CAPÍTULO SEGUNDO

IMPLICACIONES DE CARÁCTER INFORMÁTICO EN EL DISEÑO DE UN SUBSISTEMA DE VOTACIÓN ELECTRÓNICA

> El ordenador es la conquista mayor del espíritu humano desde la invención de la escritura.
>
> Mac Farlane BURNET
> Premio Nobel de Biología

I. LA EVOLUCIÓN DE DISPOSITIVOS TECNOLÓGICOS RECEPTORES DE LA VOTACIÓN

El desarrollo de los dispositivos tecnológicos receptores de la votación ha obedecido a múltiples factores, entre ellos el nivel de atención de los administradores electorales, la prioridad al desarrollo de la tecnología electoral y, por ende, la aplicación de recursos presupuestales para invertir en tecnología aplicada a las elecciones, aunado a la contención de irregularidades electorales. Esta sinergia electoral encontró varios rumbos, que han permitido establecer un panorama de las distintas tecnologías electorales que han estado presentes en la toma de decisiones a nivel político de los ciudadanos.

1. *Dispositivos de primera generación*

El punto de partida en el desarrollo de dispositivos para emitir algún tipo de votación es precisamente la aportación de Thomas Alva Edison. En octubre de 1868, Edison se encontraba laborando en la ciudad de Boston, y fue precisamente ahí donde obtuvo su primera patente, la número 90,646. Al invento realizado lo denominó "registro electro-gráfico de votos", y su mecanismo de funcionamiento consistió en un dispositi-

vo que permitía a los legisladores, votar instantáneamente presionado un par de interruptores (sí o no). Desafortunadamente, los congresistas norteamericanos de aquella época sostuvieron que la referida invención, precisamente no la necesitaban ahí. Hay que destacar que este primer desarrollo tecnológico para votar es realmente el punto de origen de los sucesivos dispositivos receptores del voto público, y además, conceptualmente, los actuales sistemas para la emisión del voto en los órganos legislativos en el mundo tienen su raíz en la inventiva de Alva Edison.

2. *Dispositivos de segunda generación*

La cabina automática de Jacob H. Myers, *lever machines* o máquinas de palanca (1892), constituyen los dispositivos de segunda generación, que permitieron que el voto de los ciudadanos en los procesos electorales fuera automatizado. El funcionamiento de las máquinas de palanca descrito por la Comisión Electoral Federal de los Estados Unidos de Norteamérica[24] radica en que cada candidato o partido político es identificado por el elector meditante una etiqueta, sistema de tiras visibles o disco visible, al que se le asigna una palanca distribuida de manera rectangular en posición horizontal en el frente de la máquina.

El procedimiento de votación efectuado por el elector consiste inicialmente en aislarse mediante una cortinilla para posteriormente tirar de la palanca hacia abajo de acuerdo con su preferencia electoral. Una vez realizada esta acción, la palanca regresa a su posición original (horizontal) de manera automática. El mecanismo a base de engranes permite que cada palanca, al regresar a su posición inicial, haga una rotación contraria conectada en la máquina a un décimo de una rotación completa. Por su parte, el engrane contrario permite una posición de cuenta numérica girando a los "diez" un décimo contrarios de una rotación para cada rotación completa de la máquina.

En síntesis, si cada uno de los mecanismos de rotación funciona correctamente y si se parte de un contador inicial de cero, la posición de cada contador permite, al cierre de la votación, contabilizar el número de votos

24 Véase Federal Election Commission, United States of America, Information about mechanical lever machines. *http://www.eac.gov/clearinghouse/docs/glossaryspanishtoenglish.pdf/attachment_download/file*, formato pdf, página 40, consultada en febrero de 2009.

de manera automática, según el número de impulsiones que haya tenido cada palanca. Este mecanismo permite que los electores no voten en más de una ocasión. No obstante, desde hace algunas décadas ya no se producen este tipo de dispositivos, y su uso es actualmente reducido.

3. *Dispositivos de tercera generación*

Las *punch cards machines* (o sistema a base de tarjetas perforadas) permiten ejercer el derecho de sufragio a través de una tarjeta que funciona como boleta electoral efectuando orificios o perforaciones a un costado de la fórmula de candidatos o partido político. También, el procedimiento para emitir el sufragio puede realizarse insertando la "tarjeta electoral" en un soporte que coloca de manera lineal el nombre de los candidatos o partidos políticos de manera previa a la realización de las perforaciones, que es propiamente la forma de indicar las preferencias del electorado. Este dispositivo cuenta, desde luego, con una especie de aguja, que permite la perforación de la "tarjeta electoral", y encuentra sus primeras aplicaciones en el ámbito electoral en 1964. Es preciso señalar que el desarrollo de las tarjetas perforadas tiene su fundamento en la tecnología Hollerith, con aplicaciones en las técnicas de carácter censal.

4. *Dispositivos de cuarta generación*

Los sistemas de escaneo óptico (también conocidos como *marksense*) han sido un elemento importante en la automatización del sufragio público. El mecanismo de funcionamiento de este dispositivo tecnológico-electoral es a partir del diseño de una boleta electoral, que contiene el listado de candidatos elaborada con un papel especial, que permite al sufragante, mediante un lápiz con determinadas características (*v. gr.* grafito densidad número 2), marcar la papeleta electoral rellenando un óvalo, o bien un cuadrado, que indican sus preferencias electorales. El procedimiento para computar los votos es precisamente introducir la boleta electoral en una máquina, que permite escanear las marcas realizadas por el elector e interpretarlas como sufragios emitidos. Con respecto a este dispositivo, refiere Julia A. Glidden que una de sus principales ventajas consiste en la posibilidad de efectuar un recuento de la votación ante alguna posible falla o deficiencia de la máquina de escaneo óptico (*v. gr.*

utilización de tintas diferentes para efectuar las marcas en la boleta electoral que el lector óptico no reconoce). Sin embargo, también reconoce que la impresión de las boletas electorales resulta costosa, ya que éstas requieren ser elaboradas con especificaciones y tintas especiales que pueden incrementar considerablemente el costo de una elección, y, adicionalmente, este tipo de papeleta electoral está expuesta a factores climáticos.[25] Adicionalmente, si un elector utiliza un marcador diferente al autorizado puede traer como consecuencia la distorsión en la lectura que realiza el escáner, o bien si el ciudadano efectúa dobleces en la boleta electoral, el lector óptico interpretará el sufragio como nulo.[26]

Este tipo de dispositivos de escaneo óptico ha sido clasificado por la *Enciclopedia Aceproject* de la siguiente forma:

a) *Optical Mark Reading* (OMR)
b) *Optical Character Recognition* (OCR)
c) *Intelligent Character Recognition* (ICR)
d) *Imaging Technology Optical Mark Reading-scanning systems* (TI)

El dispositivo de lectura óptica de marcas (OMR) ha sido comúnmente utilizado desde la década de los setenta. El funcionamiento del OMR parte de que el *scanner* da lectura a una serie de marcas en un contorno definido dentro de una página (boleta electoral). El *software* integrado al dispositivo se encuentra programado para reconocer referidas marcas y convertir la marca o imagen escaneada dentro del ordenador en datos legibles. No obstante, distintos especialistas electorales señalan que los OMR resultan ser limitados para su aplicación en sistemas electorales complejos (*v. gr*. cuando se utilizan el sistema de voto en listas abiertas, voto transferible, voto alternativo, voto simultáneo, entre otros). Así, advierten que su viabilidad resulta prudente en sistemas de voto simples, esto es, en listas bloqueadas o cerradas con voto único.

El OCR, mediante el sistema de escaneo, captura las imágenes, y mediante el *software* integrado al dispositivo reconoce íntegramente las formas de un texto impreso o caracteres escritos a mano, como letras y números, que son almacenados en el ordenador como datos legibles.

25 En las elecciones primarias del Partido Demócrata en Arizona, durante el año 2000, alrededor de 10,000 boletas electorales debieron desecharse por haberse corrido la tinta especial debido a factores climáticos.

26 Glidden, Julia A. y McLaughlin, Meg T., *La soberanía popular en la era digital*, Estados Unidos de Norteamérica, 2000.

Particularmente, los *Optical Character Recognition* (OCR) han sido ordinariamente utilizados para convertir texto impreso en texto legible dentro del ordenador.

Un dispositivo de mayor complejidad tecnológica son los sistemas de escaneo de reconocimiento inteligente de caracteres (ICR). Este tipo de escáneres aplica inteligentemente criterios lógicos para reconocer caracteres que con mayor seguridad son convertidos en datos informáticos legibles. Los ICR actúan mediante un *software* precargado que recurre a reglas de gramática y ortografía para una adecuada interpretación de los datos reconocidos. Según Aceproject, los ICR requieren de ordenadores con mayor capacidad y rapidez para procesar información. No obstante, esta tecnología está disponible desde mediados de la década de los noventa.

Para finalizar con los dispositivos de escaneo óptico, la tecnología de imagen (TI) permite capturar imágenes para ser almacenadas en imágenes legibles computarizadas. Esta realidad tecnológica logra que fotografías, dibujos e imágenes de texto sean recopilados con la posibilidad de reutilizarlas en formas legibles computarizadas. Un ejemplo de su aplicación en materia electoral lo encontramos con propósitos de identificación de los electores cuando su fotografía es integrada en credenciales que posteriormente pueden ser digitalizadas.

5. *Dispositivos de quinta generación*

El *televote*, *televoting* o voto por teléfono constituye una variante de la tecnología electoral desarrollada para la toma de decisiones a nivel político. Este dispositivo tiene sus primeras aplicaciones en la década de los ochenta en Canadá. Su funcionamiento radica en que el propio elector puede usar el servicio telefónico que cuente con teclas de tonos. En primer lugar, el votante accede al servicio marcando el número telefónico gratuito del servicio de votación, teniendo a la vista una credencial para votar asignada previamente, que cuenta con un número de identificación personal (PIN) o mensaje de datos. A continuación, siguiendo los tonos de voz indicados, se conecta usando su credencial de elector y el teclado del teléfono. Con posterioridad, siguiendo las instrucciones, el elector ingresa el código de los candidatos o partidos políticos. Después, el sistema da lectura al código del candidato seleccionado y responde al

ciudadano la confirmación de su preferencia electoral. En este punto, el votante está en condiciones de confirmar la opción electoral recibida por el sistema telefónico, o bien, regresar y cambiar su selección.

Brevemente, el funcionamiento del *televote* o *televoting* gravita en habilitar una red telefónica que simultáneamente provea la capacidad técnica de asignar números personales de identificación (PIN's) a los votantes. Esta generación de dispositivo, conceptualmente emplea el teléfono como una especie de máquina de grabación electrónica directa, en virtud de que la línea telefónica sólo es el canal para que el ciudadano registre en un sistema informático su voto habilitando el teclado telefónico.

6. *Dispositivos de sexta generación*

Las máquinas de votación de grabación electrónica directa, urnas electrónicas, *machines a voter* o *machines* DRE (*Direct Recording Electronic*) son en realidad ordenadores que permiten al votante, mediante selectores (botones) o pantallas táctiles, emitir su sufragio. El principio de funcionamiento de las máquinas DRE consiste en grabar electrónicamente los votos, generalmente bajo elementos de criptografía en dispositivos informáticos de almacenamiento (memorias). Algunos tipos de urnas electrónicas permiten la impresión en papel del voto del elector, situación que permite auditar el correcto funcionamiento de la máquina de votación. Este tipo de dispositivos tienen un alto impacto en la administración de una elección, y que sólo pueden ser amortizados, después de varios procesos electorales. En cuanto al *software* electoral, también tiende a ser complejo y costoso.

7. *Dispositivos de séptima generación*

La televisión digital interactiva o iD-TV es una opción que se ha comenzado a explorar para posibilitar el sufragio público de los ciudadanos desde su domicilio. Los canales de televisión digital operan de manera muy similar a Internet. Desde luego, la televisión digital permite navegar en un menú de sistema bastante amplio usando el control remoto. Sin embargo, hasta el momento esta posibilidad sigue siendo limitada.

8. *Dispositivos de octava generación*

La tecnología SMS (*Short Messages System*), o mensaje de texto, difiere significativamente de otros dispositivos de votación, y fundamentalmente es un canal de votación que provee menos interactividad hacia el votante. Ahora bien, la principal desventaja en este proceso de votación es el costo que implica el envío del mensaje, que es cargado por el proveedor del servicio móvil de telefonía hacia el cliente en primer término, pero que paralelamente tiene la calidad de votante, situación que no es deseable en un proceso democrático.

El procedimiento de uso para acceder al servicio de votación vía mensaje de texto consiste en que el votante redacta un sencillo mensaje que contiene su sentido de voto; esto es, introduce la palabra "voto" mediante su código de acceso, basado generalmente en doce dígitos. A continuación inserta el código o clave de su candidato. Posteriormente, el votante envía su mensaje de texto usando su NIP proveído con anterioridad en una credencial para votar, y el sistema recibe, confirma y valida el voto enviado. Excepcionalmente, si el voto enviado resultó no válido, el votante recibe un mensaje de error.

Las redes digitales públicas como Internet representan un esquema que desde hace algunos años se analiza para hacer viable el voto electrónico en su modalidad remota. El primer paso para construir una plataforma informática que permita el voto por Internet es constituir una dirección de *website* administrado por las autoridades electorales y anclado en la utilización de servidores (como recurso y soporte). En este sentido, también se procede de manera previa a la autenticación y autorización del votante generándole *smart cards*, NIP's, o bien simplemente asignándole firmas digitales que permitan su acceso al sistema de votación remoto. Este procedimiento, por cierto, bastante complejo, dadas las condiciones de involucrar a distintas autoridades, tales como la autoridad emisora de los certificados digitales al elector, la autoridad revisora de los mismos y la autoridad que valida finalmente los certificados digitales de índole electoral, las cuales son reguladas por la autoridad central electoral, permiten un acceso controlado y debidamente validado del cuerpo electoral. De forma complementaria, los sistemas de votación vía Internet deben considerar al menos una base de datos relativa al registro de los electores, el registro de la votación en línea y la transmisión de los resultados electorales procesados mediante niveles adecuados de cripto-

grafía. En resumen, éstos son algunos elementos que se integran en la modalidad de votación electrónica remota *online*, pero en sí, el procedimiento resulta más complejo para su explicitación.

II. La integración del *software* electoral en un subsistema de voto electrónico

Uno de los primeros desafíos institucionales de las autoridades electorales al incorporar subsistemas de votación electrónica radica en determinar si se acude a proveedores de soluciones informático-electorales disponibles en el mercado con sus posibles conveniencias e inconveniencias, o bien, se toma la decisión de desarrollar *hardware* y *software* electorales para ser aplicados a sus necesidades institucionales. En el primer escenario, habría que considerar el impacto presupuestal derivado de la adquisición de los mecanismos tecnológico-electorales, el pago relativo a licencias de *software*, la compatibilidad técnica de los dispositivos con los requerimientos constitucionales y legales del sufragio, pago de soporte técnico antes y durante la jornada electoral, niveles de seguridad de los dispositivos de votación electrónica, capacitación de recursos humanos, costos postelectorales relativos al mantenimiento y almacenamiento de las máquinas de votación, entre otros. En el segundo escenario, optando por el desarrollo propio o con asistencia técnica de los dispositivos receptores de la votación, habría que considerar entonces proyectos de tecnología electoral que se incubarían a mediano y largo plazo, también con un impacto presupuestal para la autoridad electoral. Este último contexto de desarrollo de tecnología electoral que se incorporaría a los subsistemas de votación electrónica motivaría, de igual forma, la decisión institucional de utilizar *software* aplicativo bajo licencia privativa o recurrir a *software* libre no comercial con código fuente abierto, aspectos que trataremos en este punto líneas más adelante.

El *software* constituye la estructura lógica que permite al ordenador la ejecución de una serie de actividades para lograr un resultado. La mayor parte de las personas se refieren al *software* comúnmente como programas de cómputo.[27] Por su parte, la Organización Mundial de la Propiedad Intelectual (OMPI) define a los programas informáticos como el conjunto de instrucciones expresadas en un lenguaje natural o formal,

27 Téllez Valdés, Julio, *La protección jurídica de los programas de computación*, 2a. ed., México, UNAM, Instituto de Investigaciones Jurídicas, 1989, p. 8.

pudiendo, una vez traducidas y transpuestas en un soporte descifrable por una máquina de tratamiento de datos, o por una parte de esta máquina, efectuar operaciones aritméticas y, sobre todo lógicas, en vías de indicar o de obtener un resultado particular. Una distinción inicial de los programas de cómputo señala que existen programas de explotación (conocidos también como "sistema operativos"), programas de aplicación y microprogramas (*firmware*). [28]

Ulteriores clasificaciones en torno al *software* se han plasmado atendiendo a la función que realiza dentro del ordenador y el grado de estandarización o uso. En cuanto a la funcionalidad del *software*, éste se clasifica en:

— *Software* de base. Es el relacionado con los controladores que regulan el funcionamiento interno del ordenador; por ejemplo, sistemas operativos, controladores para dispositivos periféricos del ordenador, *software* de memoria, lenguaje de programación.
— *Software* aplicativo. Consiste en *software* que desarrolla funciones específicas para el usuario de acuerdo con sus necesidades o requerimientos; por ejemplo, hojas de cálculo, procesadores de textos, bases de datos.

En lo que concierne a la clasificación del *software* según su grado de estandarización o uso, encontramos la siguiente:

— *Software* aplicativo. También se le denomina *package*, que es desarrollado atendiendo a la necesidad de los usuarios. Este *software* ha sido el principal punto de impulso de la industria del *software*.
— *Software* a medida. Denominado como *custom mode*, es desarrollado para atender requerimientos propios de empresas e instituciones, los cuales pueden ser modificados.
— *Software* de acuerdo con el cliente (*customized*). Se trata de programas de tipo estándar que son modificados ex profeso a las necesidades de un usuario en particular, partiendo, como se mencionó, de una estructura genérica.

28 Téllez Valdés, Julio, *op. cit.*, p. 5.

El hablar de *software* electoral nos conduce a definirlo como el conjunto de instrucciones para ser usadas directa o indirectamente en un ordenador a fin de obtener un resultado determinado primordialmente automatizado en actividades relacionadas con el desarrollo de un proceso electoral.

La mayor parte del *software* electoral es de tipo aplicativo y del tipo *custom mode* (*software* a medida). Podríamos señalar, sin temor a equivocarnos, que el *software* electoral que se incorpora a los subsistemas de votación electrónica es la parte medular que garantiza un correcto desarrollo e implementación del voto electrónico que no genere dudas o suspicacias electorales. Este tipo de *software* electoral desarrollado para ser operado en ambientes de votación electrónica contempla *software* para transmisión de información, cifrado de información, descifrado de información, *firmware*, así como *software* para introducir datos en los módulos para la recepción de la votación.

El punto de partida para desarrollar este tipo de *software* electoral comienza con la oportuna realización de un cuadro de análisis, la elaboración de una gráfica de la estructura, la realización de una gráfica IPO (*Input-Processing-Output*), la aplicación de algoritmos y su representación en flujogramas que incorporen la problemática y necesidades constitucionales y legales del sufragio, además de los lineamientos institucionales en torno a la operatibilidad, seguridad y auditabilidad o que dicte la autoridad electoral, y que son captados por los programadores, que proceden a escribir el programa informático.

La gráfica de estructura es elemento básico del desarrollo del *software* electoral mediante el cual se clasifica, divide y subdivide un problema, en este caso, el voto electrónico. A partir del desarrollo de la gráfica de la estructura como actividad inicial del lenguaje de programación, se deben determinar una serie de módulos que abordarían el problema planteado concentradamente y que a su vez motivaría el desarrollo de subtareas o submódulos que se multiplican o reducen de acuerdo con la problemática formulada al programador. De manera general, al desarrollar una gráfica de la estructura se recurre al método de solución *top-down* (de arriba hacia abajo), y posteriormente se recurre al uso de algoritmos, que en el lenguaje de la programación son propiamente la escritura de un conjunto de instrucciones inteligibles para el ordenador que solucionan el problema planteado, siendo esta la parte más importante en la escritura del

software electoral, y que son estructurados y representados a través de un flujograma.[29]

Ahora bien, la experiencia internacional sobre el desarrollo de *software* electoral que se integra a los subsistemas de votación electrónica indica que es recomendable lo siguiente:

a) El *software* electoral debe estructurase a partir de módulos, los cuales no deben permitir su automodificación.
b) El módulo del *software* que procesa el conteo de la votación recibida debe ser escrito en un lenguaje de alto nivel.
c) El *software* no debe residir en el dispositivo, excepto el *software* de base relacionado con el arranque del sistema o control de periféricos.
d) El *software* electoral debe ser instalado en el dispositivo en ocasión de cada proceso electoral, siendo supervisado este proceso por los representantes de los partidos políticos, los cuales pueden aleatoriamente aplicar un test de seguridad al *software* electoral instalado.
e) Adicionalmente, según Brunazo Filho, no pueden existir compiladores (códigos ejecutables) instalados el día de los comicios en las urnas electrónicas.

Sin embargo, acudiendo al principio de transparencia electoral, un cuestionamiento trascendente es: ¿resulta posible conocer el *software* electoral instalado en los ordenadores para receptar la votación? Más aún: ¿podemos acceder al código fuente? Aplicando el principio de transparencia electoral, debiera ser así; no obstante, habrá que reconocer que permitirlo de facto conduciría, conforme señala Brunazo Filho, a potenciar la probabilidad de ser vulnerado o modificado; en pocas palabras, esta situación autorizada sería motivo de especial atención para delincuentes electorales de alta tecnología.

Por otra parte, es una situación de facto que la mayoría de los programas informáticos integrados en sistemas de votación electrónica se encuentran escritos mediante programación estructurada que enfatiza el uso de algoritmos. La programación estructurada parte de la idea fundamental de romper o diseccionar el programa en unidades más

29 Kernighan, Brian W. *et al*., *El lenguaje de programación*, 2a. ed., México, Prentice-Hall Hispanoamericana, 1991, pp. 4 y ss.

pequeñas, tales como procedimientos, funciones, subprogramas o subrutinas.[30]

En términos de Luis Joyanes, cada una de las funciones establecidas mediante programación estructurada tiene un propósito claramente definido, y utiliza un método descendente y de constante refinamiento sucesivo, situación que produce un programa informático extremadamente extenso, que si se le pretende efectuar algún tipo de cambio en los datos, los ajustes a todo el programa se vuelven múltiples y laboriosos. Particularmente, la escritura de un *software* electoral que introduzca el voto electrónico tendría un considerable número de funciones, con algunas limitantes si se opta por una programación estructurada. Una posible opción para superar esta gran cantidad de funciones al momento de programar podría ser la programación orientada a objetos (POO).

La programación orientada a objetos pone mayor énfasis en los datos, al contrario de la programación estructurada, que enfatiza en algoritmos.[31] El POO, como método de programación, logra organizar los datos de su programa de forma paralela a los objetos que forman parte del mundo real. Cabe citar que los programas informáticos aplicados al voto electrónico procesan en mayor medida gran cantidad de datos, de ahí tal vez la pertinencia de valorar una escritura orientada a objetos.

1. Software *aplicativo bajo licencia privativa*

Con anterioridad hemos señalado la noción de *software* aplicativo; no obstante, al adicionar la expresión "bajo licencia privativa", precisemos que nos referimos a *software* electoral que ha sido desarrollado para satisfacer las necesidades específicas de los usuarios, del cual se obtiene o pretende obtener un lucro por su utilización; es decir, *software* de índole comercial y restringido en cuanto a su uso (conocido como *software* propietario). A la mayor parte de los proveedores de soluciones informáticas que ofrecen máquinas de votación electrónica se les debe retribuir el pago por concepto de *software* aplicativo bajo licencia, situación que encarece un proyecto institucional de voto electrónico, pero que puede ofrecer un cierto nivel de seguridad informática al estar restringido el acceso a su código fuente, a pesar de su lucro.

30 Joyanes Aguilar, Luis, *Microsoft C/C++7. Manual de bolsillo*, Madrid, McGraw-Hill, 1994, p. 113.

31 *Ibidem*, p. 116.

2. Software *libre*

La premisa básica para considerar a un *software* libre de uno que no lo es, consiste en que los usuarios están autorizados para estudiar el funcionamiento del programa, adaptarlo a sus necesidades y estar en condiciones de distribuirlo, incluso produciendo programas derivados, aunque no necesariamente la condición de libre implica gratuidad. En este sentido, las condiciones básicas para la utilización del *software* libre son:

a) La libertad de utilizar el *software* sin restricciones de algún tipo.
b) La facultad atribuida al usuario para estudiar el funcionamiento integral del *software*. Esta prerrogativa del programador delegada al usuario permite el acceso al código fuente.
c) La autorización para redistribuirlo, inclusive atendiendo ciertas reglas básicas otorgadas por el programador al nuevo usuario; por ejemplo, el *copyleft* o izquierdo de copia.
d) La posibilidad de efectuarle mejoras sustanciales al programa informático y difundirlas públicamente.

Un claro ejemplo de *software* de base libre es el sistema operativo GNU/Linux, el cual fue desarrollado desde 1984, mediante el proyecto GNU, y expandido en 1991 por Linus Towald, y que es el resultado de la incesante colaboración de cientos de progamadores en todo el mundo. Algunos modelos de urnas electrónicas desarrolladas en México han incorporado a sus ordenadores GNU/Linux; por ejemplo: el desarrollado por la Facultad de Estudios Superiores Aragón de la Universidad Nacional Autónoma de México. Una característica fundamental de Linux es la robustez del sistema basado en el reducido número de ocasiones para reiniciarlo. Sin embargo, la instalación del sistema Linux ofrece una serie de inconveniencias, ya que al no tratarse de una labor sencilla, se requiere de personal capacitado. Al respecto, este tipo de sistemas operativos en urnas electrónicas crearía la necesidad de personal técnico mayormente capacitado en entornos de UNIX, que complicaría la labor de soporte informático durante la jornada electoral.

En realidad, el sistema Linux ha tenido un crecimiento exponencial en los últimos años, particularmente debido a su carácter esencialmente de gratuidad. Esta situación, en países con escasos recursos económicos y con limitaciones para desarrollos tecnológicos, crea un panorama alta-

mente atractivo; por ejemplo, Brasil es un país que ha recurrido constantemente a *software* con núcleo de base Linux, y paralelamente es uno de los países que mayormente ha avanzado en cuestiones de votación electrónica.

3. *Código fuente*

El término "código fuente" (*source code*), más allá de un sentido estrictamente literal debe entenderse como el texto original de un programa informático; es decir, constituye la escritura integral del *software* como la escribió el programador. El acceso al código fuente permite comprender el funcionamiento de un programa y su eventual modificación. La noción de código fuente está estrechamente vinculada al concepto de *software* libre, en virtud de que un programa no puede ser considerado libre si su código fuente no está disponible para los usuarios, tal y como se mencionó con anterioridad. En razón de lo que precede, una reflexión institucional inicial motivaría a considerar seriamente la pertinencia de recurrir a *software* electoral libre con código abierto para integrarlo a subsistemas de votación electrónica. En resumen, acudir a *software* electoral libre con código fuente abierto tiene sus implicaciones positivas y negativas, y en el caso de recurrir a *software* electoral aplicativo bajo licencia privativa también presenta la misma disyuntiva.

En este rubro habría que considerar dos situaciones. Por una parte, emplear *software* aplicativo bajo licencia privativa con restricción de acceso al código fuente ofrece seguridad informática, pero crea cierto nivel de dependencia informática en empresas que ofrecen las soluciones de votación electrónica, situación que debería valorarse con detenimiento (véase caso Smartmatic-Consejo Nacional Electoral de Venezuela). Por otra parte, recurrir a *software* libre y partiendo de las nociones básicas para utilizarlo, que otorgan la prerrogativa del programador delegada al usuario de acceder al código fuente, sería un escenario deigual forma a valorarse.

Esta situación de eventual acceso y conocimiento al código fuente, a pesar de considerar la transparencia en todos los sentidos en la escritura del *software* de votación electrónica, haría inconveniente su conocimiento público ante eventuales ingresos no autorizados al sistema informático, al conocer la estructura del programa a fondo. Esta prerrogativa de-

bería ser arrogada exclusivamente a los órganos de dirección de las autoridades electorales, quienes por principio de neutralidad política o imparcialidad y confianza deberían constituir la única instancia que conozca y resguarde el código fuente del *software* electoral que se introduzca en los dispositivos de votación electrónica, prevaleciendo así la confidencialidad de aquél en un entorno de control. No obstante, un procedimiento que debería estar abierto a los partidos políticos es la verificabilidad en el funcionamiento correcto del *software* electoral instalado en los módulos de recepción de la votación electrónica.

4. *Verificabilidad del correcto funcionamiento y resguardo del código fuente*

Es una premisa básica en el plano informático, el debido y seguro resguardo del texto original del programa informático que se va emplear en un ambiente de votación electrónica para propiciar un nivel de confianza adecuado y estableciendo un principio de no publicidad del mismo, pero sí de verificabilidad. La escritura del texto original debe estar orientada a operaciones que no sean escritas de manera extensa y que carezca de puertas traseras en su escritura, para un correcto funcionamiento.

Un referente agregado importante en el voto electrónico es la implementación de múltiples pruebas de funcionamiento del *software* electoral *ex ante* a la decisión institucional de integrarlos a los módulos de recepción de la votación. La credibilidad en el correcto funcionamiento del *software* electoral por parte de los actores políticos y sociales depende en gran medida de un debido desarrollo y funcionamiento del *software*, razón por la cual éste es un punto sustancial que no solamente atenuaría, sino que erradicaría suspicacias electorales, atendiendo previamente a múltiples pruebas de funcionalidad programática.

III. La integración del *hardware*

1. *Módulos de control para los funcionarios electorales*

Los componentes físicos de las computadoras o de una red son elementos sustanciales junto con el *software* para operar un subsistema de votación electrónica. En realidad, los módulos de control constituyen mi-

croterminales que pueden integrar los censos o registros de electores que autorizan la emisión legal del sufragio a los ciudadanos autorizados para tal efecto en una determinada área o sección geográfica electoral. Las microterminales o módulos de control del voto electrónico son terminales controladas por una microcomputadora que validan generalmente el acceso de los electores a través de mensajes de datos o mecanismos de identificación biométrica; por ejemplo, el número de cédula de identidad, credencial de elector y la huella digital.

En la mayoría de los casos el módulo de control posibilita que en un entorno vigilado el funcionario electoral sólo autorice bajo la fiscalización de los partidos políticos, votar a quien se encuentre debidamente autorizado. En algunos casos, la microterminal, de manera visual, mediante un lead,[32] o mediante sonidos de cierta intensidad, indica el ingreso autorizado del elector y la conclusión del procedimiento de votación en un entorno legal, procedimental y técnico autorizado.

Cabe citar que estas microterminales, mediante contraseñas asignadas e informadas previamente al presidente o responsable de la mesa receptora de votación, permiten constatar, en principio, que la urna electrónica se encuentra en cero (actas de urnas vacías), validan el inicio de la votación, el cierre de la votación y la impresión del boletín de urna.

2. *Módulo de recepción de la votación*

Los módulos de recepción de la votación son, en realidad, ordenadores que permiten al votante, mediante selectores (botones) o pantallas táctiles, emitir su sufragio. El principio de funcionamiento de los módulos consiste en grabar electrónicamente los votos, generalmente bajo elementos de criptografía, en dispositivos informáticos de almacenamiento (memorias internas y extraíbles). Las pantallas sensibles al tacto, una vez corroborado el acceso al sistema, presentan una especie de boleta electoral virtual al ciudadano para elegir la opción política de su predilección. La mayor parte de estos módulos despliegan la fotografía de los candidatos e incluyen mecanismos de criptografía durante el tratamiento de la información generada a partir del sufragio de los ciudadanos. De manera general, una buena parte de los módulos receptores de votación electrónica funcionan de manera independiente, refiriéndonos al hecho de no

32 Indicador visual electrónico.

estar conectados a una red que posibilite, mediante ingresos no autorizados, que provoquen la alteración de la información electoral; no obstante, eventualmente algunos módulos ofrecen la posibilidad de conectarse a redes locales.

En algunos casos los módulos de votación para efectos de control integran un número de serie o de identificación de fábrica accesible mediante *software* aplicativo; así también, los módulos están programados para operar solamente durante la jornada electoral en un horario predeterminado.

En circunstancias de pérdida o ausencia de energía eléctrica, los módulos, por regla general, contemplan una batería que se integra al mismo ante estas eventuales contingencias de suministro de energía o ante su utilización en zonas rurales sin infraestructura.

Ahora bien, partiendo de necesidades de auditoría, de seguridad, pero especialmente por razones de otorgarle certeza al elector en el tratamiento de su sufragio convertido en información, la mayor parte de los módulos, a través de impresoras internas o externas, emiten la comprobación del voto; es decir, en soporte de papel impreso que contiene el resumen de la opción política vertida en el ordenador, que son depositados en una urna transparente o caja de resguardo.

En una primera aproximación al funcionamiento del *hardware* utilizado en el voto electrónico, su funcionamiento básico pareciera en extremo simple; sin embargo, su descripción es más compleja, pero para una mejor comprensión del mismo, sus funciones básicas que informáticamente tienen que procesar las máquinas de grabación electrónica directa las reducimos solamente a tres. El proceso básico sería entrada-almacenamiento-salida del microcomputador, que traducido funcionalmente en el procedimiento electoral del voto público sería: introducir opción electoral (1)-almacenar información fragmentada y encriptada (2)-salida mediante impresión de información electoral (3) (véase figura 1).

Un diagrama más detallado en la figura 2 ayudará a comprender de manera más minuciosa el procedimiento informático de introducir la opción electoral (*input*)- almacenar (*store*)- sacar (*output*).

Figura 1

Descripción básica de la funcionalidad del voto público informático

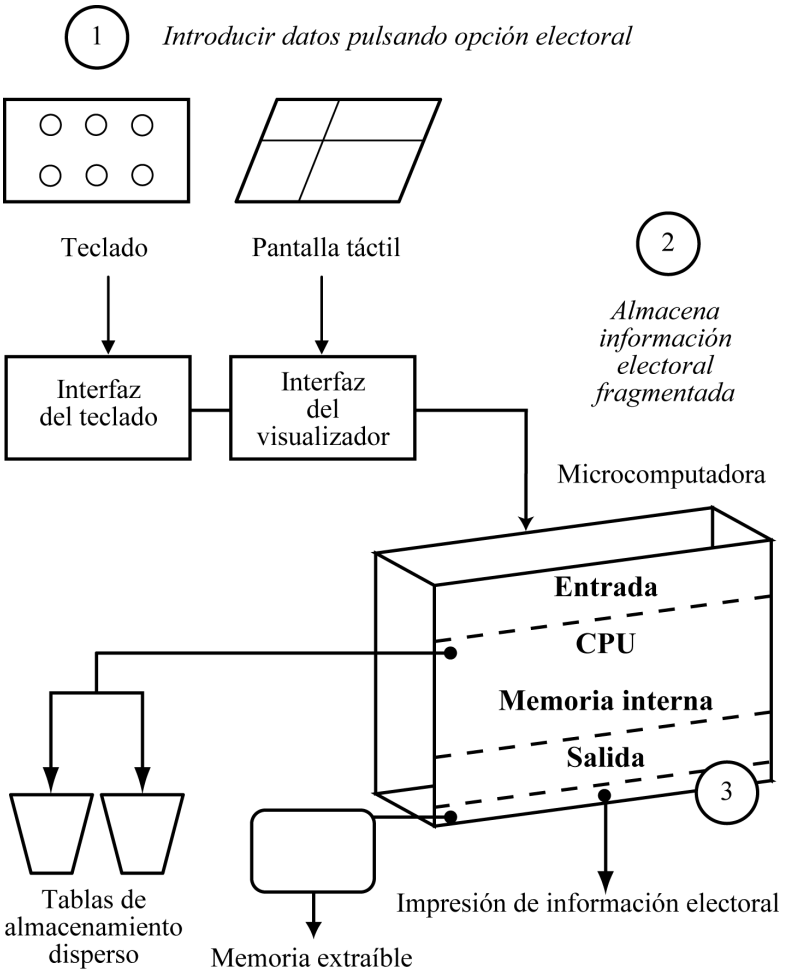
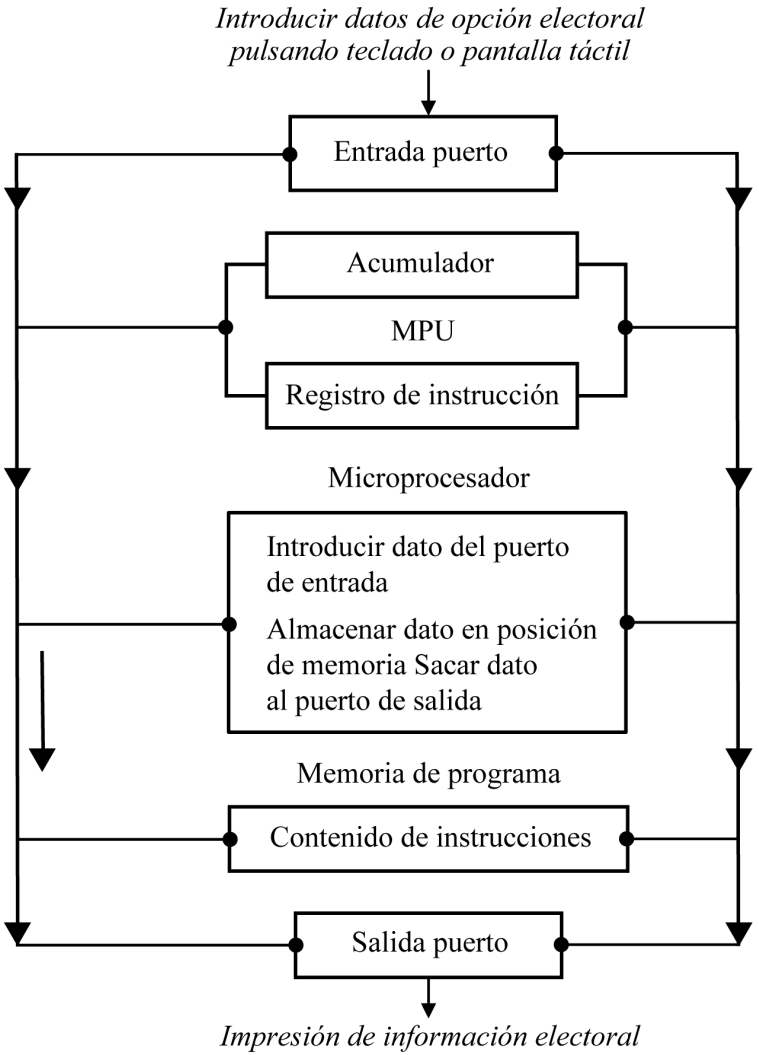


Figura 2

Descripción detallada del voto público a través de urna electrónica ejecutando instrucciones de la memoria del programa



3. *Servidores*

Los servidores son sistemas que proporcionan recursos en la red. En Internet son utilizados para designar aquellos sistemas que proveen información a los usuarios de la red. En materia de voto electrónico, los servidores de alta capacidad desempeñan un papel fundamental en la etapa de totalización de resultados con el auxilio de la telefonía y protocolos IP.

Los servidores, en la etapa de totalización de resultados electorales dentro del voto electrónico o informatizado, facilitan un amplio rango de operaciones complejas de bases de datos, siempre y cuando se realicen bajo niveles adecuados de criptografía en tiempo real. Las operaciones efectuadas por conducto de los servidores viabilizan la validación de electores, recolección de datos electorales, remisión de información a las autoridades centrales electorales, enrutamiento de la información después de la jornada electoral, administración de redes electorales establecidas para fines de computación total de la votación, regulación en el acceso de electores en votación no presencial, registro de electores, entre otros.

En resumen, los servidores en el plano del voto informatizado constituyen una serie de aplicaciones informáticas que coadyuvan a su vez a otras aplicaciones informáticas para propiciar funcionalidad. A la generalidad de aplicaciones informáticas conexas que benefician a otras aplicaciones se le denomina comúnmente "clientes". Los registros de electores en proyectos de redes informáticas aplicadas en proyectos de votación electrónica remota, como E-POLL, tienen su punto de partida en redes informáticas operables y gestionadas por algunas autoridades locales europeas mediante servidores centrales que procesan archivos de datos electorales (registros de electores).

Hay que hacer notar que un servidor también puede procesar la entrega de información electoral que puede servir a otro procedimiento electoral bajo el modelo autoridades electorales regionales o locales/autoridad central electoral. En materia de voto informatizado, los servidores establecidos por la autoridad administrativa electoral deberían analizar con mucha prudencia el recurrir al protocolo FTP (*File Transfer Protocol*), cuya característica principal consiste en procesar información basado en un protocolo de transferencia de archivos conectados a una red TCP. Las bondades de un servidor basado en FTP es que brinda un má-

ximo de velocidad en la conexión y, por ende, en la transmisión de información. El inconveniente principal de FTP es que no ofrece la máxima seguridad en la transmisión de la información, ya que el *password* de los usuarios y la transferencia de archivos se remite vía texto plano sin ningún tipo de cifrado, por lo cual la información electoral queda notablemente expuesta. Algunas aplicaciones, como SCP y SFTP, pueden atemperar esta problemática cifrando el tráfico de información.

Aunado a lo anterior, los sistemas de gestión de bases de datos pueden constituir una aplicación práctica que serviría de interfaz entre las bases de datos, la autoridad electoral y las aplicaciones informáticas que utilizarían. Por regla general, los sistemas de gestión de bases de datos se estructuran con un lenguaje definido previamente de datos, un lenguaje de manipulación de datos y de un lenguaje de consulta. El objetivo central de los SGBD es administrar, de manera clara, simplificada y con cierto nivel de seguridad, un conjunto de datos.

4. *Memorias internas y externas*

El almacenamiento informacional dentro de los subsistemas de votación electrónica se registra simultáneamente en la unidad fija interna de almacenamiento masivo (disco duro), y en la unidad externa de almacenamiento removible (*flash drive*). Cabe aclarar que la información almacenada mediante esta vía es encriptada y fragmentada mediante algoritmos que deben imposibilitar su manipulación. En algunos modelos de urnas electrónicas se emplean memorias USB; ciertos modelos más antiguos utilizaban disquetes de 3½. La pertinencia de utilizar dispositivos externos de memoria con puerto USB es de fácil manejo para almacenar información y transferir datos de un ordenador a otro, incluso a un servidor central en velocidades de transferencia que permiten recopilar información electoral de forma óptima, sin necesidad de algunos requerimientos técnicos conexos, como el uso de cables o baterías de respaldo.

Una característica adicional de las memorias USB, *memory stick*, *pendrive*, *handy drive* o *USB flash drive*, es su alta resistencia a factores climáticos externos, así como al polvo y al manejo rudo, a diferencia de otros mecanismos de almacenamiento portátil.

IV. Subsistema de registro de votantes

Bases de datos electorales

En la mayoría de casos los módulos de control que operan los funcionarios electorales registran, validan y autorizan el acceso de los electores en un ambiente de votación electrónica durante la jornada electoral; parten de la preexistencia de bases de datos o registros electorales, incluso en modalidades de votación electrónica remota o a distancia. Una parte considerable de urnas electrónicas recurren a bases de datos cuyo almacenamiento opera a partir de soportes informáticos materializados. En la terminología informática suele denominárseles a los referidos soportes como mecanismos de descarga local. En el caso de bases de datos almacenadas y consultables a través de una red pública o privada, el mecanismo de almacenamiento se le cita como descarga de tipo remoto. Esta última clasificación de almacenamiento de datos es mayormente utilizable en modalidades de votación electrónica a distancia.

La creación o utilización de bases de datos tiene implicaciones directas con el espacio disponible en la memoria de la unidad de almacenamiento fijo masivo, conocido comúnmente como disco duro. El almacenamiento de datos dentro del módulo de recepción de la votación electrónica debe considerar no sólo el universo de electores que ahí votaran, sino también la información que generarán a partir de los distintos cargos a elegir, por lo que con bastante prudencia se debe estimar el tamaño de almacenamiento necesario de la memoria interna y la extraíble para gestionar la información receptada y eficientar la concentración de información para un adecuado desempeño. En razón de lo anterior, las bases de datos incorporadas y la información producida por dispositivos de votación electrónica y que se traducen en la acumulación de datos deben revisar, según Henry F. Korth, al menos los siguientes aspectos:

a) seguridad;
b) espacio disponible en el disco duro;
c) rapidez en la actualización de datos, y
d) velocidad en la carga de tablas.

V. Códigos de control del sistema

Los códigos de control son instrucciones que permiten representar datos, programas u otras aplicaciones que se establecen para procesar y facilitar su tratamiento automático o transmisión. El Instituto Electoral y de Participación Ciudadana de Coahuila ha expresado que los códigos de control permiten la administración autorizada y restringida de un subsistema de votación electrónica. Este organismo electoral señala que los códigos de control se pueden agrupar de la siguiente manera:[33]

a) Código de apertura
b) Código de cierre
c) Código de reimpresión
d) Código de restauración

La mayor parte de estos códigos generados aleatoriamente son operados principalmente por los funcionarios electorales que presiden las mesas receptoras de votación, tratándose de votación electrónica presencial, y por el personal de soporte técnico de los organismos electorales.

Los códigos de apertura de las urnas electrónicas funcionan, como su nombre lo indica, para abrir el sistema informático de las máquinas DRE. Esta acción permite a los funcionarios electorales que integran una casilla electoral, obtener un primer reporte sobre el estado y funcionalidad del sistema e iniciar el procedimiento de recepción de la votación, además de verificar ante los fiscales o representantes partidistas que el sistema parte de cero sufragios emitidos.

Los códigos de cierre se utilizan para clausurar la recepción de la votación y obtener un reporte integral del número de electores que sufragaron y el cómputo de la votación.

Los códigos de reimpresión son utilizados cuando el sistema no emite el soporte en papel del sufragio emitido por la ciudadanía. En esta eventualidad de carencia del comprobante de votación, este código posibilita nuevamente su impresión para generarle certeza a los electores.

En el caso de los códigos de restauración, que en principio tienen un carácter excepcional, permiten, ante ciertas eventualidades, recuperar in-

33 Colina, Luis de la, "Sistema de votación electrónica del Instituto Electoral y de Participación Ciudadana del Estado de Coahuila", ponencia presentada durante el III Votobit, celebrado en Torreón, Coahuila, en mayo de 2005.

formación electoral cuando súbitamente una urna electrónica se haya apagado por causas de ausencia de energía eléctrica.

VI. Códigos de votación autorizados

Los códigos de votación son aquellos que dan acceso a los electores al sistema informático de los módulos de recepción de la votación y que simultáneamente autorizan al ciudadano, ingresar a las boletas electorales virtuales para procesar su sufragio informáticamente.

Algunas autoridades administrativas electorales, como el IEPCC en México, han procedido a la encriptación de códigos de votación mediante procedimientos parciales establecidos de la siguiente manera:[34]

a) El código de votación numérico es transformado de base,
b) En forma selectiva se transforman los caracteres numéricos de base en caracteres numéricos y en alfabéticos, y viceversa,
c) Se ordenan de forma aleatoria,
d) Se insertan dígitos o caracteres al azar, sin que tengan valor alguno, y
e) Se insertan dígitos de verificación (véase gráfica 1).

[34] *Ibidem*, pp. 10 y 11.

Gráfica 1

Procedimiento parcial de encriptación de códigos de votación[35]

Código original	*Paso 1*	*Paso 2*	*Paso 3*	*Paso 4*	*Paso 5*
01 001	02711	KMRLL	MKLRL	MDKLRL	MUKALRL
01 002	02712	02712	01722	D01722	5017G22
01 003	02713	KMRLN	LRMKN	LRMEKN	LRM1KN
01 004	02714	02714	20174	20R174	2G04174
01 005	02715	KMLRP	KLRMP	VKLRMP	NKLRAMP
01 006	02716	02716	17206	1720B6	1720LF6
01 007	02717	KMRLR	MKLRR	MK0LRR	MKQALRR
01 008	02718	02718	07218	097218	0H72F18
01 009	02719	KMRLT	KRLMT	KRMLYT	KARMLIT
01 010	0271A	KMRLA	KLMRA	GKLRMA	VKALRMA
01 011	0271B	0271B	1720B	1H720B	1L720EB
01 012	0271C	KMRLC	KMRLC	KMJRLC	KAMZRLC
01 013	0271D	0271D	2017D	20117D	2E01U7D
01 014	0271E	KMRLE	LRMKE	LRMKFE	LRAMKVE
01 015	0271F	0271F	0721F	I0721F	80F721F
01 016	02720	02720	27200	272W00	2F72J00
01 017	02721	KMRML	MKMRL	MXKMRL	MNKAMRL
01 018	02722	02722	02722	F02722	5027G22
01 019	02723	02723	02723	F02723	4024F23
01 020	02724	02724	20274	201274	2F0A274

VII. Subsistema de validación y autentificación de los votantes

Autenticar, en el plano electoral, implica autorizar o legalizar una situación especifica que se refleja en una institución jurídico-electoral, y

[35] Fuente: Instituto Electoral y de Participación Ciudadana del Estado de Coahuila.

se materializa a través de un procedimiento electoral. Es un hecho que una situación básica en el procedimiento para recoger el voto ciudadano parte de autorizar idónea y legalmente a los electores que se encuentran debidamente facultados para ejercerlo. Esta autenticación del elector en un contexto de voto electrónico se puede cumplimentar tecnológicamente de la siguiente manera:

a) Tarjetas inteligentes que incorporan *chips* de datos de los ciudadanos

Las denominadas *smart cards* incorporan cintas magnéticas con información o chips de datos que almacenan información electrónica acerca del elector. En ocasiones la información incluye datos para bioidentificación, que solamente posibilitan su lectura. También se han desarrollado tarjetas inteligentes que novedosamente autorizan la lectura-escritura de la tarjeta. Un ejemplo es cuando se usa para verificar el derecho a votar del elector, y puede ser utilizada una sola vez, y que simultáneamente puede ser grabada para ser usada durante una elección específica. En el caso del voto por Internet o a distancia, algunos países han implementado esta solución tecnológica para validar la identidad del votante.

b) Mecanismos de identidad electrónica

Los mecanismos de identidad electrónica, también conocidos como de firma electrónica, es una forma tecnológicamente avanzada para proveer la autenticación del votante, y particularmente se ha utilizado en el registro de votantes en la modalidad de votación electrónica a distancia en entornos no controlados del todo por la autoridad electoral. Los números personales de identificación (PINs), desde hace algún tiempo han sido desarrollados, y generalmente se estructuran a partir de llaves públicas encriptadas.

c) Técnicas basadas en rutinas de comparación

En cuanto a las técnicas de *match* para autenticar al elector, se ha escrito *software* que ejecuta rutinas de comparación (domicilio, fecha de nacimiento, entre otros) para determinar alternativamente qué ciudadanos pueden aplicar para ser incorporados en un registro electoral, y posteriormente ser autenticados.

d) Técnicas de reconocimiento de firma

Los escáneres pueden ser empleados para electrónicamente capturar firmas ológrafas de los electores. Estas imágenes digitalizadas de las firmas pueden estar disponibles en redes informáticas que puedan interpretar comparaciones visuales de firmas digitalizadas. En este punto, algún tipo de *software* que eventualmente identifique las firmas escaneadas puede alertar, mediante una marca o señal, posibles comparaciones erróneas de la firma del elector y determinar su correcta identidad.

e) Fotografías digitalizadas

Las fotografías digitalizadas de los rostros de las personas pueden ser usadas como un método para determinar si un ciudadano pretende registrarse en más de una ocasión en un censo o registro de índole electoral. El diseño de *software* electoral puede abarcar la comparativa de referida fotografía digitalizada confrontándola con una base de datos electorales preexistente.

f) Sistemas de bioidentificación

Los sistemas de identificación biométrica se han agrupado tecnológicamente en dos segmentos: bioidentificación visual y bioidentificación electrónica.

La bioidentificación visual incluye el uso de fotografías, firmas y huellas digitales en documentos de identidad. En la mayoría de las democracias del mundo donde opera el sistema tradicional de votación, la autenticación del elector se suministra a través de este procedimiento acudiendo a documentos nacionales de identidad o sencillamente credenciales de elector.

En cambio, la bioidentificación electrónica comprende el uso de voz digitalizada, el reconocimiento de una mano, así como el reconocimiento de huellas digitales o imágenes de la retina del ojo. En particular, este tipo de información se almacena en discos o tarjetas inteligentes, que a su vez se confrontan con datos previamente registrados a los cuales se accede por conducto de un lector electrónico.

VIII. Garantía de secrecía del voto por medio de algoritmos de dispersión

Un elemento básico a considerar en el desarrollo del *software* electoral que se integra en los subsistemas de votación electrónica es precisamente cumplimentar los requerimientos constitucionales del voto público, entre los que se encuentra la secrecía del voto. Precisamente, el desvincular la identidad del votante con el sentido de su decisión política es un asunto de primer orden en el voto electrónico o informático. La pregunta que surge es: ¿la informática puede garantizar íntegramente la secrecía del voto? Este cuestionamiento nos deriva al ámbito de la informática mediante niveles de seguridad adecuados en el procesamiento y registro de la información, que en todo momento deben garantizar el desvanecer el nexo causal entre la identidad del elector y el contenido expresado de su decisión política. Ahora bien, este asunto primordial en la naturaleza del sufragio público es una cuestión a cumplimentar con o sin tecnología, en la que la autoridad electoral debe poner especial énfasis. El voto emitido vía informática, a diferencia del voto tradicional, se convierte en información que debe ser almacenada mediante un tratamiento informatizado óptimo; esto nos remite dentro de la informática a la aplicación de algoritmos de dispersión.

Los algoritmos son definidos como una secuencia de pasos que conducen a la realización de una tarea; es decir, se trata de un conjunto ordenado y finito de etapas que conducen a la obtención de un resultado. En el lenguaje informático se traducen como instrucciones inteligibles para el ordenador, que buscan un resultado para el usuario.

En el contexto de la informática actual, resulta común utilizar tecnología de tablas o rejillas de almacenamiento disperso, que ofrecen funcionalidad en el tratamiento de la información, y sobre todo seguridad. Este tipo de tecnología, esencialmente divide los datos en múltiples segmentos, los cuales, si llegaran a ser interceptados de forma no autorizada, sólo reflejarían un mínimo de información que no permite visualizar la información en su totalidad; es decir, de su contenido informacional original. Los algoritmos de dispersión de información o IDAs habían sido utilizados con antelación para almacenar información de supercomputadoras y de sistemas informáticos avanzados.

En efecto, esta categoría de algoritmos se integran a tablas de almacenamiento disperso, entendiendo como tales, a la estructura de datos apro-

piada para representar un conjunto de elementos cuando las operaciones informáticas son eliminar o desvincular si un elemento informacional pertenece o no a un conjunto de datos. En una tabla de dispersión, los elementos se distribuyen en un conjunto de cubetas (*buckets*), que utilizan una clave y una función de dispersión. En este sentido, la función de dispersión debe considerar la distribución de los elementos de forma homogénea, la determinación del número de cubetas, el número de elementos y el factor de carga en cada cubeta.

Ahora bien, el voto ciudadano ejercido y convertido en sufragio, en un entorno de votación electrónica, se convierte en información electoral, que debe ser registrada y tratada informaticamente mediante tablas de almacenamiento. Este tipo de tablas de almacenamiento se vierten en la memoria principal (disco duro) de la mayoría de prototipos de urnas electrónicas y son alimentadas por los electores cada vez que emiten su sufragio,[36] registrando dicha información aplicando un algoritmo de dispersión que salvaguarda la secrecía del voto público. El almacenamiento informacional se registra simultáneamente en la unidad fija interna de almacenamiento masivo (disco duro) y en la unidad externa de almacenamiento removible (*flash drive*). Cabe aclarar que la información almacenada mediante esta vía es encriptada y fragmentada mediante algoritmos que imposibilitan su manipulación (véase gráfica 2).

[36] Fuente: Instituto Electoral y de Participación Ciudadana del Estado de Coahuila.

Gráfica 2

Tabla de almacenamiento de registro de información, aplicando algoritmo de dispersión[37]

	Código	*Gobernador*	*Diputados*	*Ayuntamientos*
1	0	0	0	3
2	0	0	0	0
3	0	0	0	0
4	X	0	0	0
5	0	0	0	0
6	0	5	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	3	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0

IX. Subsistema para la totalización de resultados electorales

La autoridad electoral debe considerar inicialmente si la urna electrónica debe contener un módem que le permita conectarse a una red informática pública o privada, con sus inherentes aristas en cuanto a seguridad, o bien, los módulos de grabación electrónica directa deben constituir elementos informáticos aislados de una red, y que la transmisión de los resultados electorales debe acontecer por otra vía. Estas premisas básicas dan pauta a la implementación de un subsistema para la totalización de los resultados electorales.

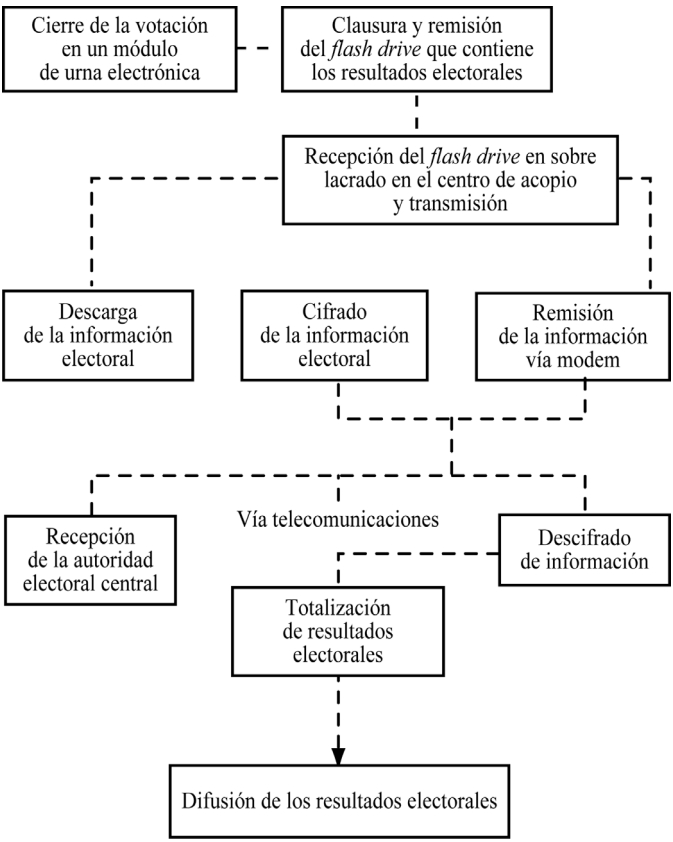
37 *Idem*.

La experiencia internacional, particularmente la brasileña, ha optado por la segunda vía, esto es, la integración de la *flash card* (soporte magnético que contiene los resultados electorales de una casilla) en un sobre electoral lacrado por los funcionarios electorales, que se remite a un centro de acopio electoral y de transmisión de los resultados electorales. El procedimiento técnico-electoral que opera en los centros de transmisión tiene su punto de partida en descargar la información electoral receptada en un ordenador, que a partir de un módem y de la conexión a una línea telefónica posibilita transmitir la información electoral.

Sin embargo, el procedimiento tiene una particularidad: los números telefónicos a los cuales se conecta el módem no son conocidos hasta la etapa del cierre de votación, posterior a la jornada electoral, para garantizar un mayor nivel de seguridad en el ámbito de las telecomunicaciones. Este tema tiene vinculación con el *software* electoral aplicativo para la transmisión de información. Los ordenadores que fungen como equipos de transmisión remiten a la autoridad electoral central, la información de los resultados electorales en formato cifrado, que ejecuta un programa para descifrar la información recibida y comunica los resultados a los actores políticos, y principalmente a la ciudadanía. Para una mejor explicitación en el funcionamiento del subsistema para la totalización de los resultados electorales véase la gráfica 3.

Gráfica 3

Funcionamiento del subsistema para la totalización de los resultados electorales



X. AUDITABILIDAD INTEGRAL DEL SISTEMA

Resulta necesaria y completamente deseable la auditabilidad de los subsistemas de voto electrónico. La importancia de la toma de decisiones políticas desahogadas por conducto de la informática y la telemática así lo ameritan, y desde luego bajo el principio electoral de que durante los comicios no debe haber lugar a suspicacia alguna. El propósito de una

acción de auditoría en un subsistema de votación electrónica consiste en determinar y exhibir públicamente su funcionalidad óptima en la emisión y tratamiento de los resultados electorales con la debida certeza. También busca propiciar un nivel de acercamiento y confianza entre el electorado y los partidos políticos en su percepción frente a la nueva tecnología electoral. Las auditorías de igual forma se encaminan a diagnosticar en el voto informático, las eventuales vulnerabilidades del mismo y las medidas para corregirlas.

Podemos sintetizar, de manera general, los siguientes puntos sobre los que deban versar las auditorías que recaigan en los subsistemas de voto electrónico:

a) análisis del código fuente;
b) examen detallado de los programas introducidos en los modelos de urnas electrónicas;
c) compilación de programas informáticos completos;
d) verificación de las funciones específicas que realizan;
e) análisis pormenorizado de las estructuras de datos electorales que procesan;
f) análisis de las herramientas informáticas auxiliares;
g) el examen integral de todos los archivos presentes en los dispositivos de memoria;
h) almacenamiento de la información electoral;
i) verificación de los dispositivos de impresión;
j) análisis de los códigos de votación;
k) revisión de la disociación de la identidad del elector con el sentido de su sufragio, y
l) análisis de las técnicas de criptografía.

De entrada, los procedimientos de auditoría al voto electrónico se podrían verificar en distintos estadios de su implementación:

— En la etapa de diseño y desarrollo de los subsistemas de votación electrónica.
— En la etapa de pruebas en vacío.
— En la etapa de verificabilidad del *hardware* y *software* electoral por los representantes de los partidos políticos.
— En su fase de implementación durante la jornada comicial.

— En el lapso de verificación de los resultados electorales de manera aleatoria y legalmente establecida, en función de un porcentaje respecto a la totalidad de máquinas de grabación electrónica directa utilizadas durante la jornada comicial.
— En la etapa de concentración y totalización de los resultados electorales.
— En la etapa de difusión de los resultados electorales.
— Durante el periodo siguiente a la calificación de las elecciones, específicamente en la conservación y lacrado de módulos de recepción de la votación.

XI. Certificación por autoridades independientes

La seguridad y confianza de la ciudadanía y los actores políticos en el voto electrónico o informatizado para mantener la secrecía del voto público y el respecto irrestricto a la expresión de la voluntad popular conlleva necesariamente a certificar los subsistemas de votación electrónica por autoridades independientes a los organismos electorales que los desarrollan o implementan.

En el plano internacional, esta responsabilidad mayúscula de certificar ha recaído en universidades públicas de prestigio; sin embargo, esta actividad de certificación no es limitativa a instituciones educativas, ya que también se puede extender o tras instituciones de manera colegiada. Por ejemplo, en Brasil se certifican rubros relacionados con el análisis del código fuente, múltiples simulaciones de elecciones utilizando los programas introducidos en sus modelos de urnas electrónicas, compilación de programas completos y verificación de las funciones específicas que realizan, análisis detallados de las estructuras de datos electorales que se procesan, interrupciones forzadas, reinicio de programas informáticos vertidos en circunstancias poco comunes que ocurrieran durante la jornada electoral, examen integral de todos los archivos presentes en los dispositivos de memoria, entre otros.

Recordemos que un elemento nodal en el proceso de certificación que puede propiciar certeza electoral debe ser la generación y preservación de pruebas físicas que hagan constar la intención de voto del elector. Esta premisa básica de certificación conlleva a utilizar periféricos de impresión dentro de la votación electrónica, los cuales fungen como meca-

nismo de respaldo para el recuento de votación y la garantía de exactitud en su tratamiento informatizado.

En Estados Unidos, debido a múltiples irregularidades en la instauración del voto electrónico se han implementado una serie de estándares técnicos para certificar sistemas informáticos que recogen el voto público. Es preciso señalar que las instancias encargadas de certificar un subsistema de votación electrónica, en forma previa deben iniciar un proceso de colecta de información que deben proporcionar las autoridades electorales que deciden implementar el voto electrónico, así como del *hardware*, *software* electoral y soportes digitales a utilizarse. Cabe citar que estas actividades previas deben emprenderse con mucha anticipación.

A continuación, estos pueden ser algunos de los puntos principales a certificarse en materia de voto electrónico:

a) análisis del flujo de información electoral que se procesa mediante votación electrónica;
b) procedimientos realizados por el subsistema de votación;
c) análisis del *hardware*;
d) examen de los microprogramas;
e) análisis integral del *software* electoral;
f) estudio detallado del proceso de totalización de resultados electorales;
g) examen de herramientas auxiliares;
h) análisis de los procedimientos para introducir los programas informáticos a utilizase durante la jornada comicial;
i) pruebas en vacío y análisis operacionales;
j) estudios sobre la seguridad en redes informáticas para la totalización de resultados electorales;
k) análisis de técnicas criptográficas incorporadas;
l) examen de los sistemas de soporte a implementarse durante la jornada electoral;
m) examen de los componentes principales de los módulos de recepción de la votación;
n) distribución del *software* electoral en bloques dentro del módulo de recepción de la votación;
ñ) escrutinio minucioso sobre desenvolvimiento del código fuente;
o) estudios acerca del proceso de compilación e integración del código fuente;

p) análisis sobre la verificación de archivos, y
q) examen en torno a los sistemas operacionales de los módulos de votación.

En este sentido, Brunazo Filho expresa que la integridad y robustez de un subsistema de votación electrónica se acredita después de los procesos de auditabilidad y certificación por autoridades independientes. La referida integridad se proyecta finalmente en el correcto escrutinio y cómputo de la votación que refleje fielmente la voluntad popular.

XII. Seguridad informática

Referirnos a la seguridad de un sistema informático nos remite a la percepción de que se encuentra exento de amenazas, daños o riesgo alguno. En este contexto, objetivamente, para determinar si un sistema informático es completamente seguro se tienen que cumplimentar las siguientes condiciones básicas:

a) La integridad del sistema, que implica la inalterabilidad de la información; es decir, la información no puede ser alterada por usuarios no autorizados.
b) La confidencialidad; esto es, sólo puede y debe ser legible para usuarios acreditados.
c) La disponibilidad de la información, que puede ser utilizable en cualquier momento.
d) El no repudio o rechazo; es decir, que quien ha realizado una transacción no puede negar después que no fue quien la efectuó.

En el lenguaje de la informática, dependiendo de la fuente de riesgos o amenazas, la seguridad puede clasificarse en seguridad lógica y seguridad física.

Ciertamente, estas condiciones básicas de seguridad informática se tienen que trasladar al ámbito de la votación electrónica, para conseguir fundamentalmente que el sufragio ciudadano traducido en resultados electorales, y convertido en información electoral, se garantice la integridad de la votación, evitándose, mediante la seguridad informática, su alteración, sustracción o destrucción. Asimismo, la seguridad informática

se complementa con una política de seguridad de la organización; en este caso, la que define la autoridad electoral.

Además, la seguridad informática la podemos categorizar en seguridad activa y seguridad pasiva. Por una parte, la seguridad activa se vincula con técnicas de criptografía, monitorización de la red, herramientas de comprobación, políticas de seguridad, documentos de seguridad en el nivel técnico, organizativo y jurídico, entre otros. Por otra parte, la seguridad pasiva se relaciona con políticas de *backups* o respaldos de seguridad (respaldo de seguridad, respaldo y restauración, y copia de seguridad).

En síntesis, la seguridad informática, particularmente la seguridad de la información electoral, describe todas las medidas para prevenir el uso no autorizado de datos disponibles en forma electrónica. Una de las medidas especiales para proveer esta seguridad son los criptosistemas.

Criptografía

La criptografía se define como la ciencia encargada de diseñar funciones o dispositivos capaces de transformar mensajes legibles o en claro a mensajes cifrados, de tal manera que esta transformación (cifrar) y su transformación inversa (descifrar) sólo pueden ser factibles con el conocimiento de una o más llaves. En la actualidad, la criptografía tiene múltiples aplicaciones en las telecomunicaciones, particularmente la telefonía celular, en cuestiones relacionadas con redes públicas, actividades de comercio electrónico, dinero electrónico, y recientemente ha migrado su aplicación a asuntos vinculados con el almacenamiento seguro de grandes cantidades de información digital. Este último uso de la criptografía nos conduce al almacenamiento y transmisión de información electoral basada en técnicas de criptografía, siendo éste un punto crucial de seguridad informática dentro de la votación electrónica.

En términos de la criptografía, la información original que debe resguardarse se denomina texto en claro o plano (*plaintext*). El cifrado es el proceso de convertir el texto plano en una serie de datos ilegibles, denominado texto cifrado o criptograma (*ciphertext*), mediante la aplicación de un algoritmo cuya entrada es una cadena de bits conocida como llave. Por lo general, la aplicación concreta del algoritmo de cifrado (también llamado cifra) se basa en la existencia de una clave; esto es, información

secreta que adapta el algoritmo de cifrado para cada uso distinto. Las dos técnicas básicas de cifrado en la criptografía clásica son:

a) La sustitución. Acción que supone el cambio de significado de los elementos básicos del mensaje a cifras.
b) La transposición. Acción que establece una reordenación de las cifras.

El descifrado es el proceso inverso que recupera el texto plano a partir del criptograma y la clave. El protocolo criptográfico especifica los detalles de cómo se utilizan los algoritmos y las claves para conseguir el efecto deseado. El conjunto de protocolos, algoritmos de cifrado, procesos de gestión de claves y actuaciones de los usuarios estructuran lo que se denomina criptosistema.

Existen dos grandes grupos de cifras: los algoritmos que utilizan una clave única tanto en el proceso de cifrado como en el de descifrado, y los que utilizan una clave para cifrar mensajes y una clave distinta para descifrarlos. Los primeros se denominan cifras simétricas o de clave simétrica, y son la base de los algoritmos de cifrado clásico. Los segundos se denominan cifras asimétricas, de clave asimétrica o de clave pública y clave privada, y forman el núcleo de las técnicas de cifrado modernas.[38]

Una explicación puntual de las técnicas de cifrado es la ofrecida por el profesor Miguel Morales. Al respecto, refiere que un criptosistema consta de los elementos (M, C, K, E, D).

En donde:

M = representa el conjunto de todos los mensajes sin cifrar (texto plano).
C = representa el conjunto de todos los posibles mensajes cifrados.
K = representa el conjunto de claves que se pueden emplear en el criptosistema.
E = es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de *M* para obtener un elemento de *C*.
D = es el conjunto de transformaciones de descifrado, análogo a *E*.

38 Morales Sandoval, Miguel, *Notas sobre criptografía*, México, INAOE, 2003, p. 2.

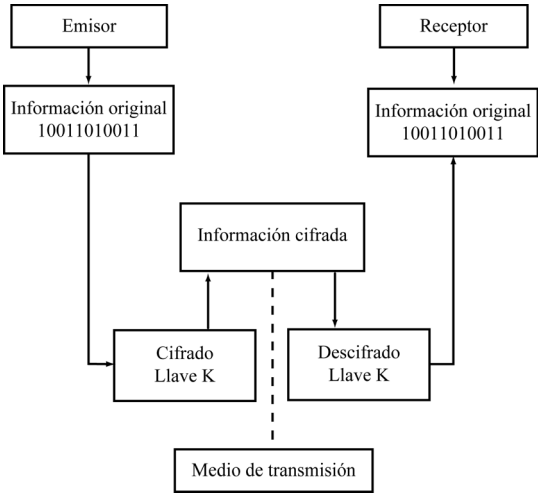
Los criptosistemas pueden dividirse en dos clases: criptosistemas simétricos (llave simétrica) y criptosistemas asimétricos, conocidos comúnmente como criptosistemas de llave pública.

a) Criptografía de llave simétrica

Los criptosistemas de llave simétrica solamente ofrecen el servicio de confidencialidad. En estos sistemas se emplea una misma llave k tanto para cifrar como para descifrar la información. Esta llave sólo es conocida tanto por el emisor como por el receptor, y ambos deben salvaguardarla. La desventaja de los criptosistemas de llave privada es que la llave para cifrar y descifrar debe estar tanto en el emisor como en el receptor, por lo que la llave debe transmitirse de forma segura previamente a realizar las operaciones de cifrado y descifrado. Bajo este esquema, al transmitir la llave por un canal inseguro, la llave puede interceptarse y poner en riesgo la integridad de los datos. Estos criptosistemas aún se utilizan, debido a que procesan los datos más rápido que los criptosistemas asimétricos (véase figura 3).[39]

Figura 3

Esquema de operación del cifrado en criptografía de llave privada



39 *Ibidem*, p. 2.

b) Criptografía de llave asimétrica

La criptografía de llave asimétrica fue propuesta por Whit Diffie y Martin Hellman en 1976. Bajo este esquema, se emplean dos llaves, una de carácter privado y una de carácter público. La llave pública se utiliza para cifrar la información, y solamente la llave privada podrá descifrarla. La llave pública del receptor es del conocimiento de cualquier entidad emisora que quiera enviar información cifrada. La llave privada es conocida y salvaguardada únicamente por el receptor. En los criptosistemas de llave pública se debe asegurar que el conocimiento de la llave pública no permitirá obtener la llave privada. Los criptosistemas de llave asimétrica ofrecen mayores niveles de seguridad que los criptosistemas simétricos; adicionalmente, tienen la ventaja de que la llave pública es la única que se transmite por el canal inseguro. La desventaja que presentan es que son más lentos comparados con los criptosistemas simétricos. Con criptografía de llave pública es posible ofrecer el servicio de confidencialidad, autenticación, integridad y no repudio. El servicio de confidencialidad se logra con el cifrado, ya que únicamente el receptor puede descifrar la información con su llave privada. Debido a que cualquiera puede tener acceso a la llave pública del receptor, no se asegura que el emisor sea quien dice ser (véase figura 4). Con el algoritmo de firma digital se logran los servicios de autenticación, integridad y no repudio.[40]

La firma digital es una operación análoga a la firma escrita. El esquema de operación es similar al proceso de cifrado, sólo que las llaves pública y privada son invertidas; es decir, la llave privada se emplea para generar la firma del mensaje, y la llave pública se utiliza para verificar dicha firma. La autenticación y el no repudio se consigue porque únicamente el emisor pudo firmar el mensaje, ya que él es el único que posee su llave privada.

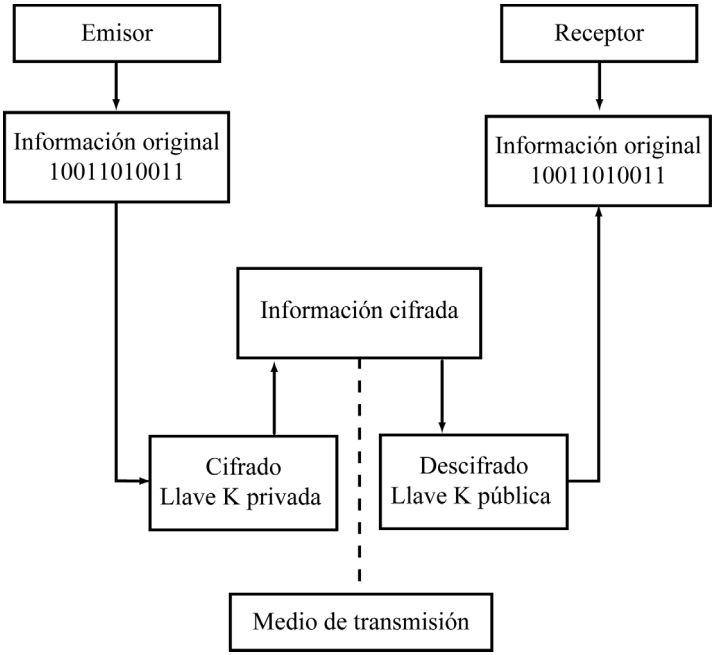
La integridad de los datos se consigue aplicando una función *hash* a los datos que se van a transmitir. La salida de la función *hash* se conoce como el resumen del mensaje, y puede verse como la huella digital del mensaje a transferirse. El resumen del mensaje es el que se cifra con la llave privada del emisor, y se transmite junto con el mensaje original. El receptor aplica la misma función *hash* al mensaje original y descifra el mensaje mediante la llave pública del emisor. Entonces compara la infor-

40 *Ibidem*, p. 2.

mación descifrada con la salida de la función *hash*; si ambas son iguales, los datos no fueron modificados, y se sabe que el emisor es realmente quien dice ser. Si son diferentes, los datos han sufrido alteración durante la transferencia, y la firma no es válida (véase figura 5).[41]

Figura 4

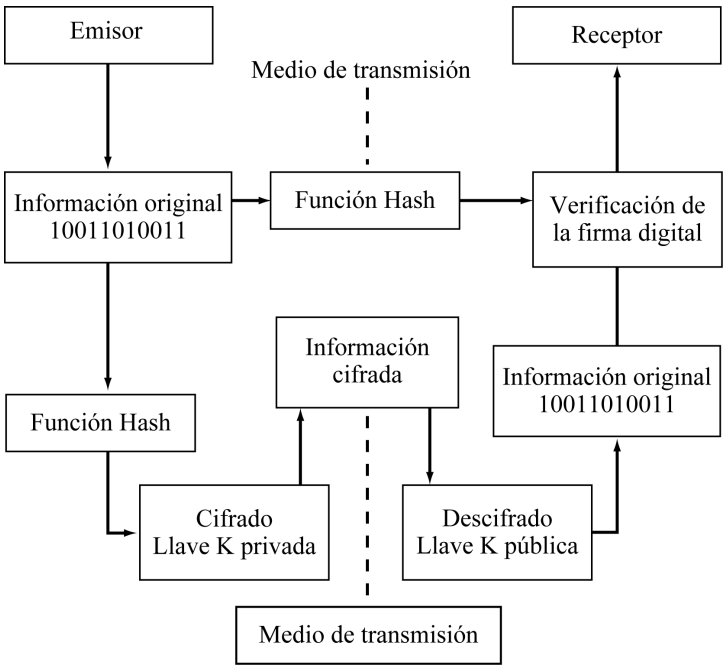
Esquema de operación del cifrado en criptográfía de llave pública



41 *Ibidem*, p. 3.

Figura 5

Esquema de operación de la firma digit



XIII. Registro de candidatos y diseño de boletas electorales virtuales

En la etapa de actividades preparatorias de la elección se debe contemplar como una actividad específica de los organismos electorales interactuando con los partidos políticos y los candidatos a puestos de elección popular, el diseño de las boletas electorales virtuales, que implicaría la aplicación del voto electrónico. En esta actividad, una vez registrados los candidatos por los distintos partidos políticos, la autoridad electoral debe abrir un espacio de tiempo prudente para incorporar las distintas candidaturas que aparecerían en la interfaz que se le presenta al electorado.

Este procedimiento electoral se vincula directamente con los aspectos relativos a la documentación electoral, al ser sustituidas las boletas electorales tradicionales en papel por una interfaz, que se presenta de manera visual al elector.

En este sentido, el órgano de dirección de la autoridad electoral, como una atribución específica, debería establecer y aprobar el modelo de boleta electoral virtual electrónica que se autorizaría para una elección, haciéndolo del conocimiento de los entes partidarios.

Asimismo, debe ser previsible el establecimiento de procedimientos especiales para modificar el diseño y plazos de la boleta electoral virtual o digital, cuando se cancele el registro de candidaturas o exista sustitución de los candidatos cuando ya se encontraran configuradas, no siendo posible su modificación, una vez que el *software* electoral se haya cargado a los módulos receptores de la votación.

XIV. Soporte técnico durante la jornada electoral

La autoridad administrativo-electoral, como una medida de seguridad informática en el aspecto técnico y organizacional del voto electrónico, debe considerar toda una serie de actividades de soporte técnico durante el día de la jornada electoral. Recordemos que gran parte de los funcionarios electorales, independientemente de una buena capacitación técnica y electoral para desarrollar las funciones electorales, siempre tendrán algún tipo de dudas o contratiempos de carácter técnico, que resulta vital atender oportuna y diligentemente por personal informático. Desde luego que esta necesidad de orden técnico se traduce en la imperiosa necesidad de contar con personal que brinde asistencia técnica durante los comicios.

En la experiencia internacional, muchas de las fallas que han trascendido en esquemas de votación electrónica se originan principalmente por factores de error humano, y no necesariamente por cuestiones técnicas, que de haberse atendido oportunamente por personal capacitado se reduciría sensiblemente la percepción ciudadana de falibilidad del voto electrónico. Ahora bien, como se ha mencionado en el tema relativo al código fuente tratado con anterioridad, la autoridad electoral debe prever que si integra *software* electoral con núcleo GNU/Linux requerirá de personal técnico altamente capacitado que brinde asistencia oportuna y además adecuada.

XV. Algunos aspectos de la votación telemática

1. *TCP/IP*

El TCP/IP es un conjunto de comunicaciones de datos. Estos protocolos permiten rutear la información mediante redes informáticas de un ordenador a otro posibilitando la entrega de correo electrónico, noticias, e incluso el uso de capacidades de registro de información remota. El nombre TCP/IP se refiere a dos protocolos principales: el Protocolo de Control de Transmisión y el Protocolo Internet.[42] No obstante, existen múltiples protocolos que operan a partir de TCP/IP y que ofrecen distintos servicios.

En cada ordenador conectado a una red pública o privada se establece una dirección específica para que la información sea remitida con éxito. Este procedimiento es el que se encuentra controlado por el Protocolo Internet (IP). En cada ordenador, al contar con su dirección IP, ésta se subdivide en dos partes. La primera parte es una porción de red, y se usa para describir la dirección de un anfitrión, y la segunda parte es la porción de anfitrión que se utiliza para establecer su identidad.

El TCP/IP como conjunto de protocolos, puede ofrecer distintos servicios. Entre estos servicios se encuentra la transmisión de información electoral, específicamente los resultados electorales, trátese de votación telemática para el registro remoto de información o en el caso de votación electrónica presencial para la transmisión y totalización de los resultados comiciales que puedan verificarse a través de una dirección IP de carácter reservado.

En la votación electrónica remota o a distancia, la transmisión de la información electoral está regulada por la autoridad electoral, que es la instancia que determina quién funge como administrador del sistema de votación telemática, y establece la configuración del mismo.

2. *Niveles de seguridad*

Los estándares de seguridad en ordenadores y redes informáticas que han sido elaborados durante algún tiempo por el Departamento de De-

42 Hare, Chris *et al*., *Internet y seguridad en redes*, México, Prentice-Hall Hispanoamericana, 1995, p. 9.

fensa de los Estados Unidos. Estos criterios se han establecido para evaluar los distintos niveles de seguridad para proteger de ataques al *hardware*, al *software* y a la información resguardada. A los referidos criterios se les conoce comúnmente como el "Libro Naranja".

La pertinencia de crear el "Libro Naranja" obedece a la necesidad de considerar los distintos niveles de seguridad física de los ordenadores, la autenticación del usuario, confiabilidad del *software* tanto del sistema operativo como de las aplicaciones del usuario; esto incluye a las redes informáticas.

En el caso de votación electrónica, por la trascendencia de la información electoral que se procesa, el nivel de seguridad deseado debe ser del tipo "A". El nivel de seguridad tipo "A" es el nivel más elevado de seguridad informática validado, el cual incluye un proceso exhaustivo de diseño, control y verificación del *software*. Un diseño informático requiere ser verificado en forma matemática, además de realizar un análisis de los canales de distribución confiable. En cuanto a distribución confiable, significa que el *hardware* y el *software* han estado protegidos durante su expedición para evitar violaciones a los sistemas de seguridad (véase apartado XII, "Seguridad informática").

3. *Archivos* password

Karanjit Siyan establece que la primera línea de defensa en contra del acceso no autorizado a un sistema es el archivo *password*; pero este autor también expresa que resulta paradójicamente el punto más débil del mismo. Por tanto, para mantener niveles de seguridad robustos es factible encriptar la contraseña, utilizando el archivo *shadow password*, el cual ofrece algunas ventajas adicionales de seguridad. Sólo el administrador de un sistema de archivo *shadow password* puede crearlo, y permite colocar la contraseña encriptada en un archivo al que no tienen acceso los usuarios normales, lo cual reduce la posibilidad de sustraer la contraseña.

La caducidad de la contraseña brinda un nivel adicional de seguridad. Este mecanismo controla en qué momento pueden los usuarios cambiar sus contraseñas mediante la inserción de un valor en un archivo de contraseña después de la contraseña encriptada. Este valor define el periodo mínimo de tiempo que debe pasar antes de que los usuarios puedan cambiar sus contraseñas, y el periodo máximo de tiempo que pueda transcurrir antes de que la contraseña expire.

La autoridad electoral, al diseñar un subsistema de voto electrónico, debe considerar además de contraseñas y técnicas de criptografía, múltiples barreras de protección. En este rubro es importante que asuma y entienda con exactitud qué recursos debe proteger si desea utilizar una red para transmitir información electoral, y qué servicios desea proteger. A esto se le llama "política de red". Una política de red, según Chris Hare, es un documento que describe los asuntos de seguridad de red en una organización, el cual constituye el primer paso para construir barreras de protección efectivas. Las políticas de red regulan asuntos relacionados con:

a. La planeación de seguridad en la red;
b. Política de seguridad en sitios;
c. Análisis de riesgos;
d. Identificación de recursos y amenazas;
e. Uso de la red;
f. Responsabilidad, y
g. Planes de acción cuando la política de seguridad ha sido violada.

4. *Enrutadores de selección*

Es preciso señalar que una de las mayores preocupaciones en la transmisión de los resultados electorales mediante redes son los accesos no autorizados que eventualmente alteren, modifiquen o sustraigan información electoral causando daños irreparables. En razón de lo que precede, la seguridad, si es que se decide utilizar redes para transmitir información resultante de los comicios, es un asunto nodal que deben prever los organismos electorales. En virtud de lo anterior, se debe poner especial énfasis en lo siguiente:

— identificación de zonas de riesgo en la red;
— pertinencia de utilizar enrutadores de selección que permitan servicios de filtración de paquetes;
— evaluación de *reuters* como medio de comunicación que implique evaluación física, enlace de datos, red, transporte y aplicación;
— filtro de conexiones entrantes y salientes, y
— filtro de partes entrantes y salientes.

5. *Barreras de protección*

En los puntos analizados con anterioridad, la arquitectura de las redes es una parte importante; no obstante, la implementación de barreras de protección mediante herramientas de *software* complementan las consideraciones de seguridad que sobre redes informáticas debe observar la autoridad electoral.

La barrera de protección más común es la compuerta Firewall, que actúa como enrutador seguro entre la red interna y la red externa de una organización, misma que remite el tráfico no confiable a dicha compuerta. Firewall incluye dos componentes principales: módulos de filtro de paquetes y módulos de control. El módulo de control, generalmente se coloca en la estación de trabajo, y puede localizarse en el mismo anfitrión o en uno distinto. El módulo de filtro de paquetes implanta las funciones de un enrutador seguro entre las redes, y está entre las capas de enlaces de datos y de red.

Entre la arquitectura de un módulo de control Firewall se encuentran los siguientes componentes:

— Administrador de objetos en red,
— Administrador de servicios,
— Administrador de reglas, y
— Visor de registro.

XVI. Plan de contingencia electoral

Es más que conveniente, sino que muy prudente, crear e implementar planes de contingencia en materia de voto electrónico debido a problemas de funcionamiento de los equipos de cómputo, interrupciones o falta de suministro de energía eléctrica o situaciones imprevistas. Entre los planes de contingencia a considerar se encuentra la posibilidad de que los organismos administrativo-electorales autoricen la impresión de un porcentaje de boletas electorales tradicionales (papel) para salvaguardar el derecho de voto activo de la ciudadanía ante eventualidades de orden técnico. Desde luego, este rubro se encuentra íntimamente relacionado con el aspecto inherente al soporte técnico durante la jornada comicial, capacitación de personal informático y los respaldos de seguridad en la información.