

Proceso Técnico Operativo del Voto Electrónico por Internet para Mexicanos Residentes en el Extranjero

1. El presente proceso técnico operativo es de observancia general y de carácter obligatorio para el Instituto Nacional Electoral, así como para las personas que participen en la organización, implementación, operación y evaluación del Voto Electrónico por Internet de los Mexicanos Residentes en el Extranjero, en las elecciones que, de acuerdo a la normatividad vigente, lo permitan.
2. El presente proceso tiene por objeto establecer y describir las fases que rigen la operación del Voto Electrónico por Internet para Mexicanos Residentes en el Extranjero, debiendo cumplirse cada una de ellas en el orden señalado y bajo los procedimientos que en el presente proceso se establecen.
3. Adicionalmente a las definiciones contenidas en el numeral 3 de los Lineamientos para el desarrollo del sistema que considere los mecanismos y procedimientos del voto electrónico por Internet para mexicanos residentes en el extranjero, para los efectos del presente Proceso Técnico Operativo, se entiende por:
 - a) **Administrador del Sistema:** representante de la UNICOM responsable de la instalación y configuración del Sistema, así como del manual de configuración del mismo.
 - b) **Administrador del HSM:** representante de la UNICOM encargado de la inicialización y operación de los HSM, así como del manual de configuración del mismo.
 - c) **Coordinador:** responsable de la implementación del Sistema.
 - d) **Fedatario:** notario público que da fe de los actos de los que es testigo.
 - e) **Hash:** es un valor o código de representación único que permite identificar a cada archivo digital. Dicho hash o código es obtenido a partir de algún algoritmo criptográfico denominado comúnmente funciones hash. Ejemplos de funciones hash son SHA256 y MD5.

- f) **Manual de configuración del Sistema:** documento que contiene los datos de la elección y las instrucciones para la configuración del Sistema; de manera enunciativa más no limitativa, este manual debe contener el cargo a elegir, partidos políticos, candidaturas independientes, figuras de participación de los partidos políticos (coalición, candidatura común, entre otros), nombre de los candidatos, periodo de votación y número máximo de Votantes.
 - g) **Operador del Sistema:** personal de la UNICOM que operará la infraestructura tecnológica del Sistema.
 - h) **UNICOM:** Unidad Técnica de Servicios de Informática del Instituto.
 - i) **VeMRE:** Voto electrónico por Internet para Mexicanos Residentes en el Extranjero.
 - j) **Votante:** ciudadano mexicano que emitirá su voto desde el extranjero utilizando el Sistema.
4. El proceso técnico operativo del VeMRE, consta de las siguientes fases:
- a) **Sesión de creación de la Llave criptográfica,** esta fase corresponde al evento en el cual el Comité Electoral, en presencia del Fedatario, se reúne con el objetivo de generar la Llave criptográfica que será utilizada para brindar seguridad a la información en el Sistema durante su operación.
 - b) **Apertura del Sistema,** esta fase comprende las actividades a realizar para configurar el Sistema con la información de las elecciones que corresponda, en presencia del Fedatario, quien además validará que la versión del sistema corresponde a la versión que cuenta con el dictamen y que las bases de datos no contienen votos. Esta fase concluye con el inicio de operación del Sistema.
 - c) **Autenticación del Votante,** esta fase describe el procedimiento a seguir por el Votante para ingresar al Sistema durante el periodo de votación correspondiente.
 - d) **Monitoreo del Sistema,** las actividades operativas a realizar durante el periodo que el Sistema se encuentra en operación se describen en esta fase.
 - e) **Cierre del Sistema,** esta fase comprende las actividades a realizar para descargar la base de datos que contiene los votos cifrados y calcular su

hash, una vez que el sistema haya cerrado operaciones en la fecha establecida.

- f) **Sesión de descifrado y cómputo de los votos**, en esta fase el Comité Electoral sesionará para habilitar el uso de la Llave de apertura de votos y con esto realizar el descifrado y cómputo de la elección.
 - g) **Resguardo y preservación de la información**, en esta fase el Comité Electoral y el Administrador del Sistema entregan al Fedatario, las tarjetas inteligentes y toda la información generada por el Sistema, para continuar con el proceso de resguardo y preservación de las mismas.
5. Para los casos no previstos en el presente proceso técnico operativo, el Secretario Ejecutivo por conducto del titular de la Unidad Técnica de Servicios de Informática del Instituto tendrá la facultad de tomar las decisiones que correspondan, debiendo en todo momento informar a los integrantes del Consejo General.

De la Sesión de creación de la Llave criptográfica

6. Esta fase inicia con la participación de las siguientes figuras:
- a) Los integrantes del Comité Electoral,
 - b) El Fedatario,
 - c) El Administrador del HSM, y
 - d) El Coordinador.
7. El Administrador del HSM, teniendo como límite el número máximo de tarjetas inteligentes permitidos por la tecnología del HSM, hará entrega a cada uno de los integrantes del Comité Electoral:
- a) Una tarjeta inteligente, que será utilizada durante la creación y repartición de la Llave criptográfica;
 - b) Un formato de acuse de recepción, para personalizar la entrega de la tarjeta inteligente, y
 - c) Una hoja de papel opaco, donde escribirá su contraseña personal.

8. Cada integrante del Comité Electoral firma y entrega al Administrador del HSM el acuse de recepción correspondiente.
9. Cada integrante del Comité Electoral escribe de forma confidencial su contraseña personal en el papel opaco proporcionado.

Es responsabilidad de los integrantes del Comité Electoral mantener en secreto la contraseña. Esta contraseña será requerida por el HSM cada vez que se necesite utilizar la tarjeta inteligente que queda a su resguardo.

10. El Administrador del HSM ejecuta los procesos de configuración en el HSM para la creación, almacenamiento y repartición de la Llave criptográfica. El Fedatario valida que la ejecución de los pasos se realiza en el orden y con la información adecuada, resguardando la evidencia de la ejecución de este proceso.
11. Cada integrante del Comité Electoral introduce al HSM la tarjeta inteligente que tiene a su resguardo, ingresa su contraseña y retira la tarjeta inteligente del HSM.

Una vez que los integrantes del Comité Electoral hayan realizado el proceso anterior, tanto la Llave de la elección como la Llave de apertura de votos habrán sido creadas y almacenadas en el HSM. Asimismo, la información que protege la bóveda en donde se guarda la Llave de apertura de votos queda repartida entre los integrantes por medio de las tarjetas inteligentes.

12. El Coordinador entrega el acta circunstanciada de hechos con las actividades realizadas en la Sesión de la creación de la Llave criptográfica, misma que firman los integrantes del Comité Electoral y el Administrador del HSM, acto que clausura la sesión del Comité.

De la Apertura del Sistema

13. El Administrador del Sistema entrega al Fedatario el dictamen emitido al Sistema y el manual de configuración del Sistema para la verificación de las actividades.
14. El Administrador del Sistema obtiene el hash del Sistema a utilizar y la muestra al Fedatario; éste último verifica que el hash obtenido coincide con la documentada en el dictamen.
15. El Administrador del Sistema realiza la configuración dentro del Sistema de los datos de la elección que se trate, y los muestra al Fedatario para que este los coteje con los asentados en el manual de configuración del Sistema.

16. El Administrador del Sistema obtiene un reporte inicial del Sistema para verificar que la base de datos no contiene votos y que los contadores están inicializados en cero. El Fedatario revisa dicho reporte.
17. El Sistema queda habilitado para permitir el acceso a los Votantes a partir de la fecha y hora que para tales efectos se haya establecido en la configuración del mismo Sistema.

De la Autenticación del Votante

18. Esta fase tiene por objeto verificar la identidad del Votante. Para que el Votante pueda emitir su voto, deberá realizar el procedimiento de autenticación en el Sistema, a través de un equipo de cómputo.
19. Con el objeto de que el Votante pueda realizar el procedimiento de autenticación, el Instituto le deberá proveer lo siguiente:
 - a) Un nombre único de usuario;
 - b) Una contraseña, la cual será enviada a través de la cuenta de correo electrónico que proporcionó en su solicitud de inscripción ante la LNERE;
 - c) Un código de un solo uso o números de identificación, que serán enviados a su teléfono móvil cada vez que el Sistema se lo solicite, y
 - d) La dirección electrónica del Sistema por medio del cual emitirá su voto, misma que se le hará llegar en el manual de uso correspondiente.
20. El Votante deberá ingresar, en el Sistema, su nombre único de usuario, su contraseña y los códigos de un solo uso que el Sistema le solicite, mismos que serán generados y enviados a su teléfono móvil, en cada ocasión.
21. Una vez que el Sistema comprueba que el nombre de usuario, la contraseña y el código de un solo uso corresponden únicamente a la identidad del Votante y son válidos en el momento en que se están utilizando, el Sistema procederá a determinar la ubicación del Votante. Si éste se encuentra fuera del territorio Nacional se le permitirá el acceso al Sistema.
22. El Votante podrá ingresar al Sistema en cualquier momento durante el periodo de votación correspondiente.

Del Monitoreo del Sistema

23. El Operador del Sistema supervisará el estado de todos los componentes tecnológicos involucrados en la operación del Sistema durante el periodo que esté en operación.
24. En caso de presentarse algún incidente durante el periodo de operación del Sistema, el Operador debe avisar al Administrador del Sistema, quien debe supervisar o ejecutar las acciones necesarias para su mitigación.
25. El Administrador del Sistema debe informar del incidente, y las acciones realizadas, al Coordinador.
26. El Administrador del Sistema debe entregar un informe de operación del Sistema al Coordinador, quien a su vez lo entregará al Comité Técnico Asesor.

Del Cierre del Sistema

27. A la fecha y hora de cierre configurada, el Sistema ejecuta, de forma automática, los procedimientos de cierre para concluir la votación por la vía electrónica por Internet.

El cierre del sistema evita que se ingresen votos adicionales y cierra la sesión de aquellos Votantes que en ese momento estén utilizando el Sistema.

28. El Administrador del Sistema ejecuta las instrucciones contenidas en el manual de configuración del Sistema para obtener la base de datos con los votos cifrados de la elección y calcula su hash. Dicha base de datos se transfiere al equipo de cómputo de la sede, preparado para llevar a cabo el descifrado y cómputo correspondiente.

De la Sesión de descifrado y cómputo de los votos

29. A las 18:00 horas del día de la Jornada Electoral, tiempo del centro de la República Mexicana, se reúne el Comité Electoral, el Fedatario, el Administrador del HSM, y el Coordinador en la sede que haya establecido el Consejo General para llevar a cabo la sesión de descifrado y cómputo de los votos.

30. El Coordinador explica al Fedatario y a los integrantes del Comité Electoral la forma en que se ejecutará un sorteo, para seleccionar de manera aleatoria a un determinado número de integrantes del Comité Electoral. Acto seguido el Coordinador realiza el sorteo.

31. El Administrador del HSM solicita a los integrantes del Comité Electoral seleccionados, que introduzcan la tarjeta inteligente que tienen a su resguardo, así como la contraseña personal en el dispositivo HSM.

Con la información de las tarjetas se abre la bóveda, en el HSM, que resguarda la Llave de apertura de votos.

32. El Administrador del HSM calcula y compara el hash de la base de datos con los votos cifrados, con el hash obtenido a través del Sistema, y ejecuta las instrucciones necesarias para que inicie el proceso de descifrado haciendo uso la Llave de apertura de votos.

33. Se procesa el cómputo y al término el Administrador del HSM imprime el acta con el resultado de la votación electrónica por Internet de la elección.

34. Los integrantes del Comité Electoral firman el acta de cómputo de la votación electrónica por Internet.

35. El acta con la votación electrónica por Internet se entrega:

- a) Para las elecciones federales, al personal del Instituto designado previamente por la Junta General Ejecutiva para realizar la suma de los resultados consignados en las actas de escrutinio y cómputo de las respectivas mesas, y con ello obtener el resultado de la votación emitida en el extranjero, y
- b) Para las elecciones locales, al Secretario Ejecutivo del Instituto, quien a su vez lo hará llegar al Secretario Ejecutivo del OPL.

Del Resguardo y Preservación de la Información

36. El Administrador del HSM obtiene el hash de al menos los siguientes archivos digitales en el equipo de cómputo de la sede:

- a) La base de datos con los votos descifrados;

- b) Las bitácoras generadas por el Sistema, y
- c) Cualquier otro documento generado por el Sistema.

Imprime un documento que contenga todas las Huellas digitales, incluyendo la de la base de datos con los votos cifrados, y lo entrega al Fedatario.

- 37. El Coordinador entrega a los integrantes del Comité Electoral un sobre y les solicita depositen dentro de éste la tarjeta inteligente que tienen en su posesión, así como la hoja de papel opaco con su contraseña.
- 38. Los integrantes del Comité Electoral sellan el sobre y lo rubrican, posteriormente entregan el sobre sellado y rubricado al Fedatario.
- 39. El Administrador apaga el equipo de cómputo de la sede, extrae el disco duro y lo entrega al Fedatario.
- 40. El Fedatario custodia los sobres, el documento con las Huellas digitales y el disco duro, y los entrega al Coordinador para que éste los traslade a las oficinas de la Secretaría Ejecutiva del Instituto para su resguardo.
- 41. El Coordinador entrega el acta circunstanciada de hechos con las actividades realizadas en la Sesión de descifrado y cómputo de los votos, y en el resguardo y preservación de la información, misma que firman los integrantes del Comité Electoral, el Administrador del HSM y el Coordinador, acto que clausura la sesión del Comité Electoral.

ACUERDO	<p>Acuerdo INE/CVMRE-02SE: 19/10/2016 La Comisión Temporal del Voto de los Mexicanos Residentes en el Extranjero aprueba recomendar a la Junta General Ejecutiva del Instituto Nacional Electoral, posponer la discusión del punto 1.1 del Orden del día de la sesión extraordinaria de fecha 19 de octubre de 2016.</p>
SENTIDO DEL VOTO	<p>Aprobado por mayoría de los Consejeros Electorales, Lic. Enrique Andrade González, Mtro. Marco A. Baños Martínez, y Mtra. Adriana M. Favela Herrera, y con el voto en contra de los Consejeros Electorales, Dr. Ciro Murayama Rendón, y Mtro. Arturo Sánchez Gutiérrez.</p>