ENCRIPCIÓN Y SECRETO DEL VOTO

¿ES POSIBLE ASEGURAR EL SECRETO DEL VOTO?

En Evoting hemos desarrollado nuestro **propio software de votación** lo que nos permite ir permanentemente actualizando, perfeccionando y adaptando nuestras medidas de seguridad a los requeriminetos que surjan.

VOTO ENCRIPTADO

La criptografía es el sistema que utilizamos para asegurar el **secreto del voto**. Trabajamos con criptografía asimétrica, técnica matemática que transforma un mensaje legible en uno ilegible. Cuando el votante marca su preferencia, un proceso de encriptación "cierra" el voto transformándolo en un mensaje ilegible y asegurando el secreto de su contenido.

Cuando el votante pasa las distintas etapas de control –estar en el padrón, no haber votado anteriormente y haber autentificado su identidad–, el voto encriptado se deposita en la urna.

Utilizamos también un algoritmo "homomórfico", que permite realizar operaciones directamente sobre los datos encriptados, es decir, sin la necesidad de desencriptarlos previamente ni de contar con la clave con la que fueron encriptados. Ello reduce la probabilidad de que puedan ser intervenidos y permite un **control más estricto sobre la disponibilidad de la información**, garantizando su integridad y confidencialidad.

TOTAL SECRETO DEL VOTO

El uso del algoritmo homomórfico nos permite sumar los votos encriptados y obtener un resultado encriptado. Terminada la votación, se desencripta la suma de votos, sin que éstos sean abiertos individualmente, ni se pueda conocer la opción marcada en cada uno. Así, mantenemos el secreto del voto.

En el lenguaje criptográfico se habla de "llaves" para denominar los inputs que permiten al algoritmo hacer la encriptación y desencriptación requeridas. Las llaves definen el **esquema de encriptación**. Existen dos tipos de llaves: una **pública**, que encripta, y una **privada**, que desencripta.

La suma final de votos –el resultado– se desencripta utilizando las llaves privadas en poder de la Comisión Electoral.

CONFORMACIÓN COMISIÓN ELECTORAL

En cada votación, EVoting trabaja directamente con la Comisión Electoral, Tribunal Supremo o TRICEL que la organización ha definido, de acuerdo a sus normas internas. La Comisión Electoral es la única **contraparte de EVoting** durante el proceso. De esta manera, aseguramos la transparencia y el respeto a los protocolos preestablecidos.

GENERACIÓN DE LLAVES CRIPTOGRÁFICA

En la ceremonia de "generación de llaves" –proceso propio de EVoting– se crean las l**laves criptográficas pública y privada**, en presencia de la Comisión Electoral o un **Ministro de Fe**. La privada se divide en varias partes, según el número de integrantes de la Comisión Electoral. No se trata de copias de una llave sino de pequeñas partes de la misma.

El tamaño de las llaves depende del número de opciones de una votación. Las votaciones con mayor números de opciones, requieren llaves más grandes.

Las llaves criptográficas son **únicas para cada votación y no tienen copias**. Si la mayoría de estas partes de llave privada se pierden, no se puede hacer el escrutinio y es necesario repetir la votación.

La idea es que la llave privada –por ende el acceso a los resultados de la votación– esté dividida en varias partes y que cada parte responda a un miembro de la Comisión Electoral, asegura que el acceso a los resultados **no dependa de una sola persona**.

ESCRUTINIO

Esta ceremonia se realiza con los **miembros de la Comisión Electoral**. Sumados los votos individuales encriptados, cada miembro de la Comisión entrega su parte de llave, que se carga para **desencriptar los resultados** (equivalente a abrir la urna).

Para este procedimiento se requiere la mayoría simple de los pedacitos de las llaves privadas.

Como **medida de transparencia** los resultados se publican automáticamente en el sitio web de la votación, permitiendo a la Comisión Electoral y a cualquier votante tener acceso a esa información de manera inmediata.