# ESTADO DEL ARTE DEL PROBLEMA

### 1.4.1 Requisitos, retos y soluciones del voto electrónico clásico

El voto electrónico (e-voting) usa datos digitales para recoger las selecciones del votante. El voto por internet (I-voting), además, requiere mayor nivel de seguridad ya que el cliente no está supervisado durante el voto (el votante puede estar en casa, en el trabajo, en una biblioteca, etc.)

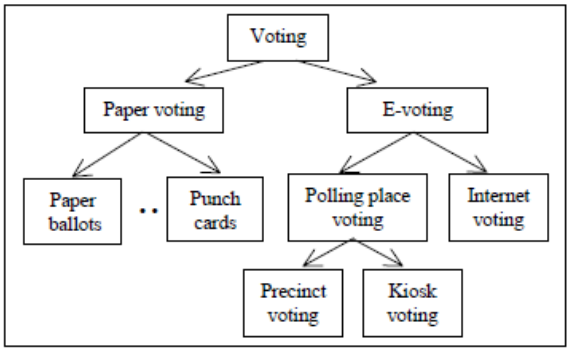


Fig. 1: Tipos de votación (Fuente: Burmester et al., 2003)

En ese sentido, y tras el desarrollo de múltiples soluciones de democracia digital en todo el mundo, es ampliamente sabido que el principal problema de seguridad y confiabilidad reside en la aparente contradicción de términos entre dos importantes requisitos exigibles a las votaciones; Integridad y privacidad.

Mientras que el requisito de integridad exige que pueda comprobarse por cualquiera (incluso por el propio votante) que los votos no son manipulados (añadidos, borrados, o cambiados) el secreto de voto exige anonimizar cada voto de tal manera que no pueda rastrearse en qué sentido ha votado cualquier votante, impidiendo así, además, la posible coerción o venta de votos. Esa contradicción es, en dos palabras, la principal fuente de problemas de cualquier votación electrónica.

Más en detalle podemos listar un serie de condiciones exigibles a cualquier votación (y por extensión, decisión) por medios electrónicos y por internet.

1) TRANSPARENCIA E IMPARCIALIDAD

Al igual que las elecciones tradicionales, las votaciones electrónicas deben tener la posibilidad de contar con observadores o interventores durante el proceso, así como la posibilidad de auditorías, una vez acabado éste. Procedimientos de auditoría restringidos, inadecuados o insuficiente atención dados al sistema o al diseño del proceso de la votación, producen elecciones sujetas a posibles errores y fraudes. Todos los pasos esenciales de la elección deben estar sujetos al control público, mientras otros derechos no justifiquen una excepción. En suma, el ciudadano o usuario/miembro debe poder controlar cada paso esencial del acto electoral/de decisión y la determinación del resultado de manera fiable y sin conocimientos técnicos especiales. Así, sería deseable:

Antes de la votación:

- Documentación fácilmente accesible del sistema en lenguaje claro y asequible.
- Esto incluye requisitos técnicos, cuestiones de elegibilidad, etc.
- Censo bloqueado durante la votación e incluso un margen de tiempo T anterior.
- Datos del censo con cortes por circunscripción (provincia, localidad, etc.)
- Si la votación es abierta, criterios claros de inclusión en el censo y medidas anti-duplicidad.
- Facilidad para incluirse como interventor para cualquier persona (con un límite por nº)

Durante la votación:

- Progreso en el nº de votos, en detalle por circunscripciones o cortes. (Hora, provincia, etc.)
- Autoridades e interventores técnicos independientes durante el proceso

Después de la votación:

- Resultados completos del escrutinio incluyendo, resultados en detalle por campos y tablas completa de votos, anonimizados.
- Verificabilidad individual del voto y su sentido. (Requisito también asociado a integridad. Este punto es discutible si conviene hacerlo antes y/o después del cierre de la votación.)

2) INTEGRIDAD

2.1. VERIFICABILIDAD UNIVERSAL

Cualquier observador debe poder ser convencido de que la elección es precisa y que el escrutinio publicado está calculado correctamente a partir de votos correctamente emitidos. Y que los votos no han sido manipulados (añadidos, borrados, o cambiados) por ningún atacante, autoridad o administrador. Normalmente, la integridad y protección ante un administrador "tramposo", es lo más difícil de asegurar.

2.2. VERIFICABILIDAD INDIVIDUAL

Cualquier observador debe poder ser convencido de que su voto ha sido correctamente emitido y contado, y no ha habido manipulación.

2.3. INCOERCIBILIDAD ("Incoercibility")

Propiedad que asegura la no existencia de presiones externas para la imposición o compra del voto a los votantes. Esta propiedad es muy difícil de asegurar en votaciones por internet (I-voting) ya que si el usuario usa un ordenador para votar no puede asegurarse que alguien físicamente pueda estar viéndole y ejerciendo coerción, aunque la posibilidad de cambiar el voto posteriormente mitiga en gran parte esta posible coerción y anula el valor de la posible "venta". En el resto de ocasiones (voto en cabinas, etc.) está relacionada con la imposibilidad de demostrar el sentido del voto imprimiendo un recibo Si no se puede imprimir un comprobante con el sentido del voto en claro ("receipt freeness") se hace difícil la coerción.

3) PRIVACIDAD

En algunos tipos de elección, todos los votos deben ser secretos y cada voto individual no puede enlazarse en claro al votante que lo emite (exceptuando el propio votante si así lo decidiese, pero sólo para su propia verificación y de nadie más). En estos casos, nadie debe poder jamás comprobar el sentido de voto de un votante (ni siquiera los administradores).

4) ELEGIBILIDAD

- Sólo los votantes autorizados, existentes en un censo, pueden votar.
- Ningún votante puede emitir más de un voto.
- Es necesario asegurar que nadie pueda suplantar la identidad de otro votante.
- En votaciones sin censo (abiertas) es recomendable asegurar una edad mínima para votar.
- Datos del censo con cortes por circunscripción (provincia, localidad, etc.)
- Censo bloqueado durante la votación e incluso un margen de tiempo T anterior.
- Si la votación es abierta, criterios claros de inclusión en el censo y medidas anti-duplicidad.

(En realidad los 3 últimos ya han sido expresados en el punto de la transparencia)

5) ROBUSTEZ ANTE ATAQUES Y SEGURIDAD GENÉRICA

Aunque este es un capitulo que puede comprometer a otros (integridad y privacidad) merece un capítulo aparte porque también el sistema ha de ser bastante robusto para estar protegido al menos parcialmente ante ataques de denegación de servicio, "phising", "sql injection", y otras vulnerabilidades genéricas del software y hardware involucrado.

Resumiendo, si tuviésemos que listar sucintamente una serie de características deseables para cualquier votación electrónica diríamos (Burmester, 2003) que una votación además de ser práctica ha de ser segura, esto es:

Justa: solo los votantes autorizados pueden emitir su voto)

Integra: ningún voto puede ser alterado, duplicado o borrado sin que se detecte)

Universalmente verificable: cualquier observador puede ser convencido de que la elección es íntegra y de que los resultados han sido correctamente calculados a partir de los votos correctamente emitidos.

Robusta: los requerimientos de seguridad deben ser plenamente satisfechos, incluso ante conducta maliciosa por cualquier coalición (de tamaño razonable) de agentes (autoridades, votantes, administradores,…)

Privada: (En muchos casos) todos los votos deben permanecer secretos, ningún voto individual puede ser enlazado al votante que lo ejerció. Además, por incoercibilidad, ningún votante debería ser capaz de probar a terceros cual fue el sentido de su voto.

Hay varios esquemas o estrategias para tratar conjuntamente el problema de la integridad y la privacidad de la votación electrónica, que mencionábamos como crucial. Para hacer la historia corta, las principales cuatro estrategias criptográficas que se citan comúnmente son la firma ciega, el uso de mix-nets, la compartición de secreto y el cifrado homomórfico. El gran problema de todas estas técnicas es que son bastante abstrusas y difícilmente comprendidas por el gran público e incluso por aquellos que tienen ciertos conocimientos de informática y son usuarios de la red, lo cual entra en colisión con algunos de los requisitos de transparencia y usabilidad que hemos mencionado anteriormente.

**Firma ciega:** Aún con dos dominios separados, de autenticación (AA) y voto (donde se reciben, almacenan y cuentan) (AV) estos pueden confabularse. Para evitar esto, el votante "firma" su voto. AA valida el voto y la firma sin conocer el sentido del voto (sólo mira si el remitente está en el censo pero no enlaza el remitente a la firma, sólo el voto). En la urna de AV están todos los votos validados y las firmas pero sólo los votantes saben cada uno cuál es su firma, y así, su voto.

**Mix-Nets:** Terceras partes de confianza ("autoridades") "barajan" los votos mediante mensajes de tal manera que nadie es capaz de identificar el emisor o receptor de mensaje. Se suele usar fundamentalmente para anonimizar los votos.

**Cifrado homomórfico:** Básicamente es un cifrado donde una operación de votos cifrados equivale al cifrado de otra operación entre votos sin cifrar. Sirve para poder hacer contajes con votos aun sin cifrar. Solo es posible utilizarlo para conjuntos cerrados de elecciones (Si/NO, etc.) pero no para voto preferencial.

**Papeletas precifradas:** En este esquema todo el cifrado se hace anterior a la votación y se envían a los votantes ya autenticados los códigos personalizados para la votación. Tiene el inconveniente que incluye un envío previo (incluso físico) por parte de la autoridad de votación y la ralentiza.

Ha habido múltiples intentos y ejemplos de solventar en conjunto todos los requisitos impuestos, pero como mencionan Sampigethaya et al. (2006) en su "*Marco y taxonomía para la comparación de esquemas de votos electrónicos*", se suelen sacrificar algunas características en beneficio de otras. En esa obra se refieren al trabajo seminal de Chaum (1981) y se divide su taxonomía de soluciones a 3 clases distintas: votante oculto (los votantes anónimamente emiten votos) voto oculto (los votantes abiertamente emiten votos cifrados) y votante oculto con voto oculto (se cumplen las dos condiciones). Se concluye en esa obra, tras mostrar toda una taxonomía de esquemas ensayados, que no hay un candidato claro cara al futuro, pues mientras que el voto oculto tiene muchas propiedades deseables (la ausencia de disputa) el formato del voto y la posibilidad de coerción hacen difícil su aplicación. Por otra parte, la clase votante oculto con voto oculto tiene características prácticas que incluyen incoercibilidad, pero está limitado por la escalabilidad de la mixnet de reencriptación, y las mixnet dejan el regusto a algo alejado de la transparencia para el usuario medio.

### 1.4.2 Retos y soluciones del voto electrónico preferencial y líquido

Es obvio que introducir la preferencia o la ponderación en el voto complica un tanto los cálculos y hace un poco más contraintuitivos los resultados. Hasta este punto solo necesitábamos contajes enteros pero a partir de aquí vamos a tener que introducir números reales, con un número determinado de decimales (en realidad se trata de nºs racionales pues en puridad no hay manera de almacenar un nº irracional exacto en un sistema informático finito) derivados de los contajes Borda, Dowdall o ponderados, y también llevar más de un contaje (p.ej. nº de votos totales por candidato u opción y peso total de esos votos).

Para el VUT (voto único transferible) se añade otro grado de complejidad ya que los resultados finales empiezan a depender no solo de los votos a una opción concreta, sino también más del entorno, es decir, de los votos preferenciales a otras opciones, pero al fin y al cabo se trata de aplicar un nuevo algoritmo.

La democracia líquida, además, introduce dos novedades con implicaciones técnicas importantes: La posibilidad de cambiar el sentido del voto/elección (revocabilidad) y la de delegarlo a otra persona (también dinámicamente). Estas dos condiciones obviamente nos obligan a mantener algún tipo de enlace entre el voto y el votante, lo cual hace más crítico la necesidad de aunar privacidad (en caso de que esta sea requerida) e integridad.

Debe aclararse que, en el caso de delegación de voto, los votos de los delegados, al menos hasta determinado nivel no son secretos sino públicos, se supone que son personas que hacen campañas públicas y por otra parte si el voto delegado no fuera público el votante no sabría el sentido de su voto atómico. Por lo tanto en caso del votante atómico que delega lo que se privatiza no es el sentido de su voto, sino a quien lo delega.

Puede además agregarse más de un nivel, si el voto delegado puede a su vez delegarse (delegación transitiva) aunque esto añade una dificultad nueva, la necesidad de comprobar algorítmicamente que no se da un ciclo recursivo (Es decir comprobar que un delegado no hace delegación sobre alguien que a su vez la ha delegado el voto directa o indirectamente).

### 1.4.3 Retos y soluciones de las decisiones abiertas e inteligencia colectiva

El reto más importante de las decisiones abiertas (que se dan cuando las respuestas no están previamente acotadas, como hemos visto en los apartados 1.3.7 a 1.3.9) es la complejidad algorítmica involucrada lo cual presenta problemas de escalabilidad cuando se intenta aplicar a grandes números. Speroni (2017) considera que, por ejemplo, su solución incluyendo el frente de Pareto (el software **"Vilfredo Goes to Athens"**) implica una complejidad algorítmica exponencial y lo ve aplicado a pequeños equipos de no más de 20 ó 30 expertos o personas involucradas en la solución de un problema concreto. Con el mismo problema se encuentran algunas herramientas de decisión ya existentes en el mercado como "**Loomio**" pensado para la toma de decisiones en juntas, comités y grupos de no más de 30 personas.

El denominado **método Delphi** es una técnica de comunicación estructurada, desarrollada como un método sistemático e interactivo de decisión (o prospectivo) usualmente aplicado por paneles de expertos que deciden, ante un problema complejo, entre un grupo de propuestas valoradas anónimamente por ellos mismos. Digamos sucintamente que las características definitoria de este método son:

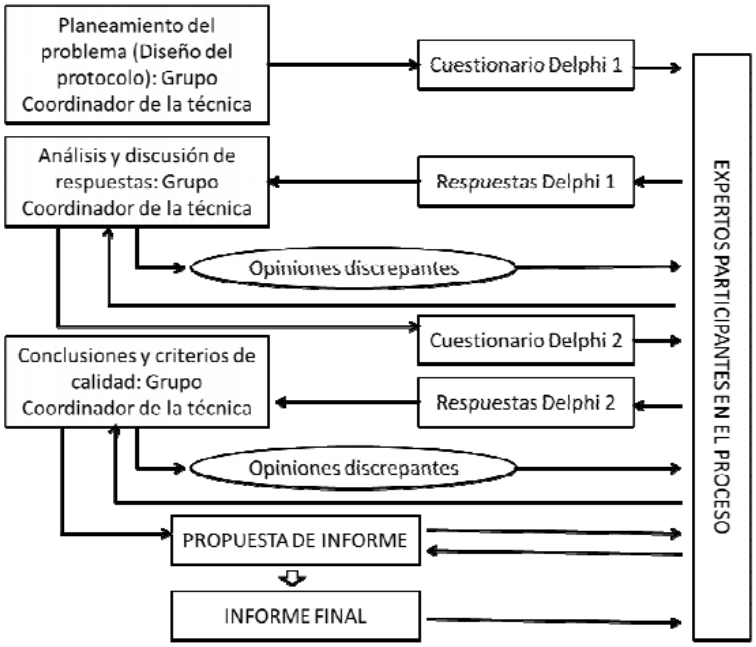


Fig. 2: Esquema del proceso en Delphi (Fuente: Pozo et al., 2003)

Proceso iterativo: los participantes valoran las propuestas en varias "generaciones". Entre una y otra consulta tienen oportunidad de reflexionar sobre las opiniones propias y ajenas.

Anonimato: los expertos pueden conocerse, pero no identificar lo que dice cada uno de ellos. Así, no hay posibilidades de sesgo por prestigio o liderazgo de algún miembro. Las opiniones emitidas se basan únicamente en las ideas, no en las personas.

Feedback controlado: El grupo analiza las respuestas recibidas y produce la nueva consulta, asegurándose que aparezcan representadas todas las opiniones dadas por los expertos. En cada generación, se destacan aportaciones significativas y acuerdos.

Respuesta estadística del grupo: Suele incluirse frecuencias y medidas de tendencia central así como valores de dispersión de las respuestas individuales, en las rondas subsiguientes. Además, la retroalimentación de cada ronda es en forma de información estadística.

Basado en ese método, en cuanto que las valoraciones de la propuestas no se asocian fuertemente a quien las propone (al contrario que se suele hacer, por cierto, en las decisiones políticas) han surgido alguna herramientas como **"iWarsM'aps"** en la cual es central el concepto de comparación entre propuestas en lo que se autodenomina "agregador de inteligencia". Pero tampoco en este caso la solución parece aplicable a grandes números (millones de opiniones, por decir un número).

El software **"Appgree"**, por el contrario, es aplicable a grandes números dado su algoritmo de troceo de muestras *DemoRank*, basado en el principio estadístico que dice que una muestra de personas elegidas al azar de un grupo es representativa de todo el grupo. Aprovechando ese hecho, permite hacer preguntas abiertas a un grupo, sea cual sea su tamaño, y recibir la respuesta con mejor aceptación en minutos. Encontramos en este caso que no hay comparación, matiz o ciclo porque las valoraciones de las propuestas siguen siendo binarias (Sí/No) aunque el planteamiento general constituye un interesante camino abierto a soluciones escalables con un poco más de definición y cantidad de información.

### 1.4.4 Ejemplos de democracia electrónica avanzada usados en este PFG

Aquí documentamos con más detalle unas pocas soluciones concretas ya existentes (alguna ya mencionada), cuyas funcionalidades servirán de base y referencia, y que en cierta manera han sido seminales e inspiradoras, de cara la herramienta a desarrollar:

- Demokratian (V.U.T., D.Líquida),
- Appgree (Preguntas abiertas, Tratamiento estadístico, algoritmo DemoRank),
- Vilfredo goes to Athens (Preguntas abiertas, Frente de Pareto) y
- iWarsM'aps (Método Delphi, comparativas, agregador de inteligencia).

**demoKratian**

Es una aplicación web instalable en cualquier servidor que puede usarse para implementar formas de decisión horizontal en cualquier organización. Está basada mayormente en el voto e incorpora actualmente cuatro tipos de votación; el organizador puede elegir entre abrir un debate, realizar una encuesta, hacer una votación con voto ponderado, o realizar una votación con recuento VUT. Los miembros registrados (censo) pueden votar de una forma sencilla y secreta. Es software libre (licencia GPL 3.0) desarrollado en lenguaje de servidor PHP y base de datos MySQL.

Sitio web para más información: http://www.demokratian.org/

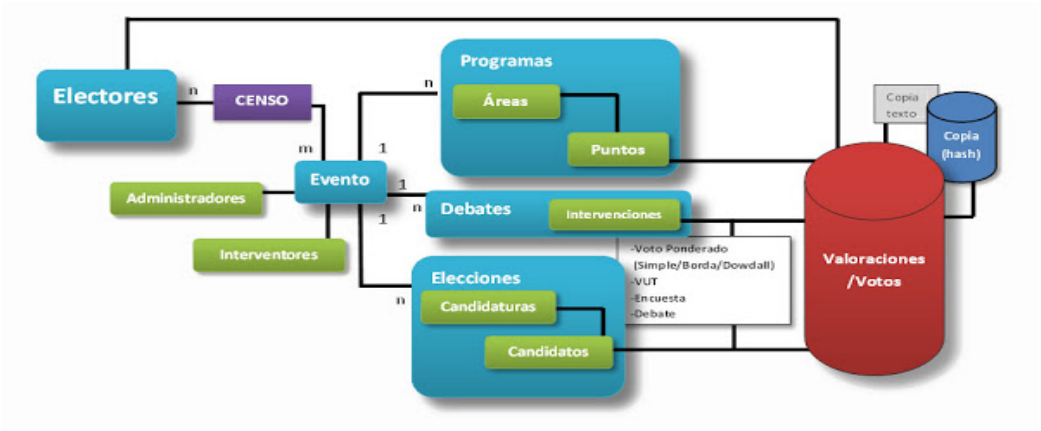


Fig. 3: Esquema de Demokratian (Fuente: demokratian.org)

Es una aplicación para web y móvil desarrollada por Meta4 que permite entresacar las opiniones más valoradas de un grupo de personas cualquiera que sea su tamaño (escalabilidad) sobre cualquier tema. Se basa en el ya mencionado algoritmo DemoRank cuyo proceso podemos ilustrar así:

1. Una persona o entidad lanza una pregunta abierta para que cualquier usuario del grupo de M personas respondan.
2. $N_0$ personas responden con sus propuestas
3. DemoRank divide estadísticamente al azar el grupo de M personas entre $N_0$ subgrupos grupos a los que pide valoración de solo una respuesta por grupo.
4. Se repite el paso anterior pero con las $N_1$ respuestas mejor valoradas (se descartan las peor valoradas) dividiendo el grupo entre $N_1$ nuevas muestras al azar y así siguiendo.
5. Según el tamaño del grupo puede ajustarse el porcentaje de propuestas que pasan a las siguientes rondas. Cuando queda solamente una respuesta se vuelve a pedir valoración final a todo el grupo de M personas.

El algoritmo se basa en el principio estadístico que dice que una muestra al azar de un grupo es representativa de todo él. Aprovechando esto, permite hacer preguntas abiertas a grupos sea cual sea su tamaño, y recibir la respuesta con mejor aceptación en minutos (3 ó 4 ciclos de valoraciones) incluso para grupos muy grandes de millones de personas.

Sitio web para más información en: http://www.appgree.com/appgree/

Es una aplicación desarrollada en Python (código en GitHub) por Pietro Speroni di Fabrizio que permite responder grupalmente a cualquier pregunta abierta orientando la respuesta hacia una solución consensuada. Para la confluencia de propuestas se usan generaciones de ellas en ciclos de mejora, y para asegurar que la respuesta final es realmente consensuada usa el denominado frente de Pareto que tiene que ver con la "dominancia" de unas propuestas sobre otras (cuales contienen a otras). Se aporta información detallada acerca del frente de Pareto en el Apéndice 1F.

Según el propio autor esta aplicación no es escalable más allá de 20 o 30 personas y su área de uso ideal sería la toma decisiones entre expertos en un determinado tema.

Sitio web para más información en: http://v1.vilfredo.org/viewquestions.php

iWarsM'aps

Es una aplicación que proclama ser "el primer agregador de inteligencia del mercado". Desarrollada por Innovation Wars (citar) está basada en parte en las técnicas del método Delphi, anteriormente mencionado y como Appgree, está orientada a preguntas abiertas. Se caracteriza por centrarse en las ideas y no en las personas (las propuestas son anónimas) entrando en varios ciclos, diferenciando la búsqueda y planteamiento de problemas con la búsqueda de soluciones.

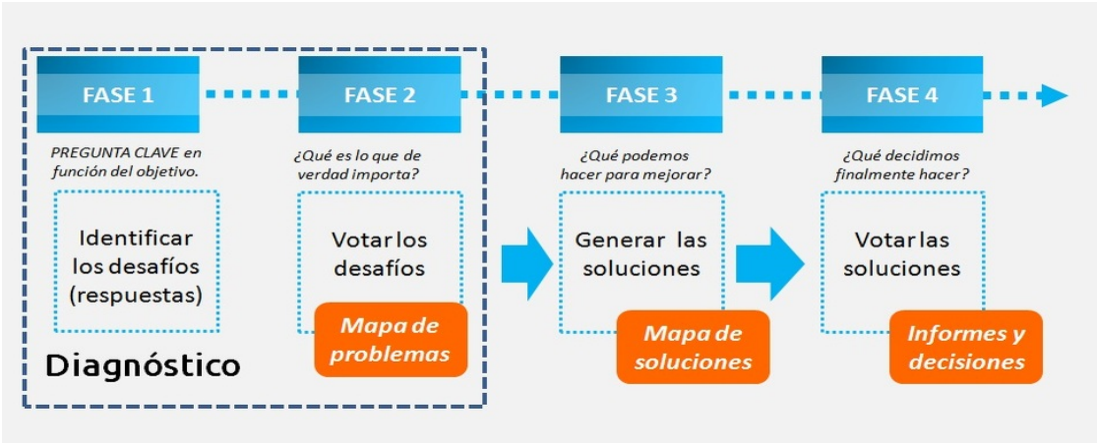


Fig. 4: Esquema del proceso en iWarsM'ap (Fuente: innovation wars)

Una diferencia con Appgree es que la valoración de las propuestas no se hace en vacío, sino por comparación con otras propuestas. Además, emplea "clusterización" para agrupar (semi-automáticamente) respuestas con alto grado de similitud (semántica y/o conceptual) e "hibridación" (semi-automática) para elegir las respuestas que mejor sintetizan el trabajo de un grupo. Asimismo los datos y resultados se segmentan "poliédricamente" según varios criterios y se ofrecen los resultados con narrativa visual, esto es, ofreciendo distintas clases de infografías para representarlos.

## CONCLUSIONES

Tras observar y estudiar en lo posible el enfoque y comportamiento de estas cuatro herramientas, nos surge la idea de tomar algunas características de cada una de ellas para el desarrollo de este proyecto. Así, nos quedamos con:

- la versatilidad, facilidad de uso y mantenibilidad de **Demokratian**, sobre todo en lo que respecta a la implementación de la teoría del voto,
- la impresionante escalabilidad y sencillez algorítmica de **Appgree**,
- la orientación al consenso de los algoritmos genéticos de **Vilfredo goes to Athens**
- el enfoque hacia las ideas, los procesos semiautomáticos de ciclos segmentados y los resultados en forma visual de **iWarsM'ap**