ANEXO 3. NOTAS TÉCNICAS

1. Requisitos del sistema para votar electrónicamente

Para poder votar electrónicamente, se necesita un ordenador o dispositivo configurado con las características que se especifican en la matriz de compatibilidad.

Si el ordenador o dispositivo cumple con todos los requisitos, y aun así no puede votar, puede contactar con el teléfono de atención de UMH indicando la incidencia encontrada.

Asistencia al elector: https://cau.umh.es Teléfono: 966 65 85 82

Sitio web: https://juntaelectoral.umh.es/

El Portal de votación es accesible a través de cualquier dispositivo con conexión a Internet a través de un navegador web. El correcto funcionamiento del Portal de votación está garantizado para las siguientes configuraciones:

Ordenador portátil o de sobremesa:

- Windows con:
  - Edge > 43.
  - Chrome > 75.
  - Firefox > 69.

- Mac OS con:
  - Safari > 10.
  - Chrome > 75.

- Ubuntu con:
  - Chrome > 75.

Movil/Tablet

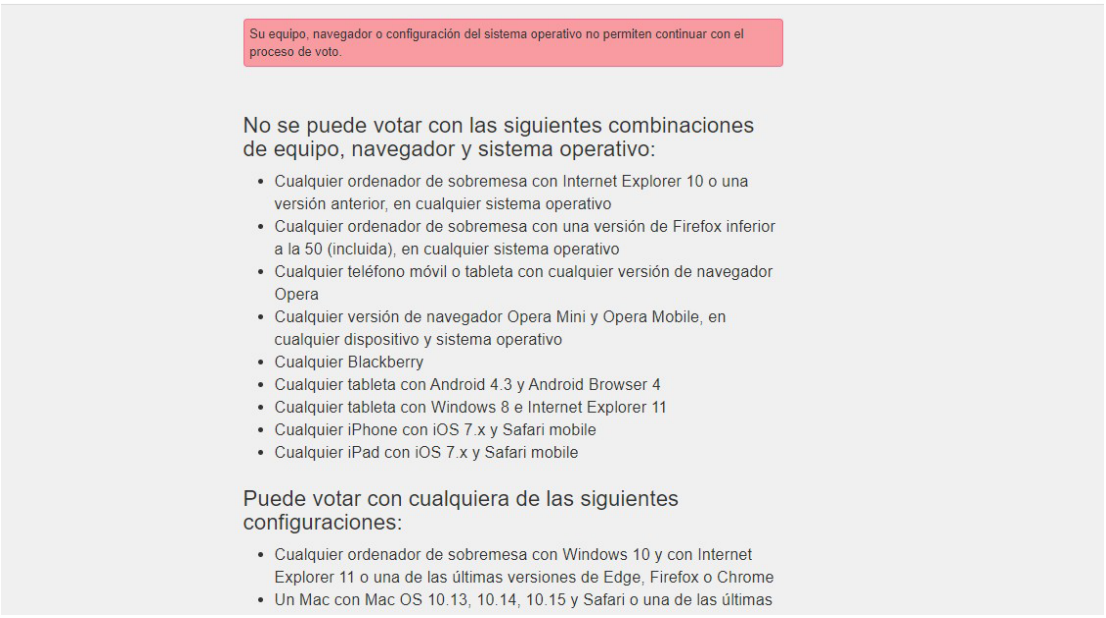
- iOS >12 con:
  - Safari > 10.
  - Chrome >73.

- iOS >13 con:
  - Safari > 10.
  - Chrome >73.

- Android 8.x, 9.x and 10.x con:
  - Chrome > 73

Los navegadores fuera de esta lista no han sido probados por el proveedor del servicio (Scytl), por lo tanto, su compatibilidad no está garantizada.

Hay un conjunto de configuraciones que son claramente incompatibles con el Portal de votación. Para estos casos, el sistema detecta y muestra un mensaje de error como el siguiente:



El Portal de votación ha sido diseñado utilizando guías de accesibilidad y ha sido validado con los siguientes lectores de pantalla:

Escritorio:

- NVDA (Windows 10 - Firefox).
- JAWS 14 (Windows 10 - IE11).

Móvil/Tablet:

- Voice Over (iOS 11.x, 12.x - Safari)

2. Actualizaciones del navegador para el voto electrónico por internet

Las versiones del navegador del ordenador que son compatibles con el Portal de voto son las siguientes:

- Mozilla Firefox (entornos Windows y Linux)

  Para descargar la última versión de Firefox:

  http://www.mozilla.org/es/firefox/new/

- Safari (entorno Mac)

  Para actualizar la versión instalada de Safari:

  http://www.apple.com/es/downloads/

- Google Chrome (entornos Windows y Linux)

  Para descargar la última versión de Google Chrome:

  http://www.google.es/chrome

Si tiene problemas para votar y el sistema operativo que utiliza no aparece en la tabla de compatibilidades, se aconseja que se utilice otro ordenador, móvil o tablet que disponga de alguno de los sistemas operativos compatibles.

3. Activación de JavaScript

Si tiene problemas para votar y el sistema operativo que utiliza no aparece en la tabla de compatibilidades, se aconseja que se utilice otro ordenador, móvil o tablet que disponga de alguno de los sistemas operativos compatibles, en cualquier caso debería tener activado el lenguaje JavaScript.

JavaScript es un lenguaje de programación incorporado en la mayoría de los navegadores que permite realizar algunas operaciones interactivas sin la necesidad de enviar datos al servidor, facilitando la navegación y visualización de páginas de Internet. El Portal de voto utiliza JavaScript en varias operaciones por lo que debe estar activado.

La activación es diferente para cada tipo de navegador:

Mozilla Firefox

1) En la parte superior del navegador, seleccione el botón “Firefox”.

2) Seleccione “Complementos”.

3) Haga clic en la pestaña “Contenidos”.

4) Seleccione la opción “Activar JavaScript”.

5) Haga clic en el botón “OK”.

6) Reinicie el navegador.

Safari

1) Haga clic en el menú “Safari”.

2) Haga clic en la opción “Preferencias”.

3) Haga clic en la opción “Seguridad”.

4) Seleccione la opción “Activar JavaScript” en la sección “Contenido Web.”

5) Cierre la ventana “Preferencias”.

6) Reinicie el navegador.

Google Chrome

1) Haga clic en el icono que muestra tres barras oscuras que se encuentra en la parte superior derecha.

2) Seleccione la opción “Configuración”.

3) A continuación, seleccione “Muestra la configuración avanzada…” al final de la pantalla.

4) En el apartado de privacidad, marque “Configuración del contenido…”

5) En el apartado de JavaScript compruebe que la opción “Permite que todos los lugares ejecuten JavaScript (opción recomendada)” está seleccionada, y si no lo está selecciónela.

6) Reinicie el navegador.

Si el navegador no soporta el lenguaje JavaScript debe utilizar otro navegador que soporte éste lenguaje o tiene que votar desde otro ordenador o dispositivo, ya que JavaScript es imprescindible para poder realizar el proceso de voto de manera segura

4. Garantía en la privacidad de los votantes y en la integridad de los votos. El sistema de Scytl.

El voto electrónico puede ser tan seguro, o incluso más, que el voto tradicional en papel, siempre que se tomen las medidas de seguridad adecuadas.

Las medidas de seguridad convencionales como los cortafuegos o comunicación SSL son necesarias, pero no suficientes para garantizar los requisitos de seguridad específicos del voto electrónico.

Además de estas medidas de seguridad convencionales, la empresa elegida por la UMH, Scytl, implementa una capa de seguridad específica para hacer frente a los riesgos planteados por el voto electrónico, garantizando así el cumplimiento de los requisitos en toda elección, como la privacidad del votante, la integridad del voto y la posibilidad de verificación por parte de los votantes del tratamiento correcto del voto.

Cuando se accede al Portal de voto se utiliza una conexión HTTPS, lo que implica que el servidor se autenticará con un certificado digital ante su navegador web. Si todo es correcto, podrá acceder al Portal de voto sin ninguna notificación de error y el navegador normalmente mostrará un candado cerrado o un icono similar para indicarlo.

Por otro lado, si aparece una ventana de alarma en el navegador indicando que el certificado digital del sitio no coincide con la dirección donde se conecta (o mensajes similares) es posible que esté accediendo a un portal falso. En este caso, por favor, contacte con el equipo de soporte para notificarlo.

El producto de Scytl proporciona **seguridad de extremo a extremo** (end-to-end) a todos los votantes, evitando así el riesgo de ataques internos por parte de los administradores de sistemas. Los votos se cifran y se firman digitalmente por los votantes a sus dispositivos de voto (ordenadores) antes de ser emitidos.

Sólo la clave privada puede descifrar los votos. Este proceso se realiza aplicando una técnica de Mixing (mezcla), que rompe la correlación entre la identidad de los votantes y los votos descifrados para garantizar el total anonimato.

Los votos almacenados en los servidores de voto están protegidos de forma segura (cifrados y firmados digitalmente) en todo momento, y por lo tanto, nadie los puede manipular, ni siquiera los administradores de los sistemas con acceso privilegiado.

Una vez cifrados, los votos son firmados digitalmente por los votantes. Los certificados digitales usados por los votantes para firmar digitalmente sus votos cifrados pueden ser certificados digitales preexistentes o certificados digitales generados ad-hoc para ésta elección específica. Antes de descifrar los votos, se verifica que las firmas digitales de los votantes pertenecen a los votantes validados. Los votos con una firma digital no válida son apartados para una auditoría posterior.

Los votantes pueden imprimir un recibo de voto que contiene un identificador único que consiste en un código alfanumérico generado de forma aleatoria en el dispositivo de voto del votante y que, por tanto, sólo lo conoce él.

El recibo de voto de Scytl es un código alfanumérico que no revela las opciones de voto seleccionadas por el votante y, por tanto, no permite ni la venta de los votos ni la coerción de los votantes.

El producto de Scytl se puede auditar ya que, genera registros para cada acción realizada durante la elección. Estos registros se encadenan de forma cifrada (cada vez que se genera un nuevo registro) para prevenir cualquier manipulación. Estos registros inalterables permiten una auditoría precisa de los resultados de la elección por parte de las autoridades electorales (y de terceras partes) al final de la elección

5. Sobre el proveedor del sistemas Scytl (Scytl Election Technologies)

Scytl Election Technologies (Scytl) es una empresa de software especializada en el desarrollo de soluciones seguras de voto electrónico. Scytl ha desarrollado protocolos avanzados para dotar al voto electrónico de un mayor nivel de seguridad, privacidad y confianza.

Scytl ha presentado múltiples patentes PCT (Patent Cooperattion Treaty) internacionales para proteger las características diferenciales de su tecnología de seguridad para el voto electrónico, también ha protegido su tecnología y software con copyright.

Puede encontrar más información visitando la página web de Scytl:

http: //www.scytl.com