Declaración de Alhambra EIDOS sobre Auditoría Forense del Sistema Voto Automatizado de la Junta Central Electoral de la República Dominicana:

1. ANALISIS DE EQUIPOS AUDITADOS

Los sistemas auditados, basados en Windows 10 personalizados en su ejecución y seguridad, disponen de un nivel de seguridad, desempeño y tolerancia a fallos que los hacen robustos, fiables y rápidos en su ejecución

2. ANALISIS DE LOGS DE COMUNICACIONES

Analizando el tráfico existente entre el servidor de la base de datos central y sus comunicaciones con el exterior y, con ello, comprobando a través de herramientas principalmente SIEM si hay contenido malicioso que pueda vulnerar el correcto funcionamiento de la plataforma a auditar, se constata que el tráfico de red auditado no contiene ninguna actividad, virus o malware detectado, con lo que no ha habido alteración en el funcionamiento del proceso electoral desde un punto de visto de código malicioso.

3. ANALISIS DEL SOFTWARE

El objetivo del análisis del software SceUrnaVotacion que corría en las estaciones de votación era determinar si este ejecutaba alguna función o tarea más allá de las necesarias para sus funciones de proveedor del servicio de votación automatizada.

Dicho análisis concluye que el sistema impide la realización de tareas maliciosas y además determina un resultado positivo en cuanto al desempeño de sus funciones normales como estación de votación.

Se comprobó que el Código Fuente no puede alterar los resultados o intentar conectar a las personas con sus votos e identificar por quien votó cada uno de los electores. No hallándose indicio alguno de ello. Todo el Código Fuente de manejo de datos hace lo que tiene que hacer y nada más.

4. ANALISIS DE BASE DE DATOS

El análisis de las bases de datos de los 390 equipos, divididos en 13 tandas de 30 mesas cada una, ha tenido un resultado coherente en el escenario auditado.

En Santo Domingo D.N. 31 de Enero de 2020