# ¿Quién hace qué durante una elección en Belenios?

## Introducción

Belenios propone un sistema de votación electrónica verificable. Cada votante puede verificar que su boleta esté de hecho en la urna, y cualquier tercero puede verificar que el resultado reclamado corresponde a las boletas presentes en la urna, y que estas boletas provienen de votantes legítimos. El secreto de votación se garantiza a través de la división de la clave de descifrado entre varias autoridades (por ejemplo, algunos miembros del Comité a cargo de la elección) con un mecanismo de umbral (por ejemplo, 3 entre 5 son suficientes para descifrar).

Pero las buenas propiedades de seguridad tienen sentidos solo si todos realizan todas las verificaciones que se supone que deben hacer. Este documento enumera en detalle, para cada rol en la elección (votante, administrador, etc.) qué se debe hacer en cada paso.

## Instrucciones para el votante.

Cuando un votante quiere votar en línea, su computadora cifra sus opciones (con un programa de JavaScript) e imprime un número de rastreo, que es una huella digital de la boleta (un *hash*). Este número de rastreo también se envía por correo electrónico al votante cuando ha completado el procedimiento de votación.

Para verificar que su votación se tenga en cuenta, el votante debe verificar que su número de rastreo esté presente en la urna electoral visitando el enlace que se encuentra en el correo electrónico enviado después del voto: "Usted puede verificar su presencia en la urna, disponible en...". El votante también debería denunciar a las autoridades si recibe un correo electrónico de confirmación que contiene un número de rastreo que es diferente del que se imprimió en la pantalla durante la fase de votación. Puede haber ocurrido que alguien haya logrado agregar una boleta en su nombre. Esto puede, por ejemplo, ser un indicio de un ataque de un administrador del sistema que tiene acceso al buzón del votante, en el caso de que tanto el inicio de sesión / contraseña como la credencial se envíen a la misma dirección.

Nota: Un votante puede votar varias veces. Sólo se tiene en cuenta el *último* voto. El votante debe verificar que el último número de rastreo esté en la urna. Los números de rastreo anteriores se eliminan de la urna.

Un votante también puede verificar todo el proceso de votación. En lugar de comprobar solo la presencia de su boleta en la urna, puede verificar la validez de todas las boletas, puede monitorear la urna para verificar que no desaparezca la boleta (excepto en caso de votar varias veces), y finalmente verificar que el resultado publicado corresponde a las boletas en la urna. Para todo esto, el votante puede seguir las instrucciones del auditor a continuación.

## Instrucciones para los fedatarios.

Durante la configuración de la elección, se espera que el fedatario guarde:

* Su clave de descifrado (o clave PKI, en modo de umbral) (archivo private\_key.json o private\_key.txt).\*\* Esta clave debe guardarse en un lugar seguro \*\* (contenedor cifrado, pendrive USB almacenado en un lugar cerrado, etc.) porque protege el secreto de los votos (en combinación con las claves de descifrado de los otros fedatarios);
* la url de la elección;
* (en modo de umbral) la huella dactilar de su clave pública PKI, simplemente llamada clave pública a continuación;
* la huella digital de su clave de verificación asociada a su descifrado, clave de verificación.

Tan pronto como la elección esté lista, se espera que el fedatario compruebe:

* que su clave de verificación está presente en la página electoral, al lado de su nombre;
* (en modo de umbral) que su PKI clave pública esté presente en la página electoral, al lado de su nombre.

Después del cierre de la elección, el fedatario participa del escrutinio. En el caso de una elección con votación alternativa (ordenamiento de los candidatos, dándoles una calificación), el escrutinio comienza por una fase de shuffle. Para esto se espera del fedatario que

* guarde la huella digital de la urna después de su shuffle: huella digital del shuffle;
* controle inmediatamente después de lo anterior, que esta huella digital esté presente en la página de la elección (para asegurarse de que su shuffle no se haya ignorado).

En todos los casos, en el escrutinio hay una fase donde el fedatario usa su clave privada para descifrar el resultado. Se espera que el fedatario:

* (solo para la votación alternativa) controle la huella dactilar de su huella digital del shuffle, como se guardó en el paso anterior y que está presente en la página de la elección, a un lado su nombre. Si este no es el caso, la clave privada no debe utilizarse.
* guardar la huella digital de la urna para descifrar: huella digital del escrutinio cifrado.

Una vez finalizado el escrutinio, los resultados se publican en la página de la elección. Se espera que el fedatario verifique que los siguientes datos estén presentes en esta página, cada vez que se asocian a su nombre:

* (en modo de umbral) su PKI Public Key;
* su clave de verificación;
* (para votación alternativa) la huella digital de su shuffle;
* La huella digital de la urna a ser descifrada huella digital del escrutinio cifrado (para verificar que su clave privada no se haya usado para descifrar algo más).

## Instrucciones para la autoridad de credenciales.

Durante la configuración de la elección, se espera la autoridad de credenciales guarde:

* la lista de las credenciales privadas: el archivo creds.txt. **Este archivo debe guardarse en un lugar seguro** (contenedor cifrado, pendrive USB almacenado en un lugar cerrado, etc.) porque es una protección contra el cambio de voto espurio. También permitirá enviar nuevamente la credencial a un votante que la ha perdido;
* la url de la elección;
* la lista de votantes voters.txt. La autoridad de credenciales debe verificar con el comité a cargo de la elección de que esta lista es correcta, así como el peso de cada votante en caso de un voto ponderado;
* la huella dactilar de la lista de votantes: huella digital de los votantes;
* La huella digital de las credenciales públicas.

La autoridad de credenciales se encarga de enviar las credenciales a los votantes. Ella debe incluir la url de la elección en el mensaje que envía (por correo electrónico, por correo postal). Para enviar las credenciales por correo electrónico, es posible usar el programa contrib/send\_credentials.py incluido en los archivos fuente de Belenios (consulte la sección Auditor a continuación para obtener las fuentes). Después de editar este programa de acuerdo con su configuración, puede ejecutarlo:

contrib/send\_credentials.py

Tan pronto como la elección esté abierta, y al final de la elección, se espera que la autoridad de credenciales:

* verifique que la cantidad de votantes corresponde a la lista de votantes utilizada durante la configuración, así como el peso total de la elección en caso de un voto ponderado, y que la huella digital de la lista de votantes corresponde a la huella digital que se guardó antes, por ejemplo usando uno de los comandos sugeridos [aquí](#hash).
* Verifique que la huella digital de la lista de las credenciales públicas corresponde a la que se muestra al lado del nombre d elos votantes.
* Durante la elección, la autoridad de credenciales puede, cuando un votante lo pregunta, envíelo nuevamente su credencial privada si la perdió.

Al final de la elección, para validar los registros, se espera que la autoridad de credenciales:

* verifique que los registros de votación dados por el administrador corresponden a las boletas en la urna. Esta verificación se puede hacer con el comando:
* belenios-tool compute-voters --privcreds /path/to/creds.txt --url https://url/to/election

La salida de lista por este comando debe coincidir con la lista dada por el administrador (tal vez en un orden diferente).

Una vez que la elección haya terminado y validado, se espera que la autoridad de credenciales:

* destruya el archivo creds.txt. De hecho, este archivo da el vínculo entre un votante y su boleta (cifrada). Este enlace podría comprometer el secreto de votación a largo plazo, por ejemplo, si las claves de cifrado se vuelven demasiado pequeñas para la potencia de computación en el futuro (o si una computadora cuántica está disponible ...)

## Instrucciones para el comité a cargo de la elección (Comité Electoral o Junta Electoral)

Como mínimo, el Comité Electoral deberá visitar la página de la elección una vez que está abierta y verificar que:

* el número de votantes corresponde a la lista de votantes;
* el valor huella digital de los votantes publicado corresponde a la que han recibido (por el sistema o por el administrador de la elección). Esta huella digital se puede calcular utilizando uno de los comandos sugeridos [aquí](#hash).
* la lista de votantes voters.txt corresponde a los votantes legítimos, con el peso correcto en caso de un voto ponderado.
* la lista de preguntas y las posibles respuestas corresponden a lo que se espera. Estas preguntas y respuestas también están en el archivo election.json que se puede obtener haciendo clic en Parámetrosen el pie de página de la página de la elección.

Idealmente, el Comité Electoral también realiza las tareas de un auditor o encarga a alguien por hacerlo (un SYSADMIN de la organización, por ejemplo).

## Instrucciones para el auditor

Cualquiera que conozca la url de la elección puede ser un auditor. La seguridad de Belenios se basa en el hecho de que las verificaciones que se describen a continuación se realizan por al menos una persona honesta. Para realizar estas pruebas, el auditor debe usar algún software. Aquí describimos cómo ejecutar las verificaciones utilizando belenios-tool. Las fuentes de las cuales están disponibles en [GITLAB INRIA](https://gitlab.inria.fr/belenios/belenios) y que se pueden instalar bajo Linux Debian / Ubuntu usando sudo apt install belenios-tool.

Nota: estas verificaciones también se ejecutan automáticamente por nuestros servidores para las elecciones que se configuran con un nivel de seguridad máxima (autoridad de credencial externa y al menos dos fedatarios externos).

Durante y después de la elección, el auditor tiene acceso a los siguientes archivos (desde la página de la elección):

* election.json: parámetros de la elección;
* trustees.json: claves de verificación de los fedatarios y sus claves públicas PKI en modo de umbral;
* public\_creds.txt: partes públicas de las credenciales;
* ballots.jsons: boletas que se han aceptado para su inclusión en la urna.

Durante la elección, se espera que el auditor:

* verifique que el número impreso de votantes es correcto y que la huella digital de la lista de votantes sea correcta (si tiene acceso a esta información). Vea las instrucciones para el Comité Electoral.
* verifique que el archivo de partes públicas de las credenciales public\_creds.txt corresponde a la huella digital de las credenciales públicas que se muestran en la página principal de elecciones, por ejemplo, utilizando uno de los comandos sugeridos [aquí](#hash).
* verifique que el número de votantes es igual al número de credenciales públicas en public\_creds.txt.
* verifique la consistencia de la urna. Se copian los 4 archivos enumerados anteriormente en un directorio /path/to/election (por ejemplo) y el siguiente comando ejecuta todas las verificaciones requeridas:
* belenios-tool verify --dir /path/to/election
* verifique que la urna evoluciona de una manera que esté de acuerdo con el protocolo: ninguna boleta debe desaparecer a menos que sea reemplazada por otra boleta que provenga de la misma credencial (caso de los votantes que votan nuevamente). Para esto, vuelve a descargar los 4 archivos en un nuevo directorio /path/to/election/new (por ejemplo) y ejecuta el comando:
* belenios-tool verify-diff --dir1 /path/to/election --dir2 /path/to/election/new
* verifique que la página de elección que ven los votantes y los recursos asociados (imágenes, CSS, archivos JavaScript) no cambie. Los programas JavaScript deben corresponder a los obtenidas después de compilar Belenios. El programa contrib/check\_hash.py, contenido en los archivos fuente de Belenios, lo hace automáticamente:
* contrib/check\_hash.py --url https://url/to/server

Tenga en cuenta que la URL es la del servidor y no la de la elección; Por ejemplo, --url https://belenios.loria.fr.

Después de la elección, el auditor también tiene acceso al archivo result.json. Se espera que el auditor:

* Ejecute de nuevo ambas verificaciones mencionadas anteriormente para verificar la consistencia de la urna final y la consistencia con la última urna guardada.
* Verifique que el resultado mencionado en el archivo result.json corresponde al resultado publicado en la página de la elección. De hecho, esta verificación debe hacerse manualmente.
* Verifique que las huellas dactilares que estén presentes en estos archivos corresponden a lo que se publica en la página electoral que leen los votantes y los otros participantes.

Para este último punto y todas las demás tareas (excepto la verificación manual del resultado reclamado), se distribuye una herramienta de software con las fuentes de Belenios. Requiere que belenios-toolsea compilada e instalada correctamente. Luego, el auditor debe crear un directorio workdir donde la información de auditoría de elección sera guardada (después de ser descargada)), en forma de un repositorio git. Durante la fase de auditoría, el siguiente comando debe ejecutarse con frecuencia:

contrib/monitor\_elections.py --uuid <uuid\_of\_the\_election> --url https://url/to/server --wdir <workdir>

y esto descargará los datos de auditoría actuales, los verificará y los comparará con los datos anteriores.

Es posible redirigir los mensajes con la opción --logfile. Luego, solo se informan los comportamientos anormales en stdout/stderr, lo que hace posible ejecutar el comando vía un crontab y ser notificado en caso de problemas.

Nota: Si se usa la herramienta de línea de comandos belenios-tool, la confianza en las verificaciones de auditoría se basa en parte en la confianza en esta herramienta. Es posible escribir un software de verificación independiente debido a que las especificaciones de Belenios están disponibles [aquí](https://www.belenios.org/specification.pdf).

## Instrucciones para el administrador de la elección.

Puede parecer extraño, pero el administrador de la elección no tenga tantas verificaciones para realizar. Esto proviene del hecho de que el sistema de votación de Belenios está diseñado para que no tengamos que confiar en el administrador. La seguridad se basa en las verificaciones combinadas de los diferentes participantes: fedatarios, autoridad de credenciales, comité de elecciones y auditores.

Los puntos importantes para el administrador son los siguientes:

* obtener la lista de votantes, como una lista de direcciones de correo electrónico válidas, una dirección por votante. En caso de un voto ponderado, se puede asignar a los votantes un peso diferente. Esta lista debe ser validada por el Comité Electoral.
* verificar y verificar nuevamente estas direcciones de correo electrónico antes de comenzar la elección (e incluso antes del envío de las credenciales en modo automático). Una vez que finalice la configuración de la elección, no es posible modificarlas y si no se puede enviar un mensaje no no se recibe alerta.
* verificar que todos los participantes usen la misma url para la elección.
* Si el administrador no delegó a alguien como autoridad de credenciales, debe descargar la lista de credenciales privadas (Descargar credenciales privadas) para poder enviar nuevamente la credencial a un votante que lo ha perdido. Sin embargo, para una mejor seguridad, es preferible encargar a un tercero para que se desempeñe como autoridad de credenciales.

Para obtener el mejor nivel de seguridad, el administrador debe tener:

* una persona (la autoridad de credenciales) a cargo de generar las credenciales y enviarlas a los votantes (el servidor puede hacer esto en sí mismo, pero esto abre la posibilidad de un ataque de para cambiar votos).
* varios fedatarios a cargo de proteger el secreto del voto: para descifrar las boletas individuales se requiere que los "ataquen" a todos (o al menos una proporción de ellos, en modo de umbral).

## ¿Cómo calcular la huella digital de un archivo

Para calcular la huella digital de un archivo, debe usar el mismo algoritmo hash que se usa en Belenios. Ofrecemos aquí posibles soluciones con líneas de comando. Utilizamos el archivo voters.txt como ejemplo, pero, por supuesto, puede reemplazarlo por cualquier otro archivo.

sha256sum voters.txt | xxd -p -r | base64 | tr -d "="

(o shasum -a256 en vez de sha256sum en MacOS)

cat voters.txt | python3 -c "import hashlib,base64,sys;m=hashlib.sha256();m.update(sys.stdin.read().encode());print(base64.b64encode(m.digest()).decode().strip('='))"

También puede usar [la herramienta en línea](https://belenios.loria.fr/compute-fingerprint) del sitio de Belenios.