicen la primera opción automáticamente queden inhabilitadas para el voto tradicional con boleta de papel.

Se propone que la vigencia del voto electrónico por Internet se lleve a cabo desde el día 14° antes del día de votación manual y por el transcurso de 7 días corridos. Una vez finalizado este plazo, el sistema quedará inhabilitado para nuevas votaciones y se procederá a confeccionar y difundir los padrones definitivos de las personas habilitadas para realizar su voto en forma manual, restándole al padrón original aquellas personas que utilizaron el método electrónico, para evitar que dichas personas puedan emitir un doble voto.

En el caso de que una persona que ya votó vuelva a ingresar al sistema para tratar de emitir nuevamente su elección, el sistema le indicará que ya ha votado y que no podrá realizarlo nuevamente. Esto sirve además para que cada persona pueda verificar en un momento posterior que su voto ha sido incluido en el recuento general.

En la siguiente figura podemos ver cómo sería la distribución de los días previos a la votación manual.

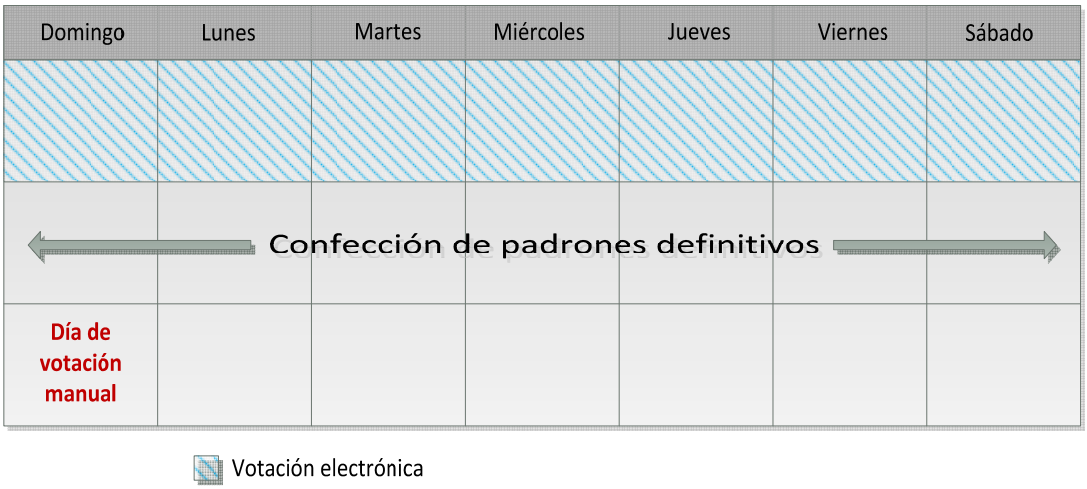


Figura 7: Cronograma de votación

Fuente: elaboración propia

Arquitectura del sistema

A continuación se especifican los componentes del sistema y se describe su funcionalidad, además se verán las interfaces entre los mismos.

El sistema está compuesto por siguientes elementos principales:

- la aplicación del votante, compuesta principalmente por un navegador web con los certificados correctamente instalados
- el servidor de cada región electoral, compuesto a su vez por dos servidores, uno para dar respuesta a las peticiones de los votantes y otro que almacenará los votos realizados
- el servidor o servidores centrales que serán los que, una vez finalizado el acto electoral, recibirán los votos de todos las regiones y realizarán el recuento final para determinar los ganadores
- un servidor que se encargará de la gestión de claves públicas de los usuarios y de los servidores intervinientes
- las aplicaciones de auditoría para que las personas designadas a tal fin puedan realizar una verificación y validación del proceso, básicamente estarán compuestas por navegadores web con los certificados correctamente instalados

En el siguiente esquema se muestra la distribución de estos elementos:

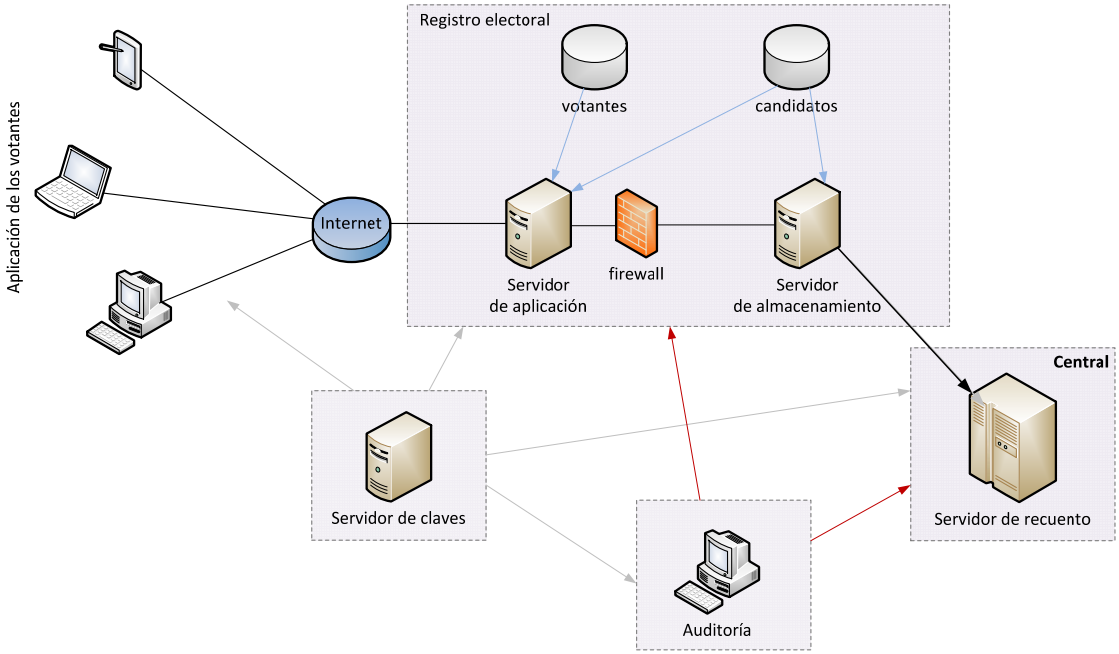


Figura 8: Arquitectura del sistema

Fuente: elaboración propia

Etapas del proceso de voto electrónico

El principio fundamental buscado con el voto electrónico por Internet es que el mismo sea lo más parecido a la votación manual, compatible con los principios electorales y la legislación vigente y, por supuesto, tan seguro como la votación tradicional.

Por lo tanto el voto electrónico debe ser uniforme y secreto, donde sólo a las personas autorizadas se les permita emitir su voto y que dicha acto sólo pueda ser realizado por única vez. Además el elector no debe ser capaz de demostrar a favor de quién emitió su sufragio, solamente se le debe permitir que verifique que efectivamente realizó la votación y que su voto ha sido tomado en cuenta para el recuento general. Además la recolección debe ser segura y confiable, y en ningún momento y bajo ninguna circunstancia se debe poder cruzar el voto emitido con la identidad del sufragante.

En base a estas premisas se determinan las etapas a desarrollar en la emisión del voto por parte de los ciudadanos y también el recuento final de los escrutinios en el momento del cierre del proceso electoral.

A continuación se detallan las etapas del proceso de votación propuesto:

1. El votante accede al sitio mediante https (Hypertext Transfer Protocol Secure, en español: Protocolo seguro de transferencia de hipertexto)
2. El votante se identifica a través de su documento nacional de identidad
3. El sistema solicita un nombre de usuario y contraseña y lo valida
4. El sistema solicita dos coordenadas de la tarjeta de coordenadas asociada al ciudadano
5. El votante ingresa las coordenadas solicitadas y el sistema y las valida
6. El sistema valida que la persona esté incluida en el padrón electoral y que no haya votado con anterioridad
7. Si hay algún error, el sistema se lo indica al votante
8. Si la información es correcta, pero el usuario ya votó con anterioridad, le indica al mismo dicha situación
9. Si todo está correcto, arma una lista de candidatos de acuerdo al distrito electoral del votante y lo muestra por pantalla
10. El votante seleccionará el/los candidato/s de su preferencia o podrá elegir la opción del voto en blanco
11. Se generará un número aleatorio para garantizar la inviolabilidad del voto cifrado
12. El voto elegido más el número aleatorio se encriptarán con la clave pública del Servidor de Recuento, para que sea éste el único capaz de descifrar dicho voto
13. El usuario firmará digitalmente el voto encriptado gracias al certificado digital instalado en su navegador
14. El voto encriptado y firmado se enviará al Servidor de Aplicación, el cual verificará la firma digital contra el identificador de sesión de Internet

15. Si está todo correcto se generará un registro de auditoría (LOG1) y se enviará la identificación del usuario más el voto cifrado al Servidor de Almacenamiento
16. El Servidor de Almacenamiento verificará nuevamente la firma digital del votante con su identificación
17. El Servidor de Almacenamiento verificará nuevamente con el padrón electoral la existencia del votante y el hecho de que este no haya emitido otro sufragio con anterioridad
18. Si se encuentra algún inconveniente registra el error en el proceso de votación en el registro de auditoría (LOG2)
19. Si todo es correcto, marca al votante en el padrón para atestiguar que el mismo ya emitió su voto. Además se genera un registro de auditoría (LOG4)
20. El Servidor de Almacenamiento genera una respuesta y la firma con su clave privada para darle autenticidad y posteriormente almacena el voto recibido
21. Esta respuesta es enviada al Servidor de Aplicación que genera un registro de auditoría si todo está correcto (LOG3) y le envía la misma al usuario
22. El votante verifica la firma digital del Servidor de Almacenamiento con la clave pública del mismo
23. Los votos recibidos se almacenan y además se genera un nuevo registro de auditoría por cada uno de ellos (LOG5)
24. Termina el proceso para el votante

Una vez finalizado el período de votación, se procede al cierre del escrutinio y al recuento de votos. A continuación se detallan las etapas de este proceso:

1. El Servidor de Almacenamiento cierra el proceso de votación, para lo cual envía una notificación al Servidor de Aplicación para que no reciba nuevos sufragios
2. El Servidor de Almacenamiento empaqueta todos los votos y los firma con su clave privada

3. Los votos encriptados y firmados son enviados al Servidor de Recuento, además se genera un registro de auditoría (LOG6)
4. El Servidor de Recuento verifica la validez del envío a través de la firma digital y la clave pública del Servidor de Almacenamiento
5. Los votos recibidos se almacenan encriptados y además se genera un nuevo registro de auditoría (LOG7)
6. Finalmente se desencriptan los votos para obtener los votos originales
7. Se procede al recuento de los votos por cada distrito electoral y por cada candidato y se genera un nuevo registro de auditoría (LOG8)
8. Se publican los resultados y se termina el proceso de votación

Las funciones que participan en este proceso son las siguientes:

Autenticación	Proceso de identificación y autentificación de los votantes
Selección	Elección del candidato/s por parte del votante
Random	Función que genera un número aleatorio
Enc	Función de encriptación de los votos
Des	Función de desencriptación de los votos
Firmar	Función que autentica un mensaje utilizando la clave privada del firmante

Y los elementos que participan en el proceso son los siguientes:

Voto	Elección del votante
R	Número aleatorio
voto_enc	Voto encriptado que sólo puede ser descifrado por el Servidor de Recuento
voto_enc_firm	Voto encriptado y firmado por el votante
ID votante	Identificación del votante en el padrón electoral
resp_firm	Respuesta de votación correcta firmada por el Servidor de Almacenamiento
votos_enc	Total de votos registrados encriptados
votos_enc_firm	Votos totales registrados firmados por el Servidor de Almacenamiento

A continuación se muestra un gráfico donde se detalla todo el proceso, tanto de votación como de recuento de sufragios:

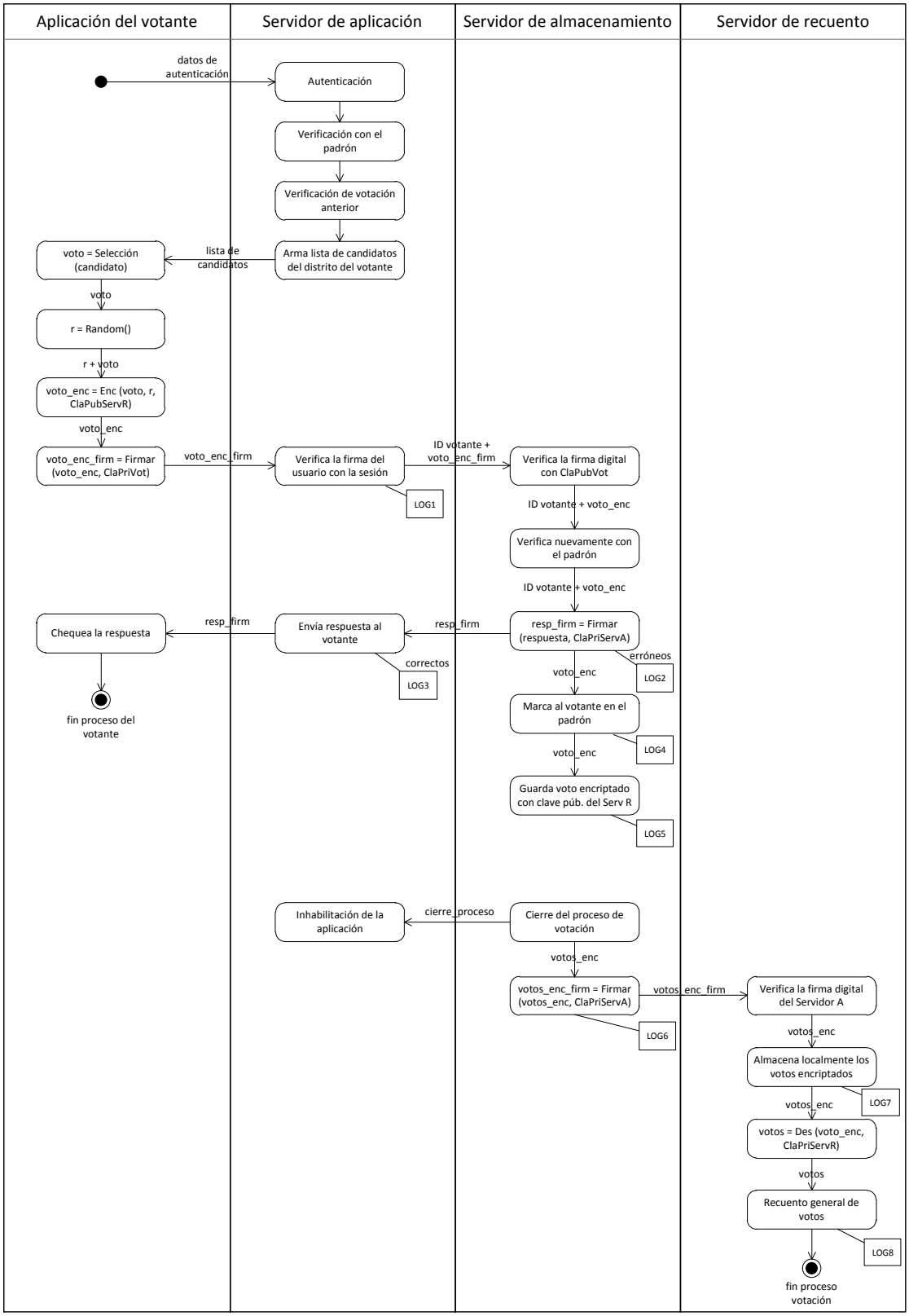


Figura 9: Proceso de votación y recuento

Fuente: elaboración propia

V.c Esquema de seguridad

Autenticación del votante

Para poder votar, el ciudadano debe poseer las credenciales necesarias que lo avalarán como votante legítimo. Dichas credenciales quedarán a cargo del RENAPER (Registro Nacional de las Personas), que es el organismo nacional que tiene por cometido formalizar el registro e identificación de todas las personas físicas que se domicilien en el territorio argentino o en jurisdicción argentina y de todos los argentinos cualquiera sea el lugar de su domicilio, llevando un registro permanente y actualizado de los mismos, desde su nacimiento y a través de las distintas etapas de su vida, protegiendo el derecho a la identidad.

Para darle un marco de seguridad que garantice la acreditación certera de las personas y que a la vez minimice la posibilidad de fraude, se combinan tres métodos, los cuales se heredan del sistema de seguridad bancario. A continuación veremos cuáles son estos elementos:

Nombre de usuario y clave de acceso

Este tipo de control constituye sin duda la forma más extendida a la que la mayoría de los usuarios están acostumbrados. En este caso se les solicitará que introduzcan un nombre y una contraseña como medio de asegurar su identidad. Dicha contraseña deberá ser suministrada por el RENAPER y para su posterior cambio el usuario deberá ingresar al sitio de dicha institución acreditando su identidad a través de los tres métodos que veremos.

Para disminuir la posibilidad de adivinación de dicha contraseña se solicitará que la misma cumpla con los siguientes requisitos:

- una longitud mínima de 8 caracteres
- deberá contener algún carácter especial y algún número
- se requerirá periódicamente cambios de contraseña
- se proveerá una opción alternativa al uso de teclados como son los teclados visuales en pantalla

- al cambiar la contraseña se comprobará que no se utilice alguna de las últimas tres empleadas con anterioridad

Además al momento del ingreso de dicho usuario y contraseña se utilizará un método denominado captcha (Completely Automated Public Turing test to tell Computers and Humans Apart, en español: Prueba de Turing pública y automática para diferenciar máquinas y humanos), se trata de una prueba desafío-respuesta utilizada en computación para determinar que quien esté accediendo al sitio en cuestión sea una persona y no un programa de computación. Además se contemplará la accesibilidad a personas con discapacidad, las cuales podrán elegir entre la validación visual o sonora.

Finalmente, para terminar de asegurar dicho esquema, se impondrá un límite de tiempo después de que sucedan tres intentos fallidos al ingreso de la clave.

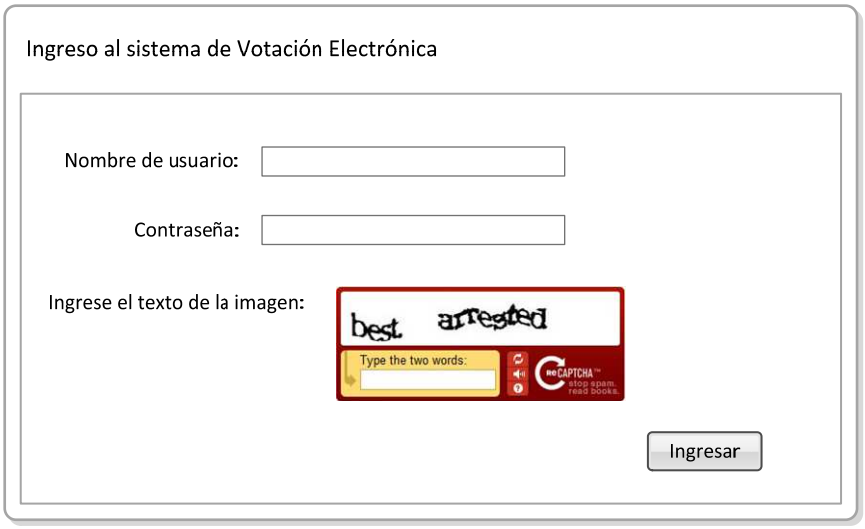


Figura 10: Pantalla de ingreso al sistema

Fuente: elaboraión propia

Tarjeta de coordenadas

La Tarjeta de Coordenadas es una tarjeta de plástico, del tamaño de una tarjeta de crédito, que contiene una matriz o serie de números (pares de datos) impresos ordenados en filas y columnas. Las filas están tituladas con

números ascendentes a partir del 1 y las columnas con letras ascendentes alfabéticamente comenzando desde la A. Trabajaremos con una de 81 coordenadas (81 posibilidades distintas), por lo cual necesitaremos 9 filas (del 1 al 9) y 9 columnas (de la A a la I). La primera celda se llamará A1 y la última I9. Además, cada tarjeta poseerá un número de serie que la identifica y la hace única.

Figura 11: Tarjeta de coordenadas

Fuente: Banco de Corrientes

Esta tarjeta de coordenadas será entregada también por el RENAPER y activada en forma personal en dicha institución.

La Tarjeta de Coordenadas posee 81 coordenadas que pueden combinarse entre sí logrando obtener 6480 claves distintas para validar la identidad del usuario. Además al momento del ingreso de la persona al sitio se le solicitarán dos coordenadas, disminuyendo la posibilidad de fraude y aumentando así su confiabilidad. Además el potencial atacante no podrá saber cuáles de las coordenadas serán solicitadas en el momento de la validación de la persona, porque las mismas serán determinadas al azar en el preciso momento del ingreso.

Como medida de seguridad adicional, después de 3 intentos erróneos consecutivos, se bloqueará la tarjeta de coordenadas, teniendo que dirigirse

la persona hasta las oficinas del RENAPER para su rehabilitación. Tengamos en cuenta que si el usuario ya llegó a esta instancia donde se le solicitaron dichas coordenadas, es porque superó la verificación anterior de usuario y contraseña, por lo cual no se verá afectado de programas que hagan intentos al azar que puedan bloquear indiscriminadamente su tarjeta.

Si la tarjeta de coordenadas ha sido robada o extraviada, le persona deberá dirigirse a cualquiera de las sucursales del RENAPER y solicitar una nueva. Automáticamente se dará de baja la tarjeta extraviada

Certificado digital y Firma digital

De acuerdo a la información recogida del sitio de la AFIP (Administración Federal de Ingresos Públicos, ente habilitado en Argentina como Certificador Licenciado), los certificados digitales son documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. De este modo, permiten verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado. Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona.

En la misma fuente podemos consultar a qué nos referimos cuando hablamos de firmas digitales. Se indica que las firmas digitales son una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos posean la misma característica que la firma hológrafa (de puño y letra) exclusiva de los documentos en papel.

En definitiva por estos medios se puede garantizar tanto la identidad del firmante como así también la integridad del mensaje.

La entidad encargada de la administración de los certificados digitales será también la RENAPER, para poder tener centralizada toda la información referida a la identificación de las personas. Para esto, dicha entidad deberá erigirse como Certificador Licenciado para Argentina, así como lo es hoy en

día la AFIP (Administración Federal de Ingresos Públicos) de acuerdo a la ley Nº 25.506.

La firma digital funciona utilizando complejos procedimientos matemáticos que relacionan el documento firmado con información propia del firmante, y permiten que terceras partes puedan reconocer la identidad del mismo y asegurarse de que los contenidos no han sido modificados.

El firmante genera, mediante una función matemática, una huella digital del mensaje, la cual se cifra con la clave privada del firmante. El resultado es lo que se denomina firma digital, que se enviará adjunta al mensaje original. De esta manera el firmante adjuntará al documento una marca que es única para dicho documento y que sólo él es capaz de producir.

Para realizar la verificación del mensaje, en primer término el receptor generará la huella digital del mensaje recibido, luego descifrará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que no hubo alteración y que el firmante es quien dice serlo.

El sistema opera de tal modo que la información cifrada con una de las claves sólo puede ser descifrada con la otra. De este modo si un usuario cifra determinada información con su clave privada, cualquier persona que conozca su clave pública podrá descifrar la misma.

En consecuencia, si es posible descifrar un mensaje utilizando la clave pública de una persona, entonces puede afirmarse que el mensaje lo generó esa persona utilizando su clave privada.

El formato del certificado digital está definido por el estándar internacional ITU-T X.509 (http://www.itu.int/rec/T-REC-X.509).

Para solicitar el certificado digital, el usuario deberá dirigirse a las oficinas de la RENAPER y llenar un formulario con sus datos, además tendrá que presentar su documento de identidad. RENAPER dará curso a la solicitud y le entregará una clave de 15 dígitos que el usuario deberá utilizar para luego

descargar por primera vez el certificado en su computadora personal. Esta clave perderá su vigencia una vez que el usuario descargue dicho certificado. Además dicho certificado deberá ser renovado cada 2 años contados desde la fecha de su emisión.

Además desde el sitio de la institución, las personas podrán verificar la instalación del certificado digital, renovar su certificado si el mismo está vencido, revocarlo y descargarlo en alguna otra computadora.

El procedimiento propuesto para descargar e instalar el certificado digital será el siguiente:

1. Ingresar a la página de la RENAPER y dentro de la misma a las opciones de certificados digitales
2. Seleccionar la opción 'Descargar Certificado Digital'
3. Introducir la clave de 15 dígitos suministrada por la entidad en el momento de tramitar dicha solicitud
4. El sistema descargará automáticamente un archivo con extensión .cer que contiene dicho certificado
5. Ubicar el archivo en el disco de la computadora y ejecutar el mismo

Se abrirá una pantalla desde la cual podremos instalar dicho certificado

Figura 12: Instalación del Certificado Digital

Fuente: elaboración propia

6. Luego aparecerá una casilla para ingresar una clave de seguridad para proteger el uso de dicho certificado en la computadora

Figura 13: Ingreso de clave para proteger el Certificado Digital

Fuente: elaboración propia

7. Luego aparecerá una pantalla que confirmará que el certificado se instaló correctamente

Una vez que tengamos instalado el certificado en nuestra computadora, podremos verificar su correcta instalación ingresando al mismo sitio y seleccionado la opción 'Verificar Certificado Digital'.

Gestión de claves

Los procedimientos de gestión de claves y el esquema de seguridad utilizados son uno de los puntos más críticos del sistema del cual dependerá el cumplimiento de los principales requisitos del sistema (la autenticidad del votante, la privacidad del procedimiento y el secreto de la votación).

La herramienta utilizada para cumplir estos requerimientos es la criptografía asimétrica donde contaremos con un par de claves, una de carácter público y una privada, conocida únicamente por el propietario de dicha clave.

Básicamente tendremos tres pares de claves públicas/privadas, instaladas en los siguientes elementos del sistema:

- Una será utilizada por el votante para firmar digitalmente su voto y así poder confirmar su identidad, además de la integridad del mensaje enviado (elección realizada)

- Otro par de claves será utilizada por el Servidor de Recuento. El votante utilizará la clave pública del mismo para encriptar su voto y dicho voto sólo podrá ser desencriptado por dicho servidor al momento del recuento final de votos. Esto garantizará que nadie dentro del circuito podrá conocer la opción elegida por el votante, ya que cuando dicho voto llega al Servidor de Recuento, no hay información que lo relacione con el emisor de dicho sufragio

- Un tercer par de claves será utilizado por el Servidor de Almacenamiento para dos finalidades: por un lado para firmar la respuesta del 'voto recibido correctamente' que luego será enviado al votante para que este pueda verificar la validez de dicha respuesta, y por otro lado para firmar el lote de votos que serán enviados al Servidor de Recuento para que este también pueda verificar la identidad del servidor que realiza dicho envío.

Este esquema puede ponerse en riesgo básicamente por tres motivos: la intersección y posterior modificación de la información enviada por el votante, el compromiso de la seguridad de la clave privada de los votantes y la corrupción del certificado instalado. Para mitigar estos inconvenientes se proponen las siguientes medidas:

Modificación de la información enviada: para evitar este inconveniente toda la información será transmitida por un canal seguro a través del protocolo HTTPS, el cual encripta la comunicación en la salida y la desencripta la misma a su llegada, por lo tanto un potencial atacante lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar. Sumado a esto se dispondrá también del uso de la firma digital del usuario para prevenir cualquier modificación de la información enviada,

ya que si se llegara a producir cierta alteración, a su llegada al servidor no validará al ser confrontada con la clave pública del votante.

Compromiso de la seguridad de la clave privada de los votantes: esta información puede verse comprometida por medio de malwares (software malicioso que tiene como objetivo infiltrarse o dañar una computadora) o hackers que intenten acceder a la misma, en el caso de los votantes dicho esquema se verá protegido por el agregado de otros elementos probatorios de su identidad (usuario y contraseña, tarjeta de coordenadas y la clave de uso del certificado digital). En el caso de los servidores se pondrá énfasis en la utilización de potentes antivirus y de robustos firewalls que impidan dichos peligros, además las claves públicas y privadas de dichos servidores serán generadas en el momento de inicio del sufragio y se destruirán una vez finalizado el acto electoral.

Corrupción del certificado instalado: si el certificado instalado en las computadoras de los votantes es destruido o si el mismo está corrupto, el usuario no podrá realizar el proceso de votación, para lo cual se preverá la habilitación, unos días antes de que comience el escrutinio, de un sitio de simulación del voto electrónico donde las personas podrán ingresar como si fuera a realizar la votación y las verificaciones que se realizarán serán las mismas que se utilizarán el día del escrutinio definitivo. Además como el período de votación propuesto es de 7 días, si el usuario encuentra algún inconveniente, puede dirigirse a las oficinas del RENAPER para solucionar los mismos.

En el caso de los certificados de los servidores, los mismos se encontrarán respaldados por una copia de seguridad guardada en un lugar seguro y de sólo acceso al personal autorizado para que las mismas puedan ser restauradas en caso de que se presente algún inconveniente.

Para evitar que se ponga en peligro la seguridad de las claves privadas de los servidores se designarán 8 personas encargadas de las mismas y para poder acceder a operaciones críticas de seguridad será necesario que se cuente por lo menos con cuatro de ellos que serán validados a través de

tarjetas electrónicas con chips de seguridad, una clave de seguridad y su documento de identidad.

V.d Auditoría

Uno de los desafíos de los sistemas de voto electrónico es ofrecer mecanismos de transparencia que permitan tanto al votante como a cualquier parte implicada directa o indirectamente en el proceso de votación, verificar la integridad de los resultados. Si cada votante verifica el correcto tratamiento de su voto se logra un alto grado de auditoría, sin embargo hay elementos que quedan fuera del alcance de los votantes. Un ejemplo de esto es la práctica de adición de votos ilegítimos en la base de datos de votos recibidos. En este caso, aún cuando cada votante puede verificar la gestión de su propio voto, ningún votante se percataría de la adición de dichos votos ilegítimos.

En términos generales, la auditoria en un sistema de voto electrónico pretende:

- Comprobar que todos los votos registrados fueron correctamente contemplados en el escrutinio final
- Detectar manipulaciones en cualquiera de los procesos en los que el sistema de votación esté involucrado
- Detectar errores de funcionamiento en el sistema de votación, los cuáles podrían haber afectado el resultado de la elección

Veremos cómo podemos solucionar dichos inconvenientes en los procesos de elección llevados a cabo con el sistema propuesto de voto electrónico por Internet a través de dos tipos de auditoría, la que se lleva a cabo antes de la elección y la auditoría posterior a la elección.

Auditoria previa a la elección

El objetivo de la auditoria previa a la elección es asegurar que todos los elementos que se usarán en los diferentes procesos funcionan de acuerdo a

las especificaciones. Las tareas realizadas en una auditoria previa a la elección son las siguientes:

- **Verificación de componentes**: se verifica la integridad de los componentes físicos y lógicos que se utilizarán en la elección

- **Auditoria de la seguridad**: se lleva a cabo un análisis exhaustivo de la arquitectura y funcionalidad del sistema de votación con el fin de determinar su seguridad y confiabilidad.

- **Validación de la configuración de la elección**: por una parte, se valida que la información que se utilizará para la elección (distritos electorales, candidatos, partidos políticos, etc.) corresponde al objetivo de dicha elección. Además, se verifica que los componentes que se utilizarán corresponden a los que se han validado previamente.

- **Certificación del código fuente**: es importante la verificación del código fuente de los sistemas que se emplearán para llevar a cabo la totalidad del acto electoral, tanto por parte de personal efectivamente contratado para realizar dicha labor, como por cualquier persona o agrupación que desee participar en la revisión de dicho código, para así transparentar todo el proceso. Para poder llevar a cabo esta verificación se pretende que la totalidad del código fuente correspondiente al sistema de votación propuesto se haga público, lo que también ayudará a recibir colaboraciones de personas interesadas en mejorar dichos sistemas.

  Después de la certificación del software a emplear, la autoridad de la elección estará a cargo de custodiar el software certificado y de vigilar la instalación de dicho software. La certificación del software es un problema crítico tanto para la autoridad de la elección como para los desarrolladores del software de votación. Por ejemplo, si una vez que el software ha sido certificado se detecta algún error de

funcionamiento, tendría que volverse a certificar el software corregido.

Auditoria durante la elección y posterior a la misma

En este caso lo que se pretende verificar es el correcto funcionamiento de todas las fases de la elección durante el proceso de votación y también una vez que esta ha finalizado.

A esta auditoría, a su vez, la podemos diferenciar en la verificación individual de los votantes y la realizada por los organismos de fiscalización que tendrán a cargo el proceso general de votación.

Verificabilidad individual de los votos

En sistemas de voto convencionales basados en papel los votantes pueden verificar que su voto es recibido correctamente ya que son ellos mismos quienes colocan la boleta en la urna física. Sin embargo, los votantes no pueden verificar que sus votos son parte del escrutinio.

Por su parte, los sistemas de voto electrónico remoto pueden proveer medios que permitan a los votantes verificar el correcto tratamiento de su voto durante el proceso de escrutinio, es decir, que el voto ha sido correctamente incluido. Si los votantes tienen la oportunidad de verificar la inclusión de su voto en el escrutinio, la fiabilidad del sistema de votación se incrementa considerablemente.

El principal objetivo de la verificación individual es que el votante pueda estar seguro que su voto se ha registrado correctamente y que además su voto ha sido incluido en el escrutinio, para ello se dispondrá de dos elementos:

- **Reingreso al sistema**: si el votante reingresa al sistema de votación (y hasta un período determinado luego de concluido todo el proceso electoral) el sistema le informará que su voto ha sido recibido y contabilizado en el escrutinio final. Para poder realizar dicha confirmación se dispondrán de elementos de auditoría interna que

veremos en el apartado de auditoría realizada por los organismos de fiscalización.

- **Tablón de anuncio electrónico**: hace referencia a la publicación en un sitio de consulta de la totalidad de votos recibidos, y dicha publicación se mantiene aún después del cierre de los comicios para mostrar la totalidad de votos recibidos y contados. El votante podrá consultar aquí su participación en la votación, pero no se mostrará ninguna información referida a su elección.

Auditoría realizada por los organismos de fiscalización

Para dotar de elementos que permitan la autenticación del proceso se dispondrá de registros de auditoría (logs de auditoría) independientes del sistema de voto electrónico.

Un log es un registro de los eventos que suceden en un período específico, y que pueden ser luego utilizados para certificar la validez de un determinado proceso. En el sistema de voto electrónico propuesto se llevará un registro de los eventos generados en la elección a fin de tener evidencias de lo que ha sucedido en caso de que se dude o se sospeche de la integridad de una elección.

El sistema de votación propuesto genera varios registros de auditoría en diferentes etapas del proceso:

LOG1: votos recibidos de los votantes

LOG2: respuesta de votación incorrecta de los usuarios

LOG3: respuesta de votación correcta enviada a los usuarios

LOG4: personas que emitieron su voto

LOG5: votos correctos acumulados en el Servidor de Almacenamiento

LOG6: votos enviados al Servidor de Recuento

LOG7: votos recibidos por el Servidor de Recuento

LOG8: votos contabilizados al final del proceso electoral

Como medida de control se deberá verificar que se cumplan las siguientes igualdades:

LOG1 = LOG4

LOG1 = LOG2 + LOG3

LOG5 = LOG3

LOG5 = LOG1 - LOG2

LOG5 = LOG6 + LOG7 + LOG8

LOG8 = LOG1 - LOG2

Por lo tanto se cuenta así con una pista de auditoría independiente para verificar el proceso de votación electrónica y para ayudar a resolver los problemas que puedan presentarse durante su implementación.

Protección de los logs de auditoría

Debido a que los logs contienen los eventos que suceden en la elección, un atacante que ha manipulado una elección podría también tratar de manipular los registros generados para eliminar el rastro del ataque. Para mantener los logs seguros, es necesario contar con técnicas de prevención y detección de manipulaciones. Para detectar manipulaciones en los logs se han propuesto los siguientes métodos:

1. Encriptación de los logs de auditoría a través de una clave privada que permita verificar por medio de su contrapartida (la clave pública) la autenticidad e integridad de la información almacenada

2. Almacenar los registros de auditoría en archivos redundantes y en diferentes servidores que luego puedan ser cruzados para constatar la integridad de la información almacenada.

3. Generar cada cierta cantidad de registros (lote) un registro de control a través del cálculo de un hash (cadena de caracteres que sirve como una representación compacta de los elementos) par que luego, en un momento posterior, se pueda generar nuevamente dicho hash y compararlo con el guardado para verificar que no se haya alterado la información del lote.

4. Generar y almacenar un número y un grupo de dígitos que indican el distrito electoral y un número secuencial. Por ejemplo, el identificador “036408975” representa que el voto pertenece al distrito electoral 0364 y que es el voto secuencial número 08975. La generación de este identificador se debe llevar a cabo durante una sesión de voto, de esta manera, si se añaden votos ilegítimos directamente en la base de datos no se contará con un identificador válido y podrá ser reconocido.

Las personas encargadas de la fiscalización del proceso, tanto las afectadas directamente al mismo como así también los fiscales de los partidos políticos (quienes, para ingresar al sistema, contarán con elementos de validación similares a los utilizados para realizar la votación) podrán realizar en forma permanente una auditoría del proceso a través de una opción creada para tal motivo que figurará también en el sitio de votación. Esta verificación la podrán realizar gracias a una herramienta del sistema que permitirá analizar de manera automática y en tiempo real, los eventos (logs) generados. Dicha herramienta pretende evitar la complejidad que supone llevar a cabo el análisis propio de los logs en forma directa.

V.e Ventajas y desventajas del sistema propuesto

El sistema de voto electrónico por Internet puede ofrecer ventajas comparativas con relación a los métodos tradicionales de votación en papel, pero a la vez puede presentar desventajas respecto al mismo. A continuación analizaremos ambas perspectivas.

Ventajas del voto electrónico por Internet

A continuación se enumeran las principales ventajas del sistema propuesto:

- Rápido conteo y totalización de los sufragios registrados
- Se puede certificar la identidad de los votantes a través de varios métodos que sumados otorgan un esquema seguro y confiable
- Permite la eliminación del voto nulo ya el sistema verifica el voto antes de que éste sea enviado y si se presenta algún inconveniente se lo informa al usuario
- Se puede votar en blanco, seleccionando el número de opción correspondiente
- Permite la emisión de votos en pocos pasos para darle sencillez al proceso
- Permite a las personas discapacitadas emitir votos sin necesidad de asistencia, por lo que se garantiza la accesibilidad para todos los ciudadanos
- El voto es anónimo y secreto ya que la identificación de la persona se realiza en una computadora diferente a donde se contabilizan los votos y no existe ningún dato que relacione ambos registros
- El sistema no permite votar más de una vez a cada ciudadano. Además no permite votar a quienes no se encuentren empadronados o no posean los elementos que acrediten su identidad
- Posee medidas de seguridad para que las comunicaciones entre las computadoras no sean alteradas
- Posee controles cruzados para no permitir el agregado de votos no emitidos ni la eliminación de sufragios

- Otorga equidad a los partidos políticos eliminando la disparidad causada por los recursos que poseen para imprimir las boletas correspondientes o controlar cada mesa electoral
- Utiliza funciones de hash y cifrados para garantizar la integridad de los datos
- Permite al votante verificar realmente el voto emitido luego de finalizado el escrutinio

Desventajas del voto electrónico por Internet

También veremos las desventajas de dicho sistema, las que tendrán que ser tenidas en cuenta para ir refinando el sistema con su implementación y acercarlo en la mayor medida posible a los niveles de exactitud y confiabilidad necesarios:

- Al no respetar el sistema tradicional de votación, puede existir cierta resistencia en la implementación del método propuesto
- Requiere de capacitación de la población en el uso de la tecnología
- Existen posibilidades de fallas o debilidades en cualquier componente electrónico que forma parte del sistema
- Pueden generarse inconveniente relacionados con ataques externos al sistema, como pueden ser virus informáticos o hackers, entre otros.
- Si se detectan inconvenientes graves que afecten al proceso podrá anularse la totalidad de los votos recibidos obligando a los votantes a volver a realizar el escrutinio por medios tradicionales
- El software que compone el sistema puede contener fallos que puedan llegar a afectar el correcto funcionamiento del proceso
- Se pueden recibir ataques de denegación de servicio (DOS: Denial of Service), que consiste en un ataque al sistema o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la misma

- No hay constancias físicas (en papel) que avalen el proceso si se quiere realizar una auditoría física
- Inseguridad en que el software certificado sea el que realmente se ejecuta en la votación electrónica

CONCLUSIÓN

Las innovaciones tecnológicas abren y cierran puertas para potenciar los derechos cívicos. La implantación de sistemas de votación remota por Internet debe servir no sólo para garantizar que sean respetados los derechos y salvaguardas actualmente reconocidos en los esquemas de votación convencionales, sino para aprovechar las posibilidades que ofrecen las nuevas tecnologías.

El principal objetivo del trabajo presentado ha sido el estudio de mecanismos que proporcionen seguridad y transparencia a los diferentes procesos electorales que hacen uso del voto electrónico por Internet. El criterio principal de la propuesta presentada ha sido la necesidad de generar mayor confianza en estos sistemas de voto electrónico remoto y pretende aportar mecanismos que ayuden a la fiabilidad de dichos sistemas, desde el punto de vista de los votantes como así también del resto de los participantes de la elección.

Tras haber analizado la problemática de los sistemas de votación electrónica existentes y las experiencias realizadas en diferentes países, se ensayó una solución con un claro objetivo: la simplicidad del proceso de emisión de sufragio, que se puedan verificar los votos emitidos, la corrección de su funcionamiento y el cumplimiento con los requisitos intrínsecos del voto.

El sistema propuesto, además consigue que todos los candidatos o partidos políticos que se presentan en los comicios posean la misma posibilidad de resultar electos, resolviendo el problema de los presupuestos con que cuentan para la emisión de las boletas que presentan los sistemas tradicionales de votación y la disparidad que se pueda presentar en la distribución de las boletas en las mesas de votación.

También se consigue verificar los sufragios sin resignar las cualidades básicas que deben ofrecer este tipo de sistemas: velocidad, simplicidad y corrección. Por eso se concluye que la votación electrónica es verificable bajo ciertas condiciones de seguridad que garanticen la libertad y privacidad de los electores durante la comprobación.

Además de las ventajas presentadas sobresalen las características de usabilidad del voto por Internet, como la prevención de errores involuntarios al seleccionar el voto o la facilidad que se ofrece a los votantes con alguna discapacidad visual para llevar a cabo la selección y la emisión de su voto sin asistencia de terceros, ya que es posible utilizar fotos de los candidatos que faciliten la selección de los mismos.

No obstante, será preciso que los votantes adquieran nuevas destrezas para manejar estos sistemas y, por tanto, puedan ejercer su derecho al voto con la misma facilidad con que lo hacen en la actualidad con el método tradicional de boleta impresa.

Para lograr la confianza de los ciudadanos es conveniente que el proceso de introducción de los sistemas de voto electrónico por Internet se realice paulatinamente, en entornos muy pequeños y con votaciones cuyos resultados sean vinculantes, pero no críticos, de manera que los votantes puedan comprobar el funcionamiento correcto de estos sistemas y poco a poco ir confiando en ellos (en un proceso de confianza similar al seguido en el uso de los cajeros automáticos o de las transacciones bancarias por Internet). Es fundamental, por lo tanto, no dar pasos en falso que puedan ocasionar un retraimiento de los ciudadanos hacia el uso de estos sistemas.

Confiamos que la implantación de este sistema de votación será un proceso creciente e imparable y que, con toda seguridad, en algún momento la votación electrónica por Internet será "lo natural" (como lo es actualmente usar el correo electrónico en lugar del correo postal).

BIBLIOGRAFÍA

Libros

- CÁRCANO, Miguel Ángel: Sáenz Peña: la revolución por los comicios, Editorial Hispanoamérica, 1986.
- KUROSE, James y ROSS, Keith: Redes de Computadoras: Un enfoque descendente. Madrid, Pearson Educación S.A., 2010.
- STALLINGS, William: Comunicaciones y redes de computadores. MadridPearson Educación, 2004.
- TANENBAUM, Andrew: Redes de Computadoras. México, Pearson Educación de México, 2003.

Sitios web

- http://www.dtc.umn.edu/~odlyzko/doc/internet.size.pdf (AT&T Labs., consultado el 02/11/2012).
- http://http://lema.rae.es/drae (Diccionario de la Lengua Española - Vigésimo segunda edición, consultado el 14/11/2012).
- http://oreilly.com/web2/archive/what-is-web-20.html (O'Reilly, What Is Web 2.0, consultado el 04/10/2012).
- http://www.sciencemag.org/content/suppl/2011/02/08/science.1200970.DC1/Hilbert-SOM.pdf (Science Magazine, consultado el 10/11/12).
- http://www.ietf.org/rfc/ (Request for Comments, consultado el 12/10/2012).
- http://www.internetworldstats.com/stats.htm (Internet World Stats, consultado el 14/10/2012).
- http://www.mininterior.gov.ar/asuntos_politicos_y_alectorales/dinap/publicaciones/HistoriaElectoralArgentina.pdf (Historia electoral Argentina, consultado el 07/10/2013).

- http://www.mininterior.gov.ar/asuntos_politicos_y_alectorales/dine/infogral/legislacion_electoral.php (Legislación Electoral del Ministerio del Interior y Transporte, consultado el 18/10/2013).
- http://www.indec.gov.ar (INDEC, consultado el 25/01/2013).
- http://www.fec.gov (Federal Election Commission, consultado el 09/07/2013).
- http://votingmachines.procon.org (ProCon.org, consultado el 09/07/2013).
- http://news.xinhuanet.com/english/2008-10/28/content_10264661.htm (Sci & Tech News, consultado el 09/07/2013).
- http://www.cs.elte.hu/~rfid/gerck.pdf (Gerck, Ed. Internet Voting Requirements, consultado el 18/09/2013).
- Enguita González, José María. Apuntes: Redes - Seguridad en las Comunicaciones. Recuperado el 4 de septiembre de 2013, del Sitio web del Departamento de Ingeniería Eléctrica, Electrónica, de Computadores y de Sistemas de la Universidad de Oviedo: http://www.isa.uniovi.es/docencia/redes/Apuntes/tema8.pdf
- http://servesecurityreport.org/paper.pdf (A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), consultado el 11/11/2013).