VISTO la disposición del Consejo Departamental del Departamento de Computación acerca del proyecto de Ley de Reforma Electoral enviado por el Poder Ejecutivo Nacional actualmente en discusión en el Congreso de la Nación, en el que se contempla la implementación de una variante de voto electrónico conocida como *Boleta Única Electrónica;* y

CONSIDERANDO:

Que el Departamento de Computación apoyó la declaración "Decimos NO al voto electrónico" avalada por los siguientes departamentos de Computación de Universidades Nacionales e institutos del CONICET: Sección de Computación, Facultad de Astronomía, Matemática, Física y Computación, Universidad Nacional de Córdoba; Departamento de Computación, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires; Departamento de Ciencias de la Computación, Facultad de Ciencias Exactas, Ingeniería y Agrimensura, Universidad Nacional de Rosario; **Departamento de Computación, Facultad de Ciencias Exactas, Físico-Químicas y Naturales, Universidad Nacional de Río Cuarto**; Instituto UBA-CONICET de Investigación en Ciencias de la Computación; Facultad de Informática, Universidad Nacional del Comahue; Centro Internacional Franco Argentino de Ciencias de la Información y de Sistemas (CONICET-Universidad Nacional de Rosario), en la que expertos en informática describen los potenciales problemas de aplicar un sistema como el que propone el proyecto de ley.

Que los procesos electorales deben consagrar a gobernantes y representantes del pueblo a partir del respeto a la voluntad popular.

Que los procesos electorales no sólo deben garantizar el derecho al voto, sino que deben preservar el derecho al voto secreto, para evitar que la ciudadanía pueda ser coaccionada, amenazada o intimidada a votar de cierta forma.

Que los sistemas informáticos aplicados a sistemas electorales han tenido muchas críticas, porque de ser defectuosos podrían comprometer uno de los pilares de la democracia representado por el voto popular.

Que los diversos mecanismos empleados para aumentar la confiabilidad del software (inspección ocular, revisión entre pares, *testing*, análisis estático y dinámico de código, etc.) pueden ser efectivos para detectar la presencia de fallas, pero nunca pueden garantizar su ausencia.

Que aun en sistemas de código abierto que fueron sometidos al escrutinio de expertos informáticos y del público en general se han encontrado fallas que permanecieron ocultas por años o incluso décadas.

/.

Que existe evidencia de que algunos defectos en los sistemas informáticos, que fueron intencionalmente introducidos con el objetivo de debilitar su seguridad, fueron detectados luego de varios años, habiendo afectado durante ese tiempo a millones de usuarios.

Que una adulteración del sistema de voto electrónico podría permitir desde manipulaciones muy notorias hasta algunas cuantitativamente más sutiles, pero igual de categóricas en términos cualitativos, sobre todo en elecciones de alta importancia institucional con resultados reñidos.

Que los sistemas que proveen como medida adicional el recuento en papel podrían almacenar de forma digital una opción y de forma impresa otra, erosionando la legitimidad del resultado.

Que el "Informe Final de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires sobre la elección para Jefe de Gobierno de 2015" señala que "[...] una vez cerrada la mesa, el 83,9% de los presidentes pudo realizar el escrutinio sin inconvenientes. Durante el conteo de votos, sólo el 10,1% de las mesas contó con fiscales que realizaron algún reclamo", lo que representa una cantidad de votos significativa en el caso de una elección reñida. Asimismo, surge del mismo informe que un 26,2% de los votantes dijo no haber verificado que el voto impreso coincidiera con lo que había elegido.

Que a pesar de que el sistema electoral utilizado en aquella elección fuera auditado por un equipo de expertos, que alertó sobre la ausencia de prácticas seguras en la forma en la que se desarrolló el código, varias fallas fueron encontradas posteriormente a la auditoría por investigadores independientes, destacándose entre ellas la que permitía que un chip adulterado computara varios votos y la que manifestaba un manejo poco seguro del mecanismo de encriptación utilizado, con la consecuente posibilidad de envío al centro de cómputos de resultados apócrifos pero que aparentaban ser oficiales.

Que el técnico informático que hizo pública esta última vulnerabilidad fue allanado en su hogar, y sometido a un proceso judicial que, luego de un año, dictaminó su inocencia y el reconocimiento de que su accionar había contribuido a la mejora del sistema.

Que en dicho proceso judicial la empresa responsable del sistema electoral declaró que sus servidores habían sufrido intrusiones cuyo origen y alcance aún hoy se desconocen.

II.

Que es bien conocida en la comunidad informática la importancia de auditar no sólo el software de aplicación, sino también el entorno en el que se ejecuta y el conjunto de herramientas conocida como la *cadena de compilación*, ya que un compilador adulterado podría producir código de máquina malicioso a partir de código fuente sin defectos.

Que el comportamiento final de cualquier sistema informático está dado por la interacción de hardware y software, y existe amplia evidencia académica que documenta la posibilidad de adulterar incluso el hardware, para que se comporte de forma maliciosa.

Que por ende, en el caso de un sistema electoral, debería auditarse tanto el hardware, como el entorno de ejecución de la cadena de compilación y el software de aplicación utilizado, configurándose así un sistema muy complejo, de enorme tamaño, que podría involucrar incluso componentes de terceras partes de los cuales no se disponga del código fuente.

Que dicha auditoría requeriría un proceso de revisión por parte de un grupo de expertos altamente calificados, señalamiento de dificultades, corrección y vuelta a empezar que se extendería por largos periodos de tiempo hasta lograr un nivel de confianza suficientemente alto, aun así no asegurando la ausencia de fallas.

Que muchas fuerzas políticas, en especial las más pequeñas, podrían no contar con tales expertos, ni con posibilidad real de contratarlos.

Que si bien existen mecanismos para asegurar que el software auditado es el que finalmente llega a cada máquina electoral, esto requiere que cada fiscal partidario cuente con equipamiento informático propio para verificarlas, y que de producirse cualquier modificación de último momento por más mínima que sea, se convoque nuevamente a los expertos partidarios para recompilar el sistema en su totalidad, recomputar la firma digital e informarla a todos los fiscales partidarios.

Que las verificaciones mencionadas anteriormente resultan inviables en la práctica.

Que no existen mecanismos equivalentes para el hardware, debiendo los fiscales partidarios y la ciudadanía en general recurrir a actos de fe para suponer que el hardware que conforma cada máquina electoral es el mismo que fuera auditado y no ha sido adulterado con objetivos maliciosos.

///.

Que si bien el mecanismo tradicional basado en votación en papel y recuento manual requiere el despliegue de grandes cantidades de ciudadanos que sirven como fiscales partidarios, este requisito no desaparece con un sistema electrónico, ya que de no haberlos, los distintos partidos no podrían atestiguar que los sistemas no sean alterados in situ.

Que incluso a sistemas informáticos de votación más simples, como aquellos donde el elector manifiesta su voluntad en una terminal que luego imprime una boleta para su recuento manual, se le aplican todas las consideraciones previamente mencionadas.

Que incluso las impresoras más sencillas cuentan con procesadores y memoria, y por ende, podrían registrar el voto de cada elector o codificar el horario de emisión de cada sufragio, permitiendo así vulnerar el secreto del voto.

Que la mera posibilidad de que estos mecanismos se pongan en práctica, y la imposibilidad absoluta del elector de tener certeza de que no es así, podrían servir como mecanismo de coacción o persuasión ilegítima.

Que toda auditoría de sistemas de software/hardware debe tener como objetivo encontrar errores (voluntarios o involuntarios) en todo el sistema, lógica mal intencionada, vulnerabilidades de seguridad y mecanismos de fuga de información que permitan descubrir canales encubiertos (los cuales podrían, por ejemplo, vulnerar el secreto), etc., y tal auditoría resulta inviable en los plazos disponibles para el desarrollo e instalación de los sistemas de boleta única electrónica, como lo confirman las declaraciones de voceros de empresas involucradas en estos procesos.

Que en otras experiencias en las que se ha utilizado sistemas informáticos en elecciones locales o regionales en nuestro país y en el resto del mundo, han ocurrido inconvenientes significativamente más serios que aquellos observados en los casos en los cuales se utilizó el sistema tradicional de boletas en papel.

Que según versiones periodísticas, en las últimas elecciones en Salta se debió reemplazar 299 máquinas, sólo en la capital provincial. Se observaron además manipulaciones de DVDs sin control por parte de las autoridades electorales.

Que en el año 2009 la Corte Suprema de Alemania prohibió el uso de urnas electrónicas porque contradice el principio de que todos los pasos de la elección estén sometidos al escrutinio público sin requerir conocimientos técnicos especiales.

////.

Que la complejidad que tiene la tecnología a utilizar elimina la posibilidad de control que debería poder ejercer cualquier ciudadano sobre el proceso electoral.

Que países conocidos por su alta capacidad tecnológica no utilizan el voto electrónico en elecciones generales de carácter nacional, y otros cancelaron o postergaron su uso luego de efectuar algunos ensayos.

Que el proyecto de ley, actualmente en debate en el Congreso de la Nación, criminaliza el estudio o análisis de estos sistemas para encontrar vulnerabilidades, lo cual va en la dirección contraria a garantizar la seguridad de este tipo de sistemas.

Que el Departamento de Computación cuenta con docentes e investigadores en Ciencias de la Computación que tienen la obligación de cuestionar y enseñar a cuestionar estos sistemas, así como detectar anomalías que permitan su mejora.

Que se considera de vital importancia la incorporación de conocimiento científico en la argumentación de propuestas de políticas públicas.

Por ello y en uso de las atribuciones que le confiere el Artículo 32 del Estatuto de la Universidad Nacional de Río Cuarto.

EL CONSEJO DIRECTIVO
DE LA FACULTAD DE CIENCIAS EXACTAS
FÍSICO-QUÍMICAS Y NATURALES

RESUELVE

ARTÍCULO 1ro.- Rechazar el proyecto de Ley de Reforma Electoral enviado por el Poder Ejecutivo Nacional actualmente en discusión en el Congreso de la Nación, en el que se contempla la implementación de una variante de voto electrónico conocida como *Boleta Única Electrónica*.

ARTÍCULO 2do.- Rechazar categóricamente la criminalización de la investigación sobre cualquier aspecto de los sistemas informáticos electorales u otros sistemas de uso público que sean de importancia para la sociedad.

/////.

ARTÍCULO 3ro.- Elevar al Consejo Superior para su tratamiento.

ARTÍCULO 4to.- Regístrese, comuníquese. Tomen conocimiento las Areas de competencia. Cumplido, archívese.

DADA EN LA SALA DE SESIONES DEL CONSEJO DIRECTIVO A LOS DIEZ DEL MES DE NOVIEMBRE DE DOS MIL DIECISEIS.

RESOLUCION NRO. 325

Lic. Teresa de C. QUINTERO
Sec. Académica Fac. Cs. Exactas Fco-Qcas. y Nat.

Dra. Rosa Irene CATTANA
Decana Fac. Cs. Exactas Fco-Qcas. y Nat.