

**INSTITUTO INTERAMERICANO DE DERECHOS HUMANOS
CENTRO DE ASESORÍA Y PROMOCIÓN ELECTORAL**



IIDH / CAPEL

**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN
ELECTRÓNICA PARA LAS ELECCIONES GENERALES
PARAGUAY 2023**

**INFORME FINAL
Nº. 001-2023-TRIBUNAL SUPERIOR DE JUSTICIA
ELECTORAL(TSJE)**

**POR EL PERÍODO COMPRENDIDO
DEL 27 DE MARZO AL 02 MAYO DE 2023.**



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



TRIBUNAL SUPERIOR DE JUSTICIA ELECTORAL

**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN
ELECTRÓNICA PARA LAS ELECCIONES GENERALES
PARAGUAY 2023**

**INFORME FINAL
Nº. 001-2023-TRIBUNAL SUPERIOR DE JUSTICIA
ELECTORAL(TSJE)**

**POR EL PERÍODO COMPRENDIDO
DEL 27 DE MARZO AL 02 DE MAYO DE 2023.**



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



CONTENIDO

CAPÍTULO I	1
MOTIVOS DE LA AUDITORÍA	1
OBJETIVOS DE LA AUDITORÍA	1
ALCANCE DE LA AUDITORÍA	5
CAPÍTULO II	8
ANTECEDENTES	8
CAPÍTULO III	10
EVALUACIONES REALIZADAS DURANTE LA ETAPA DE EJECUCIÓN DE LA AUDITORÍA	10
EVALUACIÓN DE LA SEGURIDAD	10
PRUEBAS PARA LA REVISIÓN DE LA SEGURIDAD	11
EVALUACIÓN DEL HARDWARE	26
PRUEBAS PARA LA REVISIÓN DEL HARDWARE	28
EVALUACIÓN DEL SOFTWARE	49
PRUEBAS PARA LA REVISIÓN DEL SOFTWARE	51
EVALUACIÓN DE LOS PROCESOS	80
CAPÍTULO IV	103
CONCLUSIONES FINALES	103
AUDITORÍA DE LA SEGURIDAD	103
AUDITORÍA DEL HARDWARE	108
AUDITORÍA DEL SOFTWARE	114
AUDITORÍA DE LOS PROCESOS	119
ANEXOS	125



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



CAPÍTULO I

INFORMACIÓN INTRODUCTORIA

MOTIVOS DE LA AUDITORÍA.

La presente auditoría se realizó en cumplimiento al Convenio de Cooperación internacional entre el Tribunal Superior de Justicia Electoral de Paraguay (TSJE) y el Instituto Interamericano de Derechos Humanos (IIDH)/Centro de Asesoría y Promoción Electoral (CAPEL), el cual tiene como objetivo principal realizar una auditoría y acompañamiento técnico internacional para la evaluación de los sistemas informáticos dispuestos para las elecciones generales del 30 de abril de 2023.

OBJETIVOS DE LA AUDITORÍA.

Los objetivos principales de la auditoría son:

1. Objetivos Generales

1. Realizar una evaluación técnica del sistema de votación electrónica mediante boleta única electrónica (BUE) que será utilizado en las elecciones nacionales y departamentales que se realizarán en Paraguay el 30 de abril de 2023, a fin de valorar su calidad como instrumento para satisfacer las necesidades del proceso electoral.
2. Contar con un diagnóstico que refleje la situación actual del software, del hardware, del nivel de seguridad de la información utilizado en el proceso de votación electrónica.

3. Contar un diagnóstico de los procedimientos y procesos utilizados en el proceso de votación electrónica.
4. Contar con un informe que incluya hallazgos de auditoría y sus recomendaciones para que las autoridades superiores del Tribunal Superior de Justicia Electoral puedan tomar decisiones oportunas.

2. Objetivos específicos

Los objetivos específicos de la auditoría son:

Auditoría del Hardware:

- Evaluar el diseño y construcción para las condiciones particulares de exigencia del proceso electoral.
- Evaluar una operación aislada de cualquier tipo de conectividad con el exterior durante el proceso de votación.
- Evaluar la garantía de voto secreto, sin almacenar información relacionada con el voto de cada elector.
- Evaluar la garantía de integridad (no alteración) de la información de votos registrados electrónicamente durante todo el proceso electoral.
- Evaluar las Condiciones para la continuidad de la operación durante toda la jornada electoral.
- Evaluar que el registro electrónico utilizado no admita lectura a distancia.

Auditoría del Software:

- Evaluar que los procedimientos de diseño, desarrollo y versionado son adecuados.
- Evaluar que los aplicativos desarrollados se encuentren individualizados e identificados en un catálogo que permite validar su integridad.

- Evaluar los esquemas y estándares de seguridad utilizados.
- Evaluar que las capacidades de parametrización se adecúan a los requerimientos.
- Evaluar que se realice una adecuada gestión y control de cambios.
- Evaluar los procesos de control de calidad y pruebas.
- Evaluar que los casos de uso estén completos, detallados y acordes a las necesidades del proceso.
- Evaluar que los casos de prueba sean exhaustivos y estén acordes a los casos de uso.
- Evaluar el análisis de los sistemas desde una perspectiva de desarrollo de software, de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.
- Evaluar la integridad y la consistencia de los datos, de la información transmitida desde las máquinas de votación a las boletas de votación.

Auditoría de la Seguridad:

- Evaluar los controles para arranque seguro de las máquinas de votación.
- Evaluar los controles y niveles de aseguramiento del sistema operativo.
- Evaluar la confidencialidad de la información del elector durante todo el proceso.
- Evaluar los controles de integridad que garantizan la inalterabilidad de la votación.
- Evaluar los controles para garantizar la disponibilidad del sistema de votación durante toda la jornada electoral.
- Realizar análisis de vulnerabilidades.
- Realizar análisis de penetración
- Realizar análisis de código fuente mediante ejecución de pruebas de código estático y dinámico.
- Realizar Pruebas de caja gris.

Auditoría de los Procesos:

- Evaluar el alcance y amplitud del manual del sistema.
- Evaluar la documentación de características funcionales y no funcionales del sistema.
- Evaluar los procedimientos para la carga de los datos de la elección.
- Evaluar los procedimientos para la verificación y validación de las pantallas.
- Evaluar los procedimientos para la verificación de la autenticidad del software a utilizar.
- Evaluar los procedimientos para la distribución y personalización del software a utilizar en cada mesa de votación.
- Evaluar los procedimientos de despliegue y repliegue de las máquinas de votación.
- Evaluar los procedimientos de almacenamiento, distribución y custodia de las máquinas.
- Evaluar los Procedimientos de soporte técnico.
- Evaluar el alcance y amplitud de los manuales de capacitación al electorado.
- Evaluar los procedimientos y herramientas de capacitación al electorado.
- Evaluar el alcance y amplitud de los manuales de capacitación de las autoridades de mesa.
- Evaluar los procedimientos y herramientas de capacitación a las autoridades de mesa.
- Evaluar el alcance y amplitud de los manuales de capacitación al personal técnico de soporte en campo y remoto.
- Evaluar los procedimientos y herramientas de capacitación del personal técnico de soporte en campo y remoto.
- Evaluar los procedimientos y herramientas de capacitación de los operadores técnicos de los sistemas de transmisión, recuento y publicación de resultados
-

ALCANCE DE LA AUDITORÍA

Esta auditoría comprende la revisión del software, hardware, seguridad, procesos y documentación de respaldo presentados por los funcionarios del Tribunal Superior de Justicia Electoral (TSJE) y el Proveedor Grupo MSA, cubriendo el período del 27 de marzo al 02 de mayo del año 2023, con énfasis en la revisión de sistema de votación electrónica y sus componentes. Los rubros que se evaluaron fueron los siguientes:

Rubros Evaluados:

No.	Rubro y/Área a Examinar	Alcance
1	Hardware	Revisión detallada de la arquitectura de las máquinas de votación, análisis documental de su diseño, componentes y funcionamiento. Revisión física y pruebas de cada modelo, incluye verificación de diseño, aislamiento de la máquina, tipos de almacenamiento, tecnología RFID, registro y seguridad, entre otros.
2	Software	Revisión detallada del diseño de software, documentación técnica, documentación de usuario, casos de uso, casos de prueba, QA, sistema operativo, parametrización, control de versiones, control de cambios, custodia de código, pruebas y simulacros.
3	Seguridad	Análisis de vulnerabilidades, análisis de código estático, pruebas de penetración,

		evaluación de integridad, disponibilidad y confidencialidad del ambiente tecnológico y la información, análisis de infraestructura tecnológica, evaluación de la gestión de riesgos.
4	Procesos	Revisión de los procesos de capacitación, soporte técnico, carga de datos, validación de pantallas, aceptación y sellado de versiones, distribución de software, procesos en mesa antes durante y después de las elecciones, verificación de autenticidad del software y revisión de manuales técnicos del sistema, de procedimientos, de capacitación para miembros de mesa, soporte técnico y electorado en general.

Los procedimientos de auditoría aplicados fueron los siguientes:

- a) Entrevistas con el Director de Tecnología de Información y Comunicación del Tribunal Superior de Justicia Electoral (TSJE) y con personal de áreas operativas encargadas del proceso de votación.
- b) Entrevistas con el personal de la Empresa Grupo MSA.
- c) Acompañamiento en las actividades de auditoría de los apoderados técnicos de los partidos políticos sobre el hardware y software de las máquinas de votación. Durante la actividad realizada para ese fin por funcionarios del TSJE y por la Empresa Grupo MSA.

**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**

- d) Las solicitudes de la documentación para realizar la auditoría se realizaron mediante correos electrónicos y de forma verbal.
- e) Examinar el funcionamiento, efectividad y confiabilidad del hardware para determinar la calidad, seguridad y eficiencia de este, utilizando el método de observación y aplicación de cuestionarios a través de entrevistas.
- f) Realización de pruebas para evaluar los componentes, funcionamiento, seguridad del hardware y software, con el objetivo de identificar vulnerabilidades que pudiesen comprometer la confidencialidad, integridad y disponibilidad de la información y, por ende, afectar el proceso de votación, utilizando el método de realización de pruebas in situ y con la aplicación de herramientas de hackeo ético.
- g) Revisión analítica de la documentación correspondiente al proceso de votación, con el objetivo de identificar la ausencia o debilidades de controles en las etapas de dicho proceso y así como determinar oportunidades de mejoras.

CAPÍTULO II

ANTECEDENTES

El Centro de Asesoría y Promoción Electoral (CAPEL) es un programa especializado del Instituto Interamericano de Derechos Humanos (IIDH). Fue creado en 1983 e inició sus labores en el mes de febrero de 1985.

El Estatuto del Centro establece que sus fines serán la asesoría técnica electoral y la promoción de las elecciones, con un enfoque multidisciplinario, labor que ha realizado con organismos electorales, poderes legislativos, organizaciones de la sociedad civil y partidos políticos. Establece también que el IIDH/CAPEL sustentará su acción en *“el principio de las elecciones libres como parte esencial de la teoría y práctica de los derechos humanos, condición de la democracia y fundamento del derecho a la libre determinación y de la paz en la convivencia nacional e internacional”*. En la actualidad CAPEL ejecuta los programas relacionados con derechos políticos y participación política que acoge el Instituto Interamericano de Derechos Humanos (IIDH).

El IIDH/CAPEL ha contribuido a fortalecer los procesos democráticos del Continente Americano, privilegiando, como un mecanismo para acompañar la reinserción de sus países a los procesos electorales, el fortalecimiento de los organismos electorales, a través de programas de asistencia técnica, de cooperación horizontal entre estos organismos y de campañas cívicas para el desarrollo de una cultura política democrática.

CAPEL ha propiciado el establecimiento de políticas de intercambio y transmisión de experiencias y conocimientos, lo cual permitió acuñar la expresión y desarrollar el instrumento de la cooperación horizontal en materia de asistencia técnica, de cuya utilidad han sido testigos y beneficiarios los representantes de los organismos electorales miembros de las Asociaciones Protocolo de Tikal, Protocolo de Quito y la Unión Interamericana.

El 08 de marzo de 2023 se firmó el Convenio de cooperación sobre la Auditoría técnica del sistema de votación electrónica para las Elecciones Generales y Departamentales en Paraguay 2023, entre el Centro de Asesoría y Promoción



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



Electoral del Instituto Interamericano de Derechos Humanos (IIDH-CAPEL) y el Tribunal Superior de Justicia Electoral de Paraguay. Con el objetivo de realizar una evaluación técnica del sistema de votación electrónica mediante la boleta única electrónica (BUE) que será utilizado en las Elecciones Generales y Departamentales 2023, a fin de valorar su calidad como instrumento para satisfacer las necesidades del proceso electoral.

El alcance del proyecto corresponde a la realización de una auditoría técnica de rigor internacional sobre el sistema de votación electrónica que se utilizará en las Elecciones Generales y Departamentales, organizada en 4 etapas, planificación, trabajo de campo, presentación de informe de hallazgos y recomendaciones y seguimiento a través del acompañamiento hasta las elecciones. En cada una de las etapas participará un grupo de especialistas seleccionados de acuerdo con su perfil profesional y experiencia en procesos electorales de diversos países del continente americano.

CAPÍTULO III

EVALUACIONES REALIZADAS DURANTE LA ETAPA DE EJECUCIÓN DE LA AUDITORÍA

EVALUACIÓN DE LA SEGURIDAD

Durante la evaluación de la seguridad del software y hardware de las máquinas de votación (Modelo P2 y P6), se aplicaron instrumentos de investigación y herramientas de análisis de vulnerabilidades, de captura de información y la utilización de dispositivos de hackeo ético, con el objetivo de disminuir riesgos y detectar posibles problemas y amenazas de seguridad que puedan afectar el proceso de votación. A continuación, se describen las actividades más relevantes realizadas en esta evaluación:

- Se realizó un análisis de vulnerabilidades al software de ambos modelos de máquinas de votación, para identificar debilidades, brechas de seguridad, errores de configuración y puntos de entrada de accesos inseguros a la aplicación.
- Se realizaron análisis de código estático, utilizando diferentes métodos de análisis sobre el código fuente del software de ambos modelos de las máquinas de votación, con el objetivo de identificar problemas potenciales
- Se realizaron pruebas de penetración al software de ambos modelos de las máquinas de votación con el objetivo de identificar vulnerabilidades que un atacante podría explotar durante el proceso de votación.
- Se aplicaron herramientas de hackeo ético al software de ambos modelos de las máquinas de votación, con el objetivo de evaluar la integridad, confidencialidad y disponibilidad de la información contenida en los chips.

- Se evaluaron los controles existentes para determinar si ambos modelos de las máquinas de votación cuentan con un arranque seguro del sistema operativo.
- Se utilizaron dispositivos de hardware para realizar hackeo ético, para determinar el nivel de seguridad de la información del software de ambos modelos de las máquinas de votación.

PRUEBAS PARA LA REVISIÓN DE LA SEGURIDAD

PRUEBA 1.

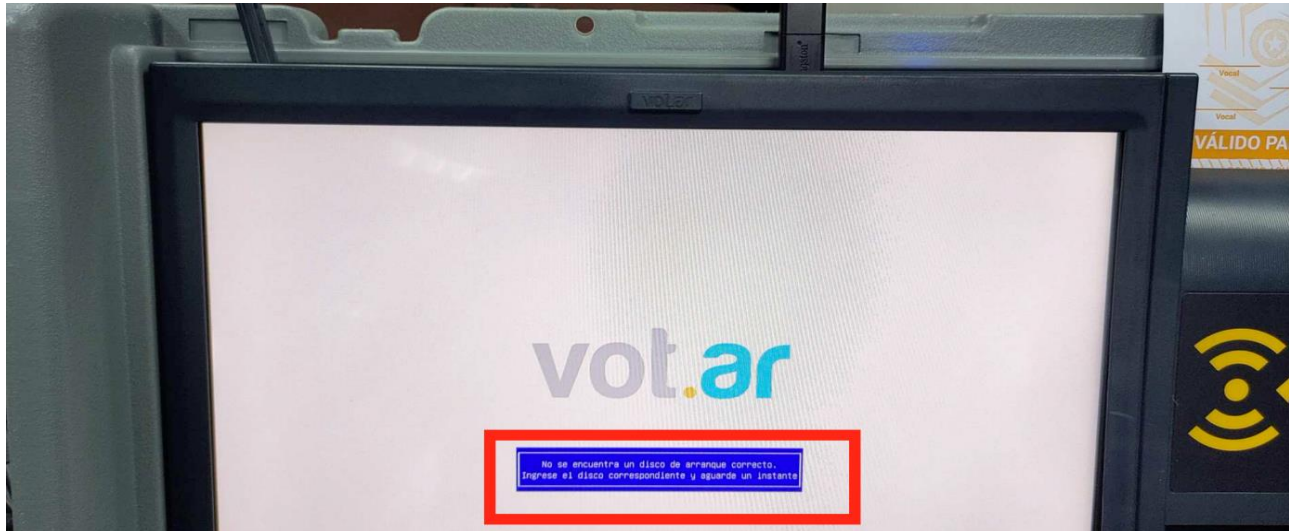
PRUEBA DE ARRANQUE SEGURO.

Objetivo de la Prueba

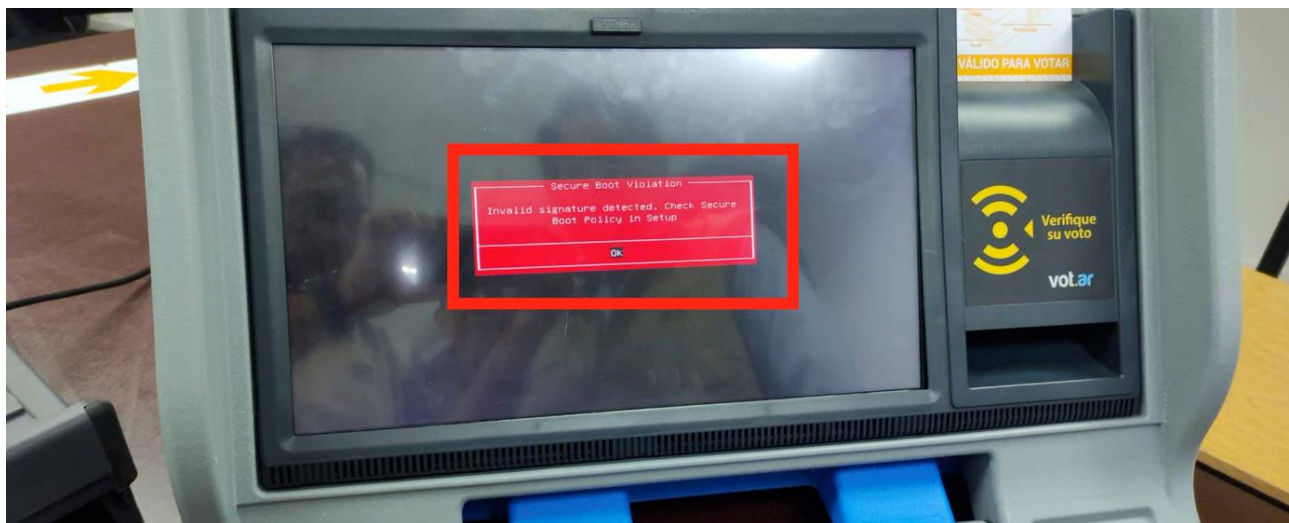
Evaluar los controles para arranque seguro de las máquinas de votación.

Descripción de la Prueba:

La prueba inicia probando el inicio de un equipo de votación con un dispositivo USB no autorizado, distinto al disco liveDVD usado por la máquina para el arranque.



La siguiente prueba fue realizada con un DVD de arranque del sistema operativo Debian. El resultado fue, un mensaje de advertencia de que la firma del disco es incorrecta.



Otra prueba fue alterar el contenido del disco liveDVD que usa la máquina de votación y validar si arranca.

```
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 25.563634] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0700 phys_seg 1 prio class 0
[ 25.613096] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 25.627584] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 25.650211] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 26.684134] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 27.724928] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0700 phys_seg 1 prio class 0
[ 27.764911] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 27.776427] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 27.802156] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 28.848971] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0700 phys_seg 1 prio class 0
[ 28.889069] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 28.901981] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 28.926774] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 29.976168] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 31.029425] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0700 phys_seg 1 prio class 0
[ 31.073439] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 31.089912] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 31.115471] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 32.158347] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 33.205647] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0700 phys_seg 1 prio class 0
[ 33.249077] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 33.264749] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 33.288869] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 34.323230] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 35.369084] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0700 phys_seg 1 prio class 0
[ 35.409002] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 35.424907] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 35.450250] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 36.488689] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 37.537048] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0700 phys_seg 1 prio class 0
[ 37.577607] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 37.594827] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 37.618986] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
```

El resultado fue un conjunto de errores y un reinicio del sistema operativo antes de que el sistema se encuentre funcional.

Resultados de la prueba:

Mediante estas pruebas, se pudo comprobar que la máquina de votación realiza una validación de los medios de arranque, y no permite iniciar desde medios no autorizados.

PRUEBA 2.

PRUEBA DE GARANTÍA DE INTEGRIDAD.

Objetivo de la Prueba

Evaluar la garantía de integridad (no alteración) de la información de votos registrados electrónicamente durante todo el proceso electoral

Descripción de la Prueba:

La prueba inicia leyendo las boletas con un dispositivo de lectura RFID, y posteriormente replicando esta lectura a las máquinas de votación.





AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



De la misma manera que se replicó los datos de las boletas, se modificó el contenido de la data del tag de la boleta por contenido aleatorio, no se obtuvo ninguna respuesta por parte de las máquinas al momento de acercar al lector el equipo de replicación.

Se pudo identificar en el código las funciones donde se puede comprobar el cifrado del contenido de la boleta.

```
def encriptar_voto(aes_key, serial_number, data):
    """Funcion de alto nivel para encriptar un voto.

    Argumentos:
    ... aes_key -- un stream de 16 bytes con la clave de encriptación.
    ... serial_number -- un stream de 8 bytes con el serial_number del tag.
    ... data -- el stream de bytes que queremos encriptar.
    """
    ret = data
    # si no queremos encriptar el voto devolvemos los datos que nos mandaron
    if ENCRYPTAR_VOTO:
        # El vector tiene que tener 12 bytes así que le agregamos 4 bytes como
        # padding
        init_vector = serial_number + PADDING_SERIAL
        gcm_tag, data_encryptada = encriptar(aes_key, init_vector, data)
        # armamos un container de construct para armar el voto con el formato
        # correcto
        contenedor = Container(gcm_tag=gcm_tag, len_datos=len(data_encryptada),
                               datos=data_encryptada)
        ret = struct_voto.build(contenedor)
    return ret
```


PRUEBA 3.

PRUEBA DE LECTURA A DISTANCIA

Objetivo de la Prueba

Evaluar el registro electrónico utilizado no admita lectura a distancia.

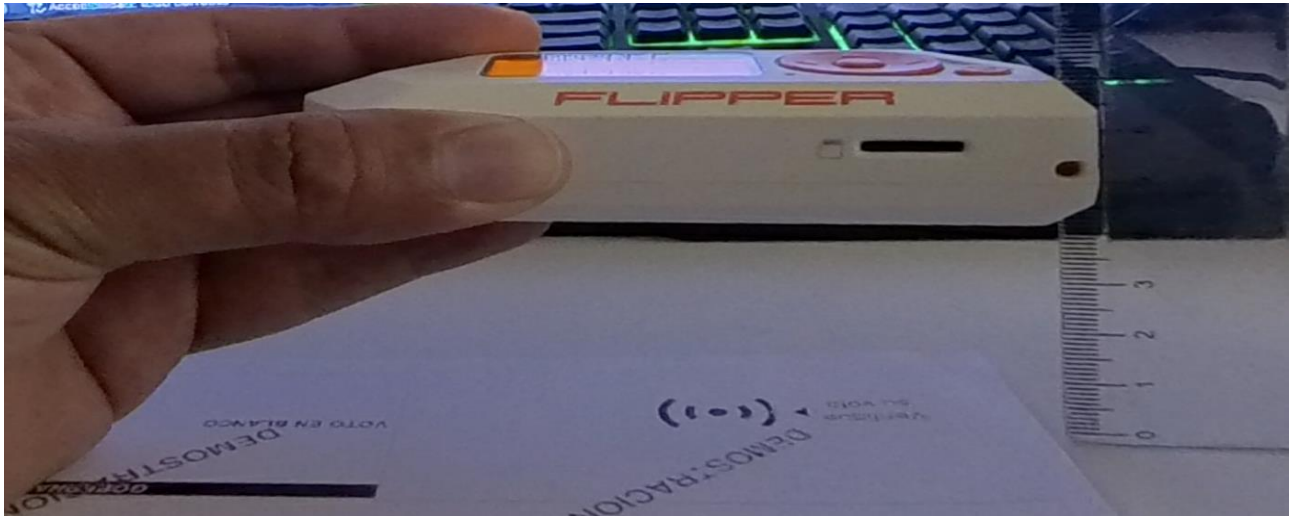
Descripción de la Prueba:

Para la prueba se utilizó un dispositivo específico de análisis y auditoría de tecnologías RFID.

El equipo utilizado, si pudo leer las boletas a una muy corta distancia.



Se hicieron varias lecturas y se pudo identificar que a una distancia aproximada de 4 cm. Es posible leer la boleta.



Sin embargo, ampliando el rango a una distancia superior a 4 cm, la lectura no es posible.

En esta fotografía se puede ver que aun cuando la boleta está bajo el dispositivo de lectura, este no puede leer el contenido de la boleta, la distancia aproximada es de 8 cm.



Resultados de la prueba:

Mediante esta prueba se comprobó que no es posible realizar a través de dispositivos portátiles una lectura a distancia de las boletas. Cabe destacar que no se realizaron pruebas con antenas de gran tamaño, amplificadores de señal u otro equipo similar, ya que se considera que la probabilidad de que alguien instale este tipo de equipos en los lugares de votación sin ser detectado por el personal de la entidad electoral o la fuerza pública es muy baja.

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.

PRUEBA 4.

PRUEBA DE OPERACIÓN AISLADA

Objetivo de la Prueba

Evaluar una operación aislada de cualquier tipo de conectividad con el exterior durante el proceso de votación.

Descripción de la Prueba:

La prueba inicia con una identificación visual de puertos de conexión físicos que permitan transmisión de datos.

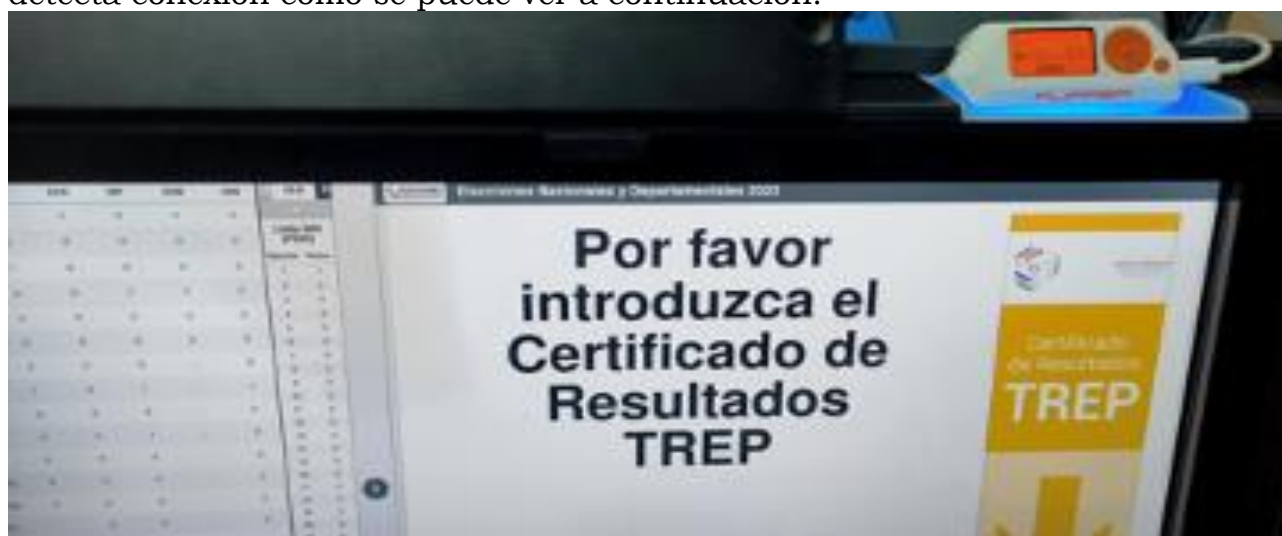


En los dos equipos se identificó puertos USB y un puerto de red.

En el caso del equipo modelo P4, se pudo comprobar que el puerto USB se encuentra energizado, se realizó una prueba para determinar si había la posibilidad de cerrar la aplicación y acceder a la línea de comandos usando fuerza bruta de combinación de teclas. No se obtuvo el acceso no autorizado.



En el equipo modelo P6 se pudo comprobar que el puerto USB está deshabilitado de manera física, el puerto no está energizado y el dispositivo de prueba no detecta conexión como se puede ver a continuación.



En ambos casos, se realizó la ejecución de un ataque de fuerza bruta con un dispositivo badUSB, sin obtener ejecución de los payloads en ninguna de las máquinas evaluadas.

También se identificó el puerto de red en las dos máquinas evaluadas, para identificar posibles conexiones a través de este puerto se utilizó un sniffer de red conectado a la máquina de votación.





AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



Se pudo evidenciar que en las máquinas modelos P4 y P6 los puertos de red no se activan al conectar el cable de red. Se probó conectando un sniffer y conectando directamente a un puerto del switch.

No existe otro tipo de puerto en la máquina de votación que permita algún tipo de conexión o transferencia de datos.

Resultados de la prueba:

Mediante esta prueba se comprobó que los puertos de conexión no están habilitados para acceso externo y proporciona una operación aislada.

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.

PRUEBA 5.

PRUEBA DE VOTO SECRETO SIN ALMACENAR INFORMACIÓN DEL VOTO Y DE LOS ELECTORES

Objetivo de la Prueba

Evaluar la garantía de voto secreto, sin almacenar información relacionada con el voto de cada elector

Descripción de la Prueba:

La prueba inicia con un análisis visual de las placas principales de los dos equipos, no se identificaron dispositivos de almacenamiento persistente.



Además, se pudo comprobar que al conectar dispositivos de almacenamiento USB estos no son energizados en el caso de la máquina P6 y en el caso de la máquina modelo P4, si se energiza, pero no hay interacción con el sistema operativo.

Máquina Modelo P4



Máquina Modelo P6



Resultados de la prueba:

Mediante esta prueba se comprobó que no existen dispositivos de almacenamiento persistente en la máquina de votación.

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.

EVALUACIÓN DEL HARDWARE

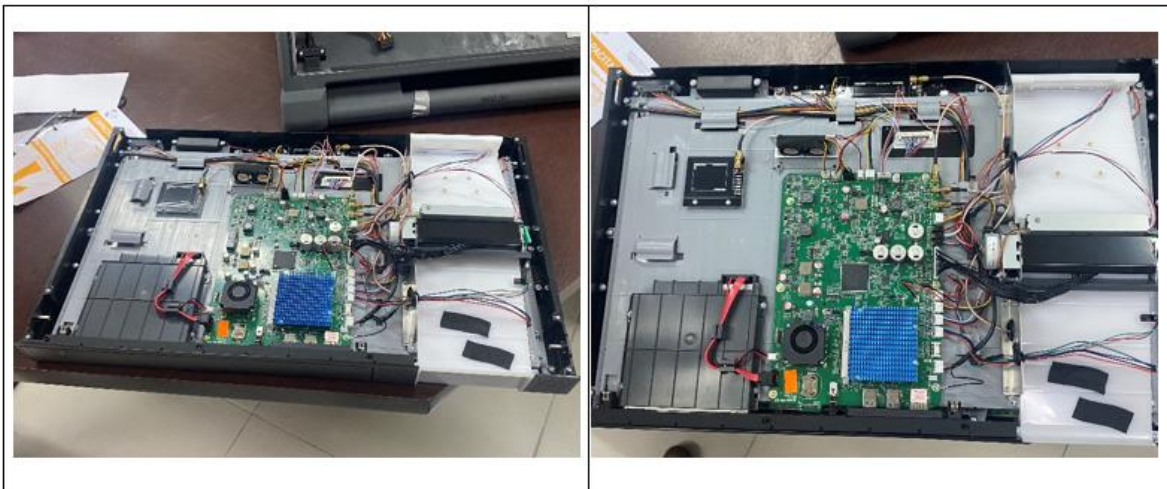
Durante la revisión y evaluación del hardware de las máquinas de votación (Modelo P4 y P6), se realizó la observación del funcionamiento de las máquinas y se aplicaron instrumentos de investigación, con el objetivo de conocer sus características, sus especificaciones técnicas, y a la vez, evaluar su diseño y construcción. A continuación, se describen los aspectos más importantes tomados en cuenta durante este proceso:

- Se evaluó el diseño y construcción de las máquinas para asegurarse que cumplieran con las condiciones y exigencias del proceso electoral. Se verificó si el hardware cuenta con periféricos propietarios y personalizados o comerciales con el fin de determinar la posibilidad de una replicación de estas máquinas de votación en el mercado.
- Se evaluó, si es posible establecer algún tipo de conectividad externa con ambos modelos de las máquinas de votación, para comprobar si existe la posibilidad de realizar un ataque remoto o si puede existir una brecha de seguridad, y a su vez, se verificó si los chips donde se registran los votos, pueden ser leídos a corta o larga distancia poniendo en riesgo la confidencialidad de la información.
- Se evaluó, si ambos modelos de las máquinas de votación cuentan con un medio o hardware de almacenamiento de información, que pudiera poner en riesgo la garantía del voto secreto y a su vez, exista la probabilidad de

poder realizar una alteración de la información correspondiente a los votos registrados electrónicamente durante el proceso electoral.

- Se evaluó, la documentación técnica de ambos modelos de las máquinas de votación, para determinar, si su arquitectura y si, sus componentes fueron creados siguiendo estándares internacionales aplicables.
- Se evaluó, si ambos modelos de las máquinas de votación cuentan con las condiciones de alta disponibilidad, para garantizar la continuidad de las operaciones durante toda la jornada electoral.

Para realizar las diferentes evaluaciones, se le solicitó al personal de la empresa Grupo MSA, abrir y desarmar las máquinas de votación, a continuación, se muestran algunas fotografías:





PRUEBAS PARA LA REVISIÓN DEL HARDWARE

PRUEBA 1.

PROBAR LA EXISTENCIA DE FECHAS EN EL HARDWARE Y VERIFICAR SI LA FECHA ES ESCRITA EN LAS BOLETAS DE VOTACIÓN.

Objetivo de la Prueba

Acceder por medio de la utilidad de mantenimiento y/o pruebas para la consulta de la fecha actual.

Verificación en las boletas impresas, que están no hagan referencia a una marca de tiempo de algún tipo.

La lectura de chip de la boleta para presentación en pantalla.

Descripción de la Prueba:

Se revisa primero la boleta que se imprime desde la utilidad de mantenimiento de la terminal para verificar si existe fecha y hora.

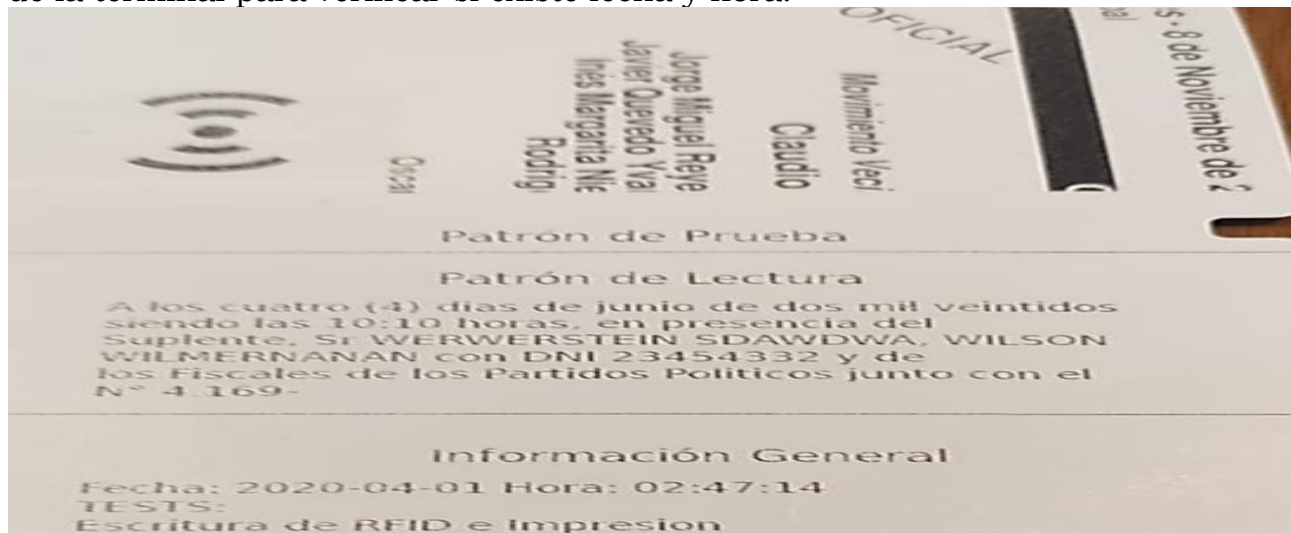


Fig 1. Boleta de mantenimiento.

En la boleta que se imprime de mantenimiento se evidencia una fecha, pero no es una fecha actualizada, esto se genera porque todo equipo de cómputo debe tener una fecha para poder funcionar y esta fecha hace referencia a la fabricación y/o versión de firmware, en este caso, una fecha actualizada no es almacenada en el equipo por el mismo principio de no “almacenar información”.

AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

En el siguiente escenario se verifican que las boletas no tengan ningún tipo de referencia en tiempo, esto verificándolo tanto en la boleta física como en pantalla.

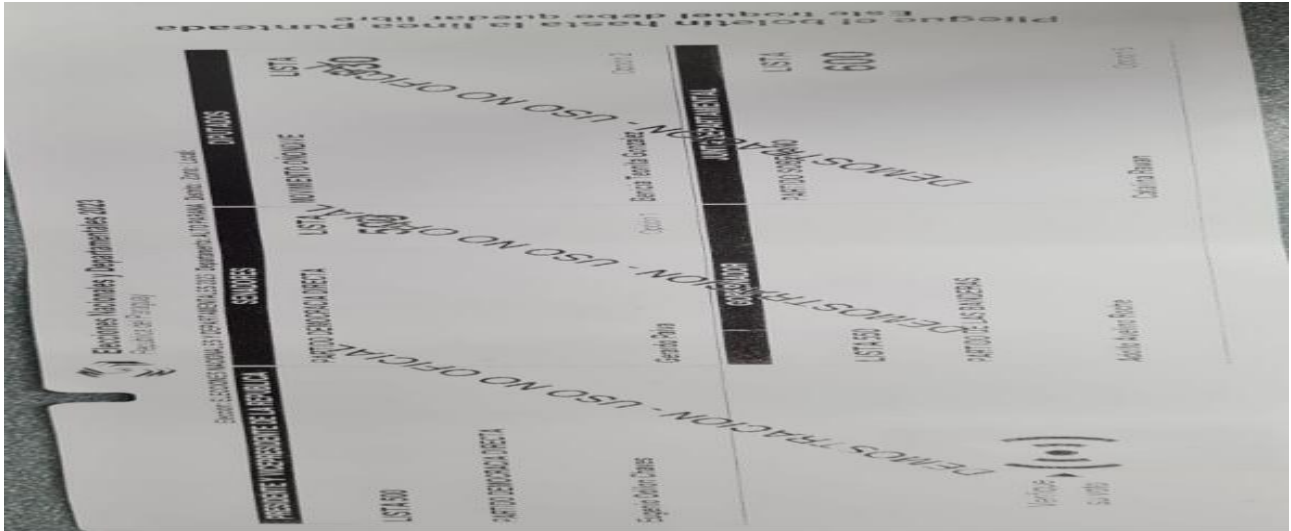


Fig 2. Boleta de votación, sin evidencia de fecha impresa.

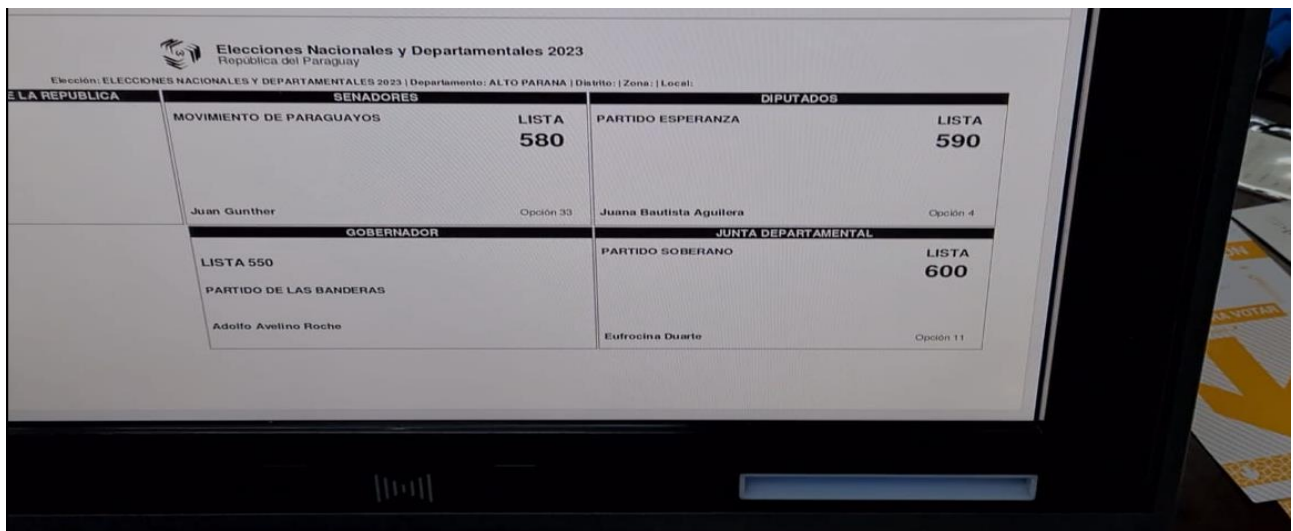


Fig 3. Boleta de votación, sin evidencia de fecha en pantalla.

Resultados de la prueba:

En la utilidad de mantenimiento solo se presenta la fecha y hora de fabricación, no se tiene una fecha actualizada, la fecha siempre se reinicia a la fecha de fabricación de la placa de cómputo cuando se enciende el equipo.

Se revisaron la impresión de las boletas de votación y estas no tienen fecha de creación en ninguno de los casos, de igual forma la lectura del chip no presenta tampoco una fecha de creación en pantalla.

PRUEBA 2.

PROBAR EL USO DE EQUIPOS CELULARES PARA LA LECTURA A DISTANCIA EN LA ZONA DEL EQUIPO DE VOTACIÓN

Objetivo de la Prueba

Usar un dispositivo común como un celular para capturar información de los chips pasivos a una distancia.

Descripción de la Prueba:

Para estas pruebas se realizó por medio de dos celulares marca Samsung modelos S20 FE y S8, la aplicación NFC Taginfo, y se usaron unas cajas plásticas de distancias de 1cm y 3cm respectivamente. Se ubicaron los dispositivos móviles de una forma paralela al chip RFID y se observó en varios intentos si se pudiera leer el chip, la distancia máxima usada fue 4 cm (usando el recipiente de 3cm y el de 1cm apilado).

En el caso de la boleta de votación y usando el Samsung S8:



Fig 1. Boleta de votación usada.



Fig.2. Distancia de 1 cm.



Fig 3. Lectura exitosa al primer intento.

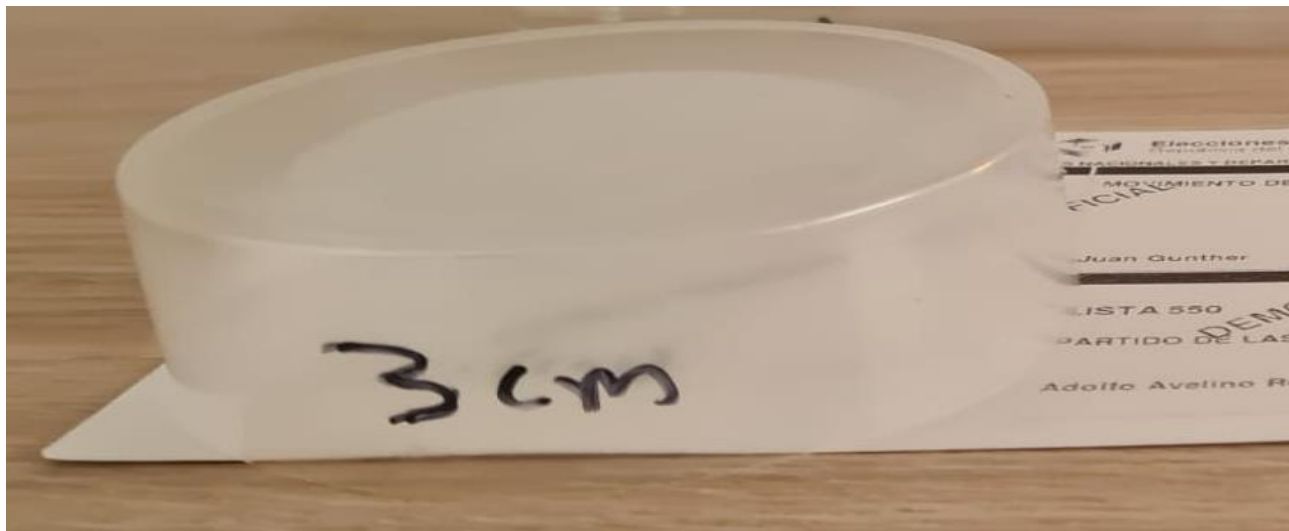


Fig 4. Distancia de 3 cm.



Fig 5. Detección no exitosa a 3 cm.

En el caso de la boleta TREP y usando el Samsung S8:

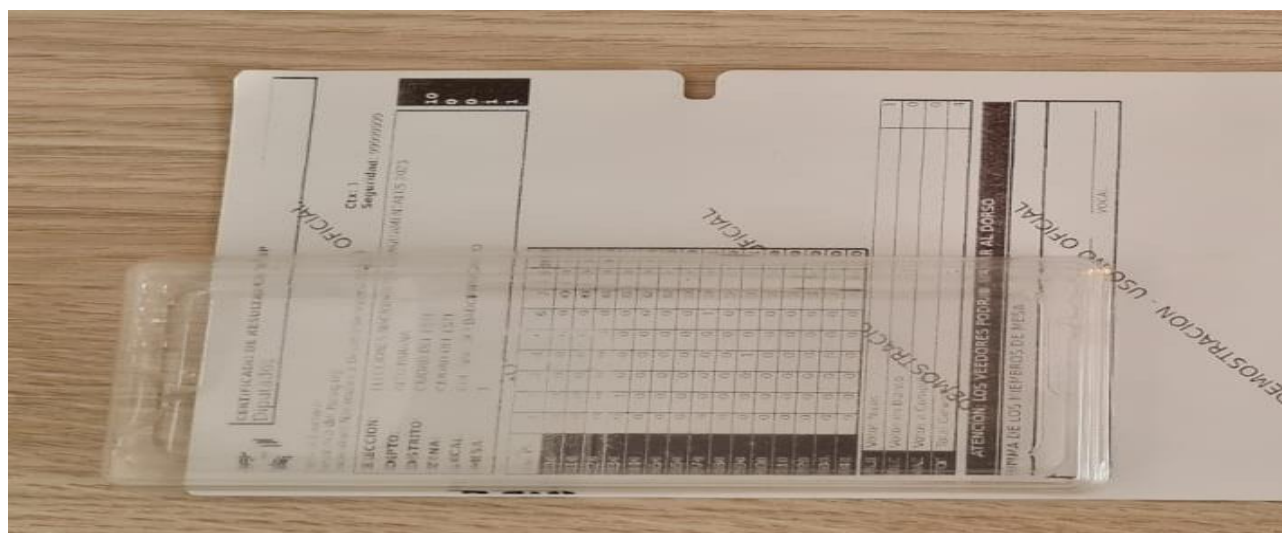


Fig 6. Boleta TREP.

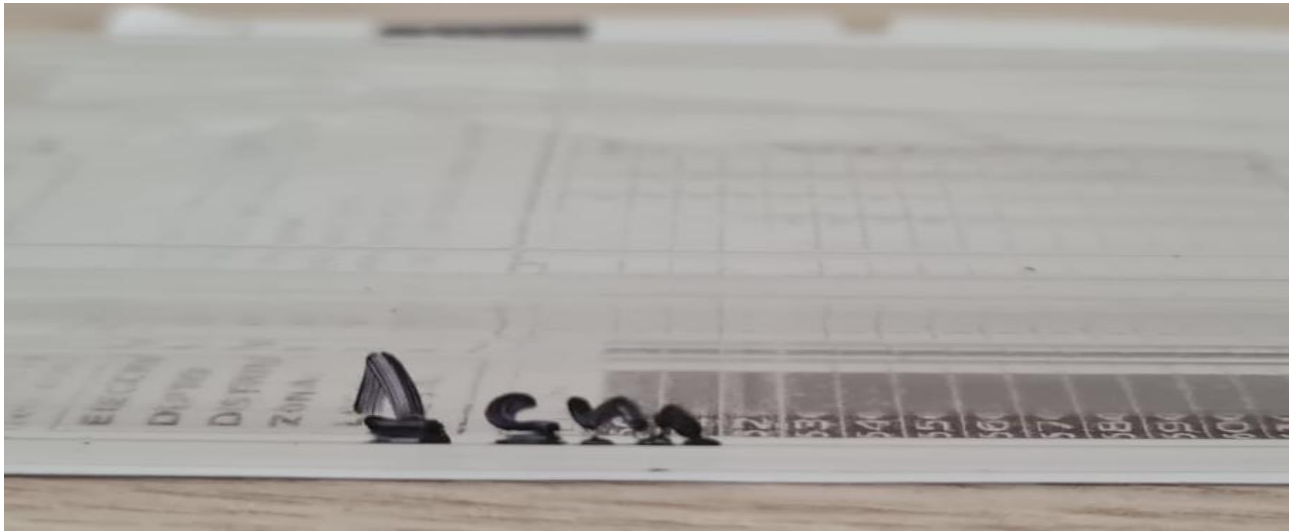


Fig 7. Boleta TREP a 1 cm.



Fig 8. Lectura Exitosa al primer intento.

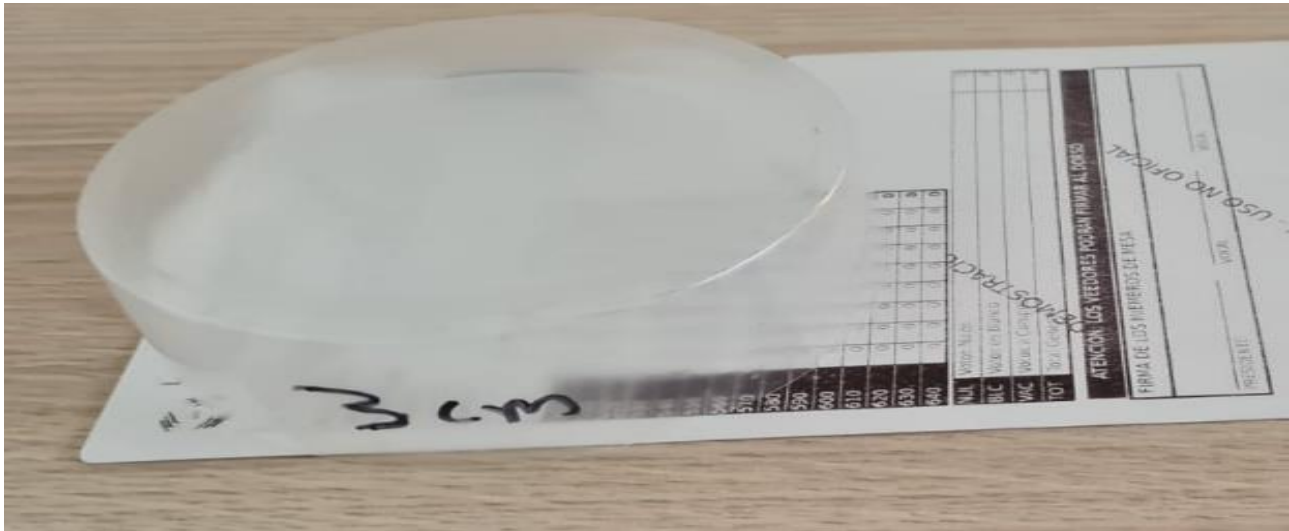


Fig 9. Distancia de 3cm.



Fig 10. Lectura inestable a 3cm.

Se realizan las mismas pruebas, pero en este caso con un Samsung S20 FE:

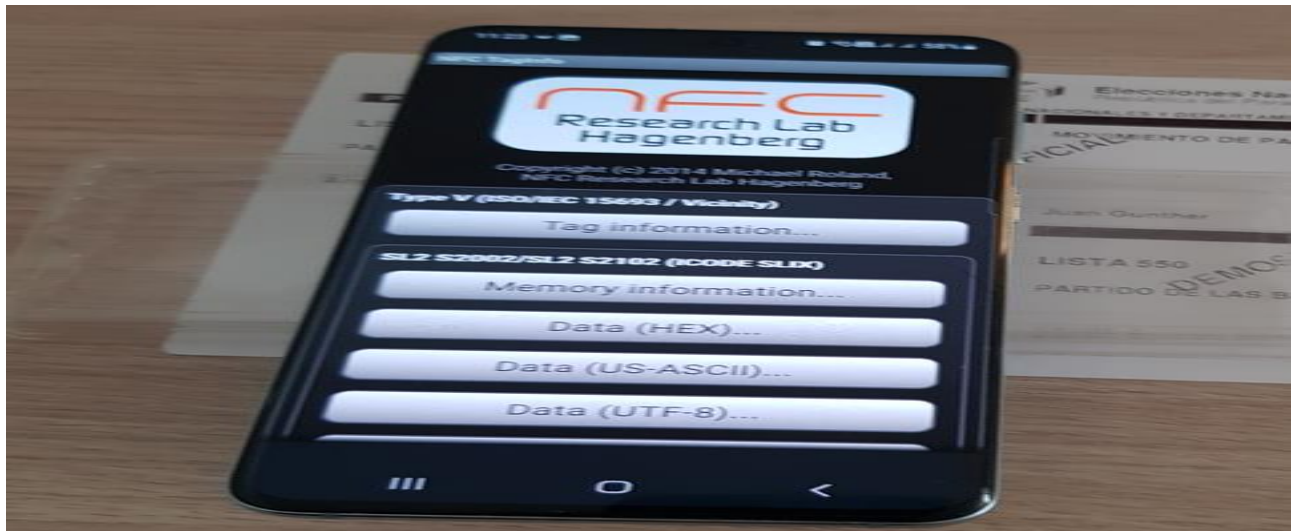


Fig 11. Lectura exitosa al primer intento boleta de votación a 1 cm.

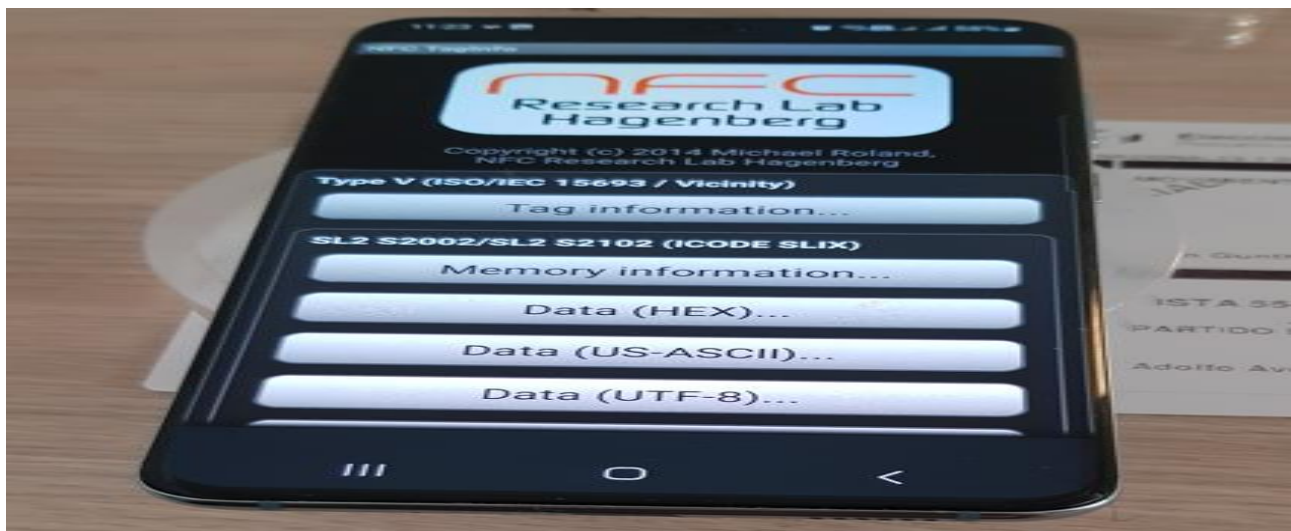


Fig 12. Lectura exitosa al primer intento boleta de votación a 3 cm.



Fig 13. Lectura no exitosa boleta de votación a 4 cm.

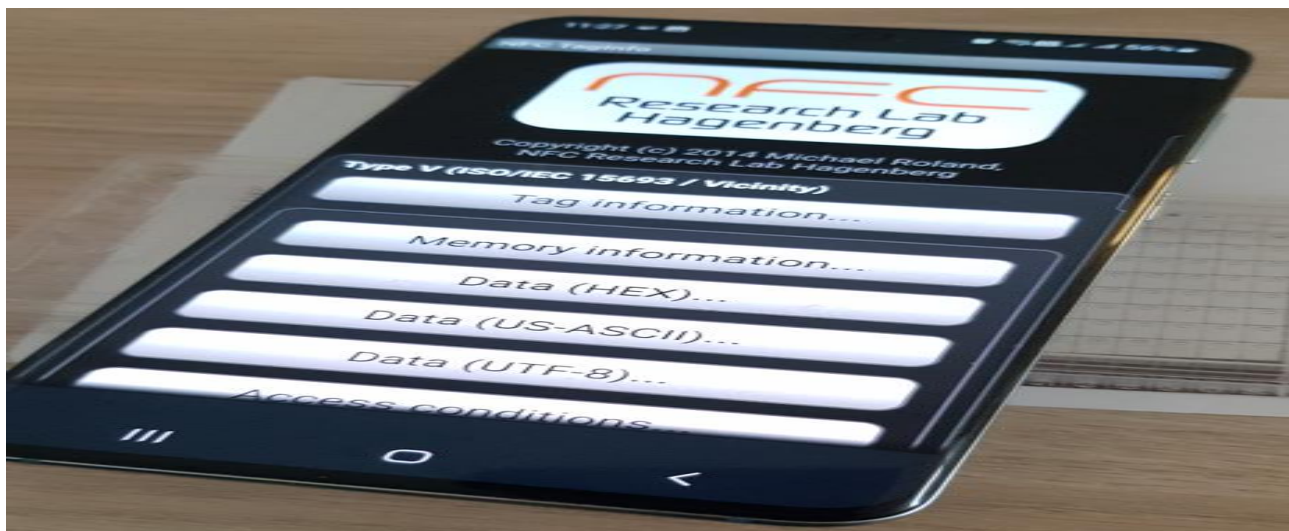


Fig 14. Lectura exitosa al primer intento boleta TREP a 1 cm.



Fig 15. Lectura exitosa al primer intento boleta TREP a 3 cm.

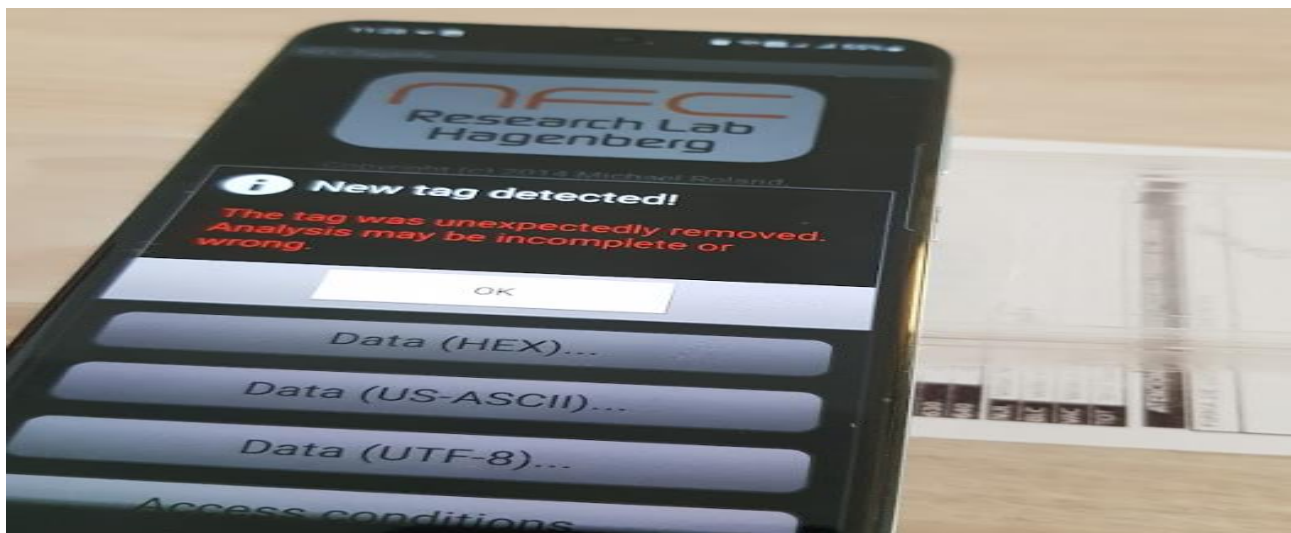


Fig 16. Lectura inestable a 4cm.

Resultados de la prueba:

Se concluye que desde un equipo como un lector NFC de un celular la única forma de capturar datos es a una distancia de menos de 4 cm y en un escenario estable sin movimiento, con esto se garantiza que las boletas no serán leídas a distancia.

Según el estándar y teniendo tecnología especializada se puede obtener datos a 1mts de distancia, y si aún existiera una antena conectada a un dispositivo de mucha potencia, obtener los datos de la boleta no serían interpretados por que esta información está cifrada para garantizar el secreto del voto.

PRUEBA 3.

PRUEBAS DE MODIFICACIÓN DE LOS BOLETAS O BOLETINES.

Objetivo de la Prueba

Constatar que las boletas de votación o TREP no se pueden modificar.

Descripción de la Prueba:

Crear en el terminal de votación una boleta y un boletín, posteriormente usar una aplicación nfc desde el celular para enviar los comandos necesarios para la modificación de la información.

Para estas pruebas se realizó por medio de un celular Samsung S20 FE, y dos aplicaciones que son NFC tools(free) y NFC Taginfo, por medio de NFC Tool, nos permite enviar comandos personalizados al chip y NFC Taginfo, nos permite revisar la información al detalle del chip RFID, su estado, y el contenido de sus bloques.

Se usa como referencia los comandos descritos en la siguiente tabla:

Table 16. Command codes

Command code standard	Function
01h	Inventory
02h	Stay Quiet
20h	Read Single Block
21h	Write Single Block
23h	Read Multiple Block
25h	Select
26h	Reset to Ready
27h	Write AFI
28h	Lock AFI
29h	Write DSFID
2Ah	Lock DSFID
2Bh	Get System Info

Command code custom	Function
2Ch	Get Multiple Block Security Status
B1h	Write-sector Password
B2h	Lock-sector Password
B3h	Present-sector Password
C0h	Fast Read Single Block
C1h	Fast Inventory Initiated
C2h	Fast Initiate
C3h	Fast Read Multiple Block
D1h	Inventory Initiated
D2h	Initiate

Tabla 1 obtenida de:

https://www.st.com/resource/en/application_note/an3163-configuring-your-iso-15693-reader-to-support-the-m24lrxxr-and-m24lrxxer-devices-stmicroelectronics.pdf

Se crea una boleta en la terminal de votación, y un boletín trep, en el caso de la boleta de votación utiliza un chip rfid de 28 bloques de marca NXP y para el trep es de 80 bloques marca ST.

Posteriormente, se usa el NFC Taginfo para entregar la siguiente información con respecto la boleta de votación.



Fig 1. Información del CHIP RFID Boleta de votación.

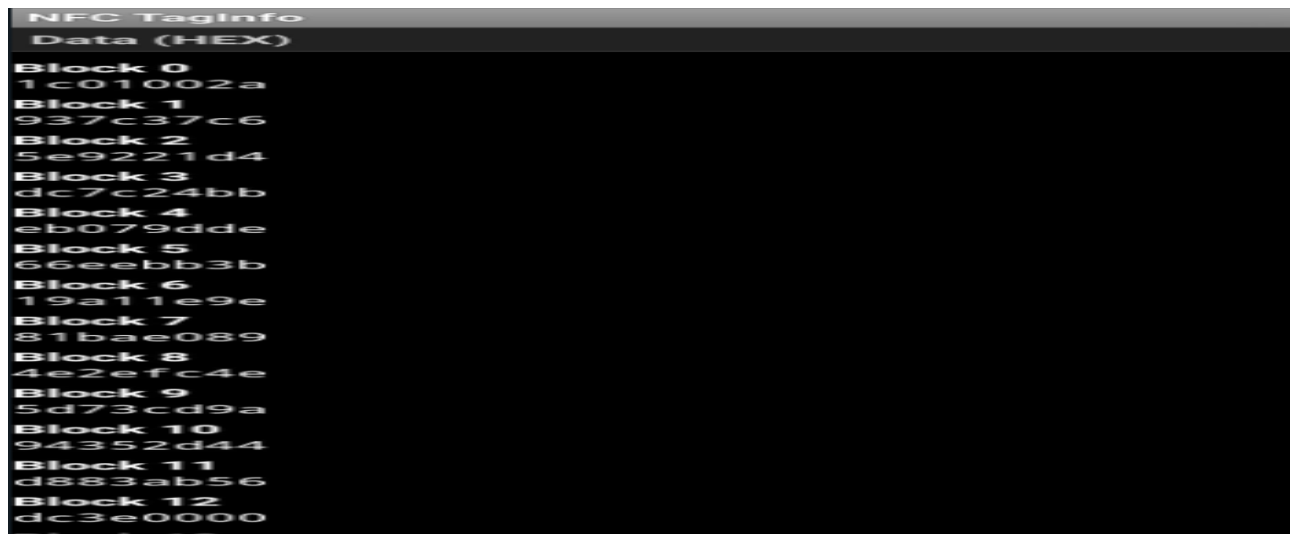


Fig 2. Información escrita en el Chip RFID de boleta de votación.

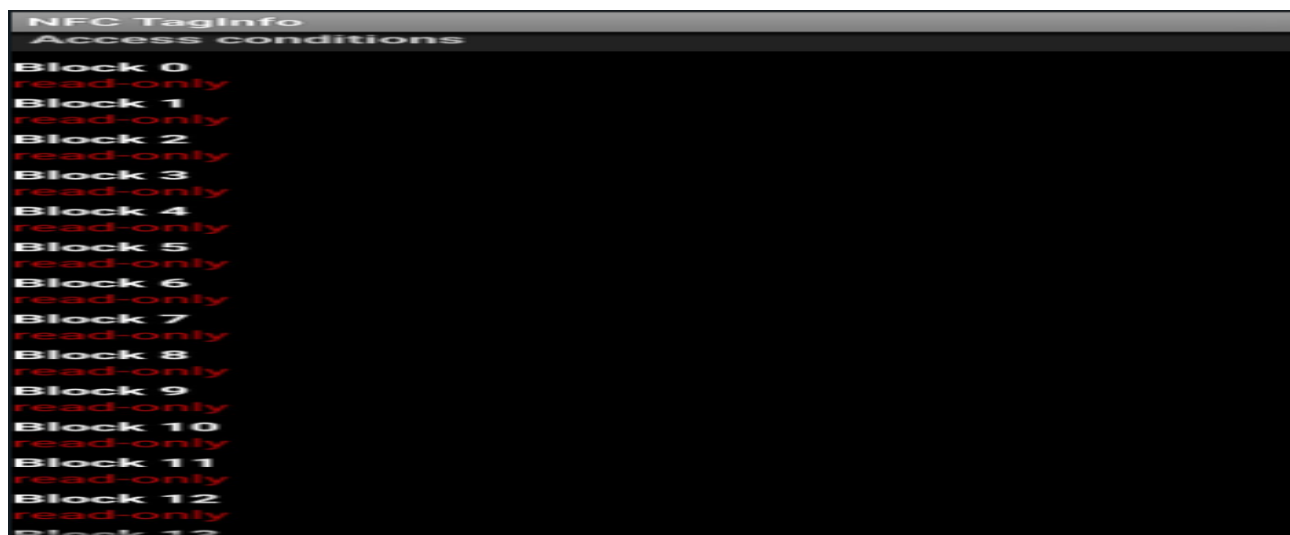


Fig 3. Estado de los bloques del Chip RFID de la boleta de votación.

A Continuación, se realizan las pruebas por medio de NFC Tools, se usan comandos de escritura y lectura, para verificar que los datos no se modifiquen.

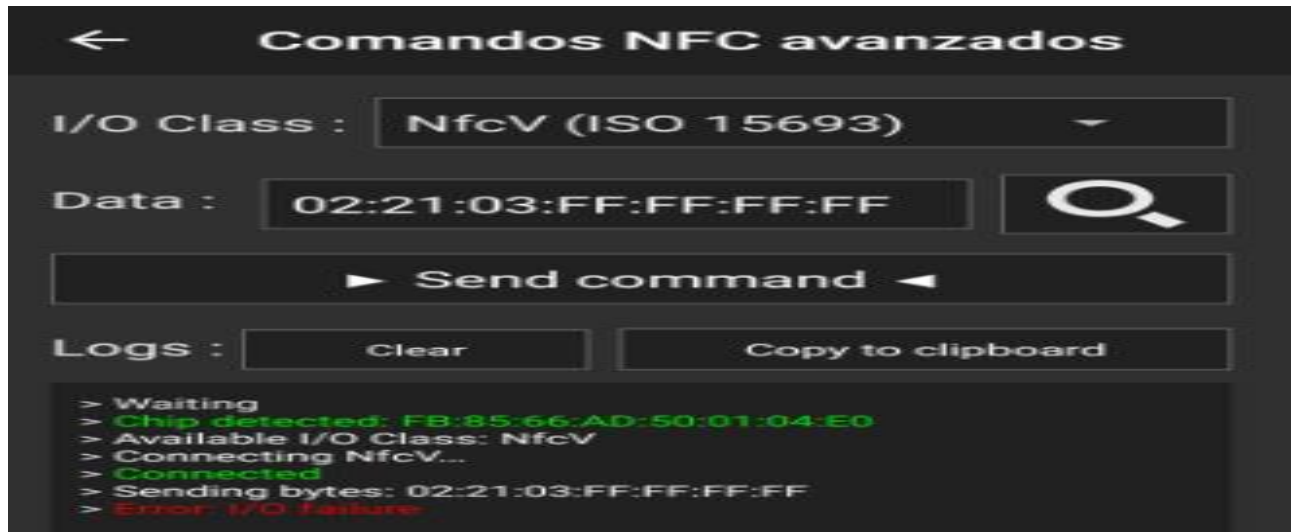


Fig 4. Prueba de escritura del bloque 3 en el CHIP RFID de la boleta de votación no exitosa.

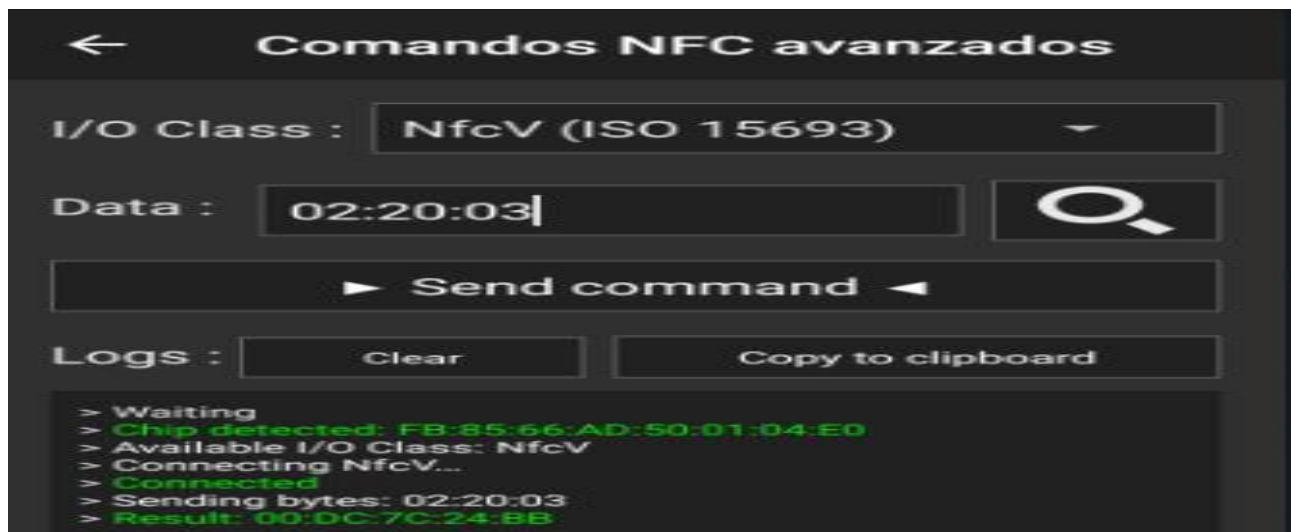


Fig 5. Prueba de lectura del bloque 3 en el CHIP RFID de la boleta de votación, resultado exitoso, el mismo del bloque 3 en la Fig 2.

Con respecto a la boleta TREP se realiza el mismo ejercicio anterior.

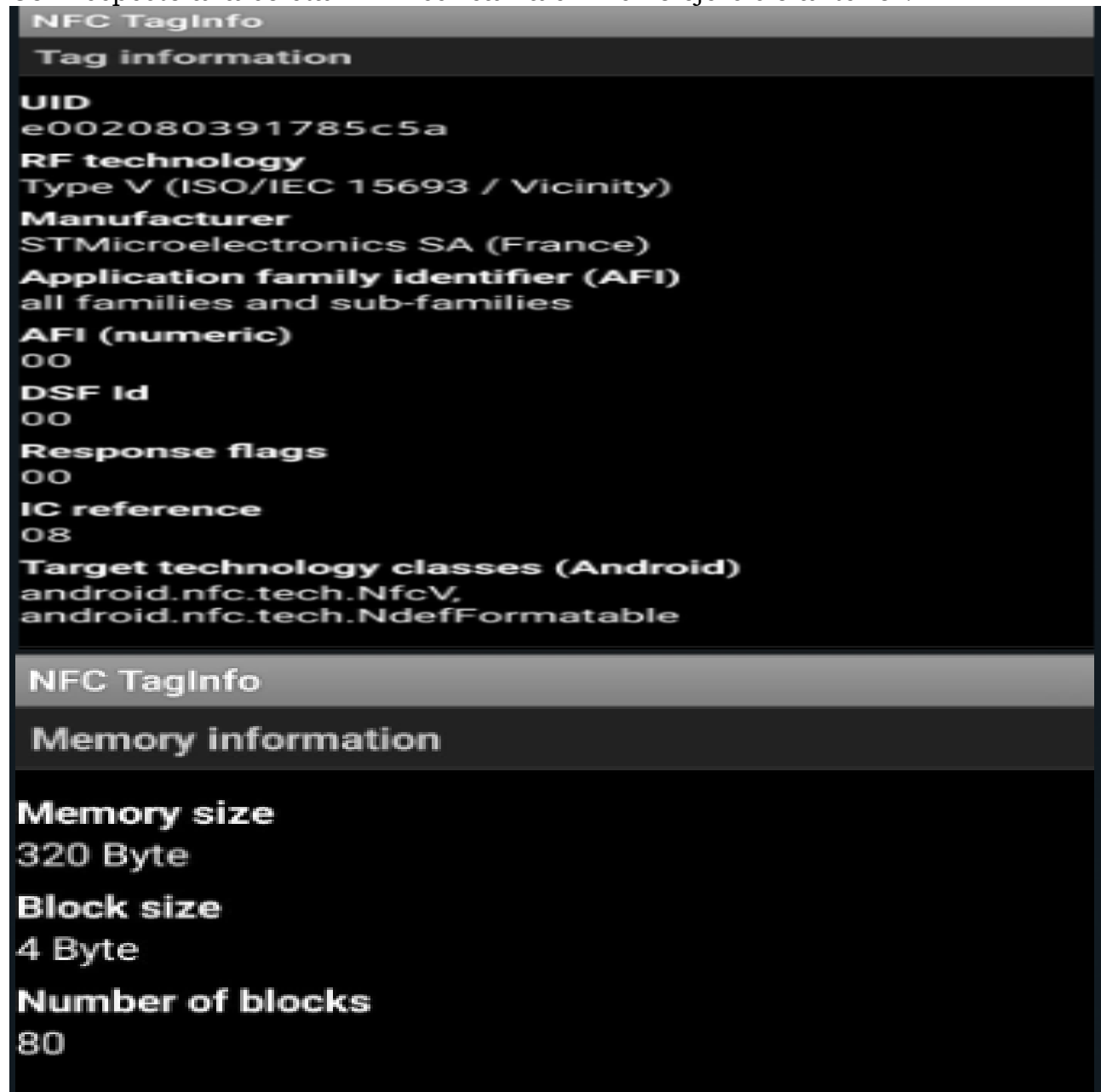


Fig 6. Información del CHIP RFID Boleta TREP.

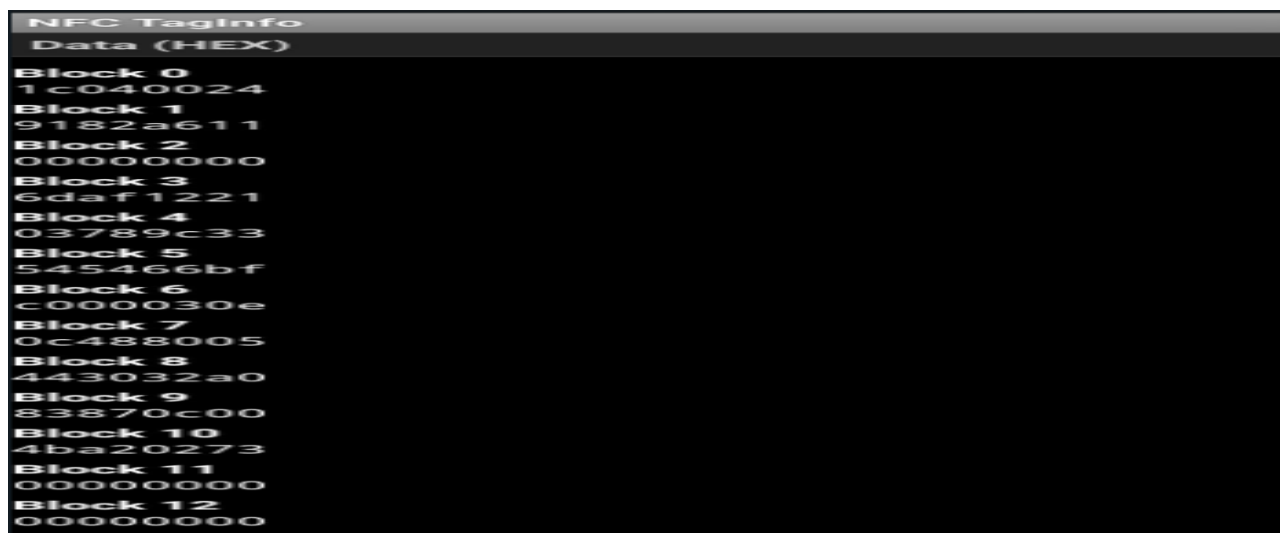


Fig 7. Información escrita en el Chip RFID de boleta TREP.

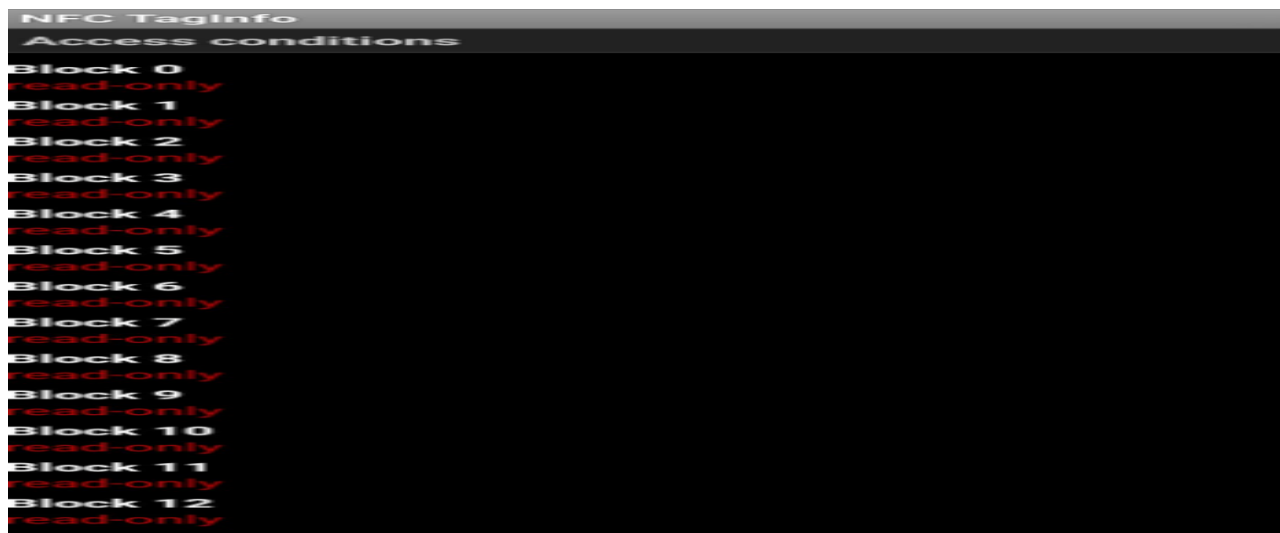


Fig 8. Estado de los bloques del Chip RFID de la boleta.

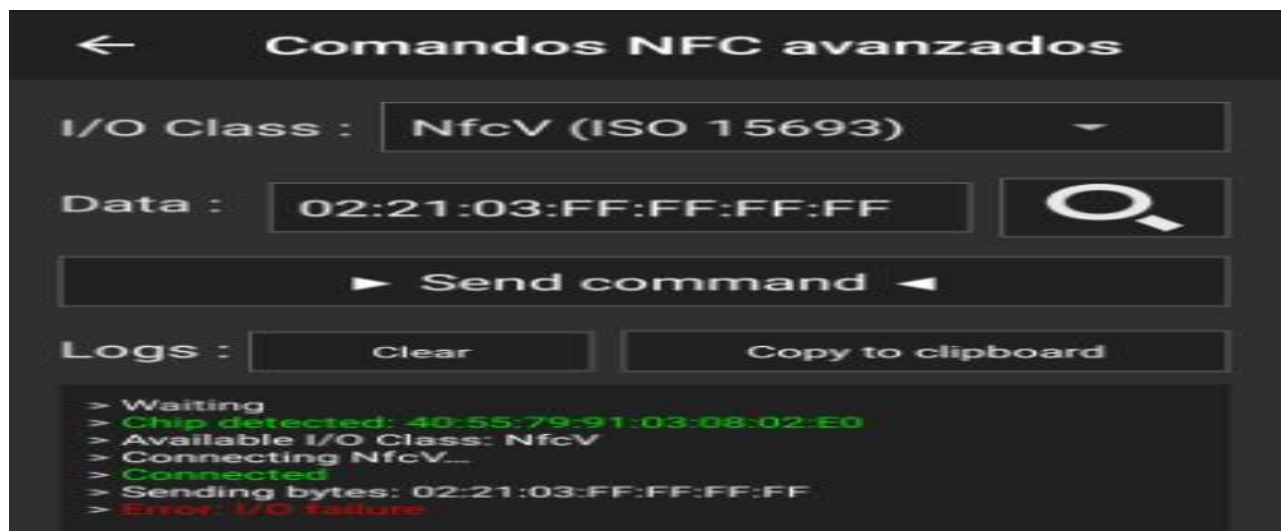


Fig 9. Prueba de escritura del bloque 3 en el CHIP RFID de la boleta TREP.

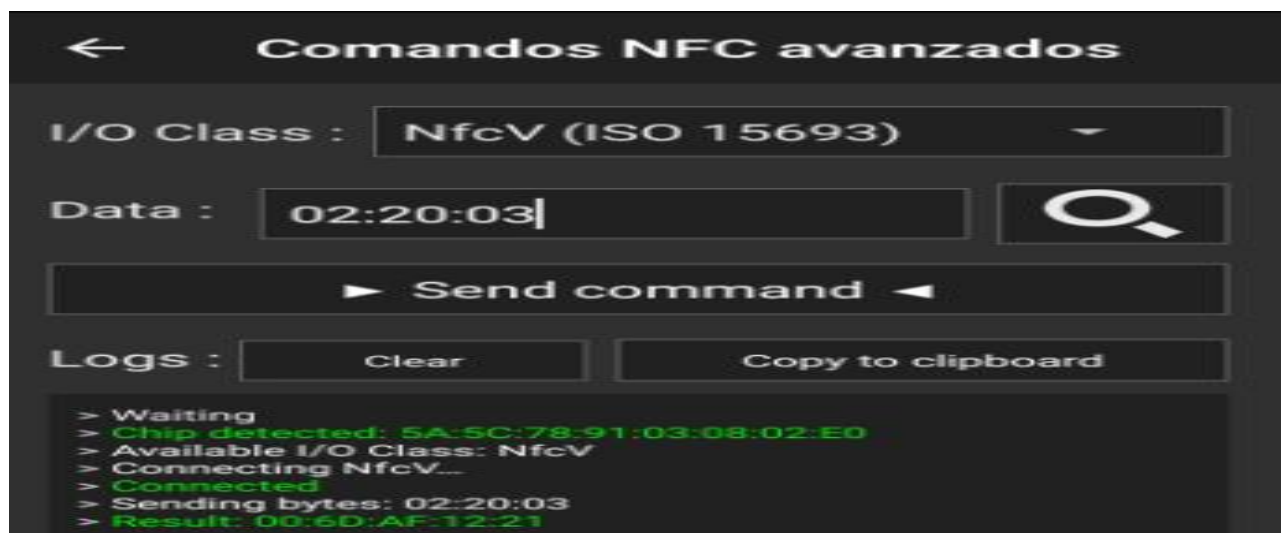


Fig 10. Prueba de lectura del bloque 3 en el CHIP RFID de la boleta TREP, resultado exitoso, el mismo del bloque 3 en la Fig 7.

Se puede comprobar desde el NFC Tool que para los dos tipos de chips que se usan estos una vez escritos en la terminal de votación quedan en estado bloqueado.

Resultados de la prueba:

Mediante esta prueba se confirmó que las boletas de votación y TREP no se pueden modificar una vez escritas en la terminal de votación, Esto garantiza que los votos o los boletines no serán alterados de ninguna forma.

Se tuvo en cuenta los comandos más comunes Del estándar ISO 15693 para hacer las diferentes pruebas.

EVALUACIÓN DEL SOFTWARE

Durante la evaluación del software de las máquinas de votación (Modelo P4 y P6), se realizó la revisión y análisis del código fuente del software, revisión de la configuración del sistema operativo, revisión de la parametrización, revisión de la documentación técnica y manuales de usuario y se aplicaron instrumentos de investigación y herramientas de análisis de vulnerabilidades y de captura de información (sniffer de red) y la utilización de dispositivos de hackeo ético, con el objetivo de identificar riesgos que puedan afectar el proceso de votación. Los elementos que fueron incluidos en esta evaluación son los siguientes:

- Se evaluó el software de ambos modelos de las máquinas de votación, para conocer, cuál es el mecanismo de encriptación utilizado en los chips de las boletas de votación, las credenciales y los certificados de resultados TREP, con el objetivo de garantizar la integridad y confidencialidad de la información.
- Se evaluó la configuración del sistema operativo, para determinar si contaba con parámetros que garanticen la seguridad de la imagen ISO del disco DVD.
- Se evaluó el software de ambos modelos de las máquinas para verificar la seguridad del acceso al sistema de votación.

AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

- Se evaluaron los procesos de identificación, autenticación y autorización de los usuarios en el software de ambos modelos de las máquinas de votación.
- Se revisó el código fuente del software y la documentación técnica, para conocer su diseño, estructura, funcionalidad y estándares de seguridad utilizados durante el desarrollo de la aplicación de voto electrónico, y a su vez, para verificar si se encuentra debidamente documentado.
- Se revisaron los manuales de usuario para verificar su conformidad con relación al software desarrollado y al versionado de ambos modelos de las máquinas de votación.
- Se revisaron los casos de uso, con el objetivo de identificar si estaban acorde con los requerimientos solicitados por el TSJE.
- Se analizó el procedimiento de gestión de cambios utilizado por la empresa Grupo MSA, para determinar el grado de cumplimiento con relación a los ajustes y controles sobre las diferentes versiones del software utilizado por ambos modelos de las máquinas de votación.
- Se evaluaron los procesos de calidad y pruebas, con el objetivo de identificar errores en la aplicación y a su vez, conocer el grado de desempeño de las principales características del software durante su ciclo de vida.

PRUEBAS PARA LA REVISIÓN DEL SOFTWARE

PRUEBA 1.

PRUEBA DE ARRANQUE Y DEL MÓDULO DE CALIBRACIÓN DE LA MÁQUINA DE VOTACIÓN ELECTRÓNICA

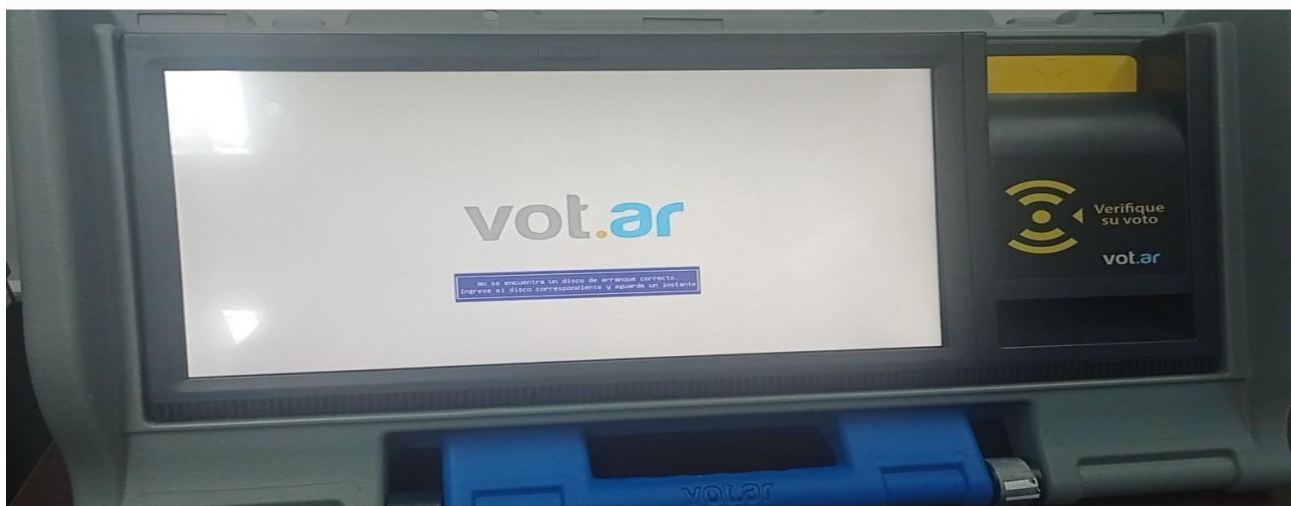
Objetivo de la Prueba

Constatar el arranque y la funcionalidad de las opciones de calibración con las que cuenta la máquina de votación Electrónica

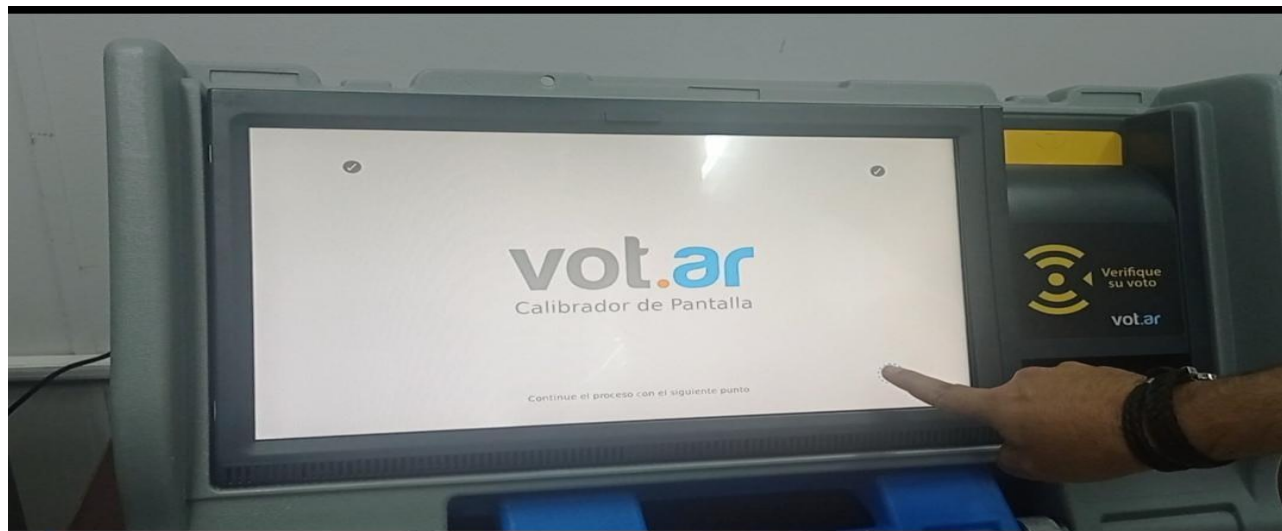
Descripción de la Prueba:

La prueba inició con la comprobación del encendido del equipo, carga del sistema operativo y el software de votación que están contenidos en el DVD de arranque.

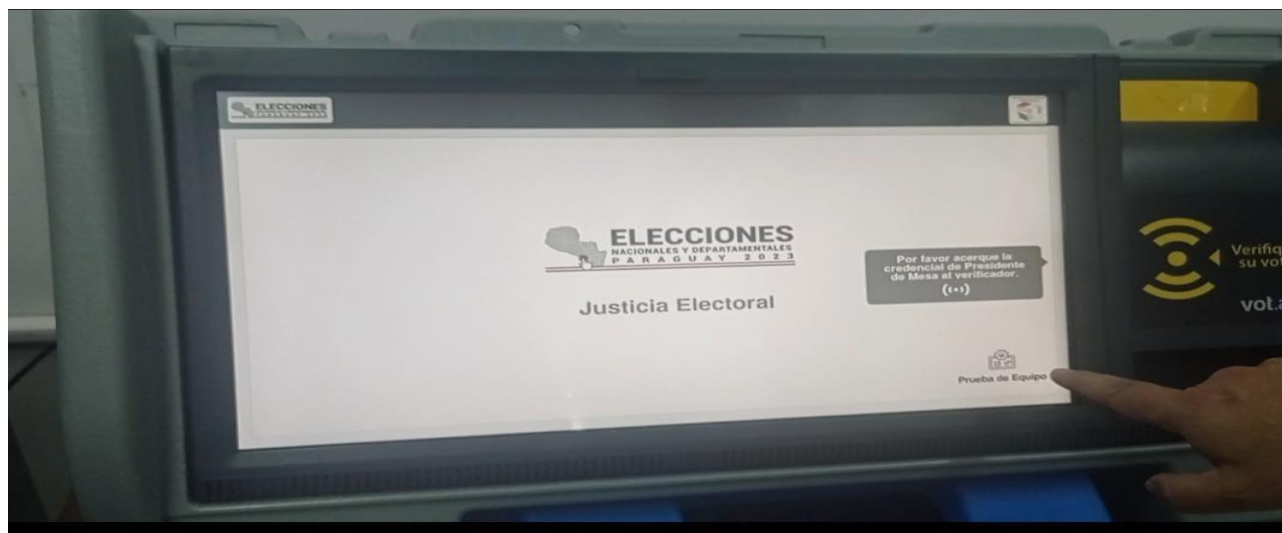
Durante este primer proceso se comprobó que el equipo queda a la espera del inicio del sistema a través del DVD de arranque sin el cual la máquina no inicia ninguna aplicación.



Una vez cargado el Sistema Operativo y el Software de Votación, se probó la función de calibración de la pantalla.



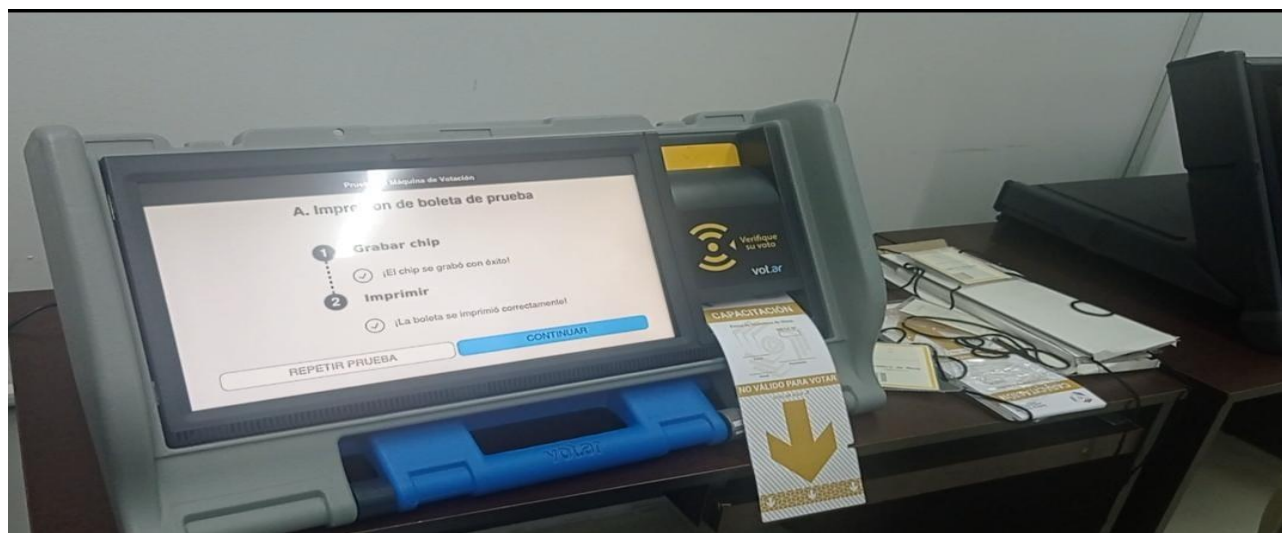
Luego de esto se probaron las opciones de calibración y prueba de los componentes del equipo a través del módulo de **“Pruebas de Equipo”**.



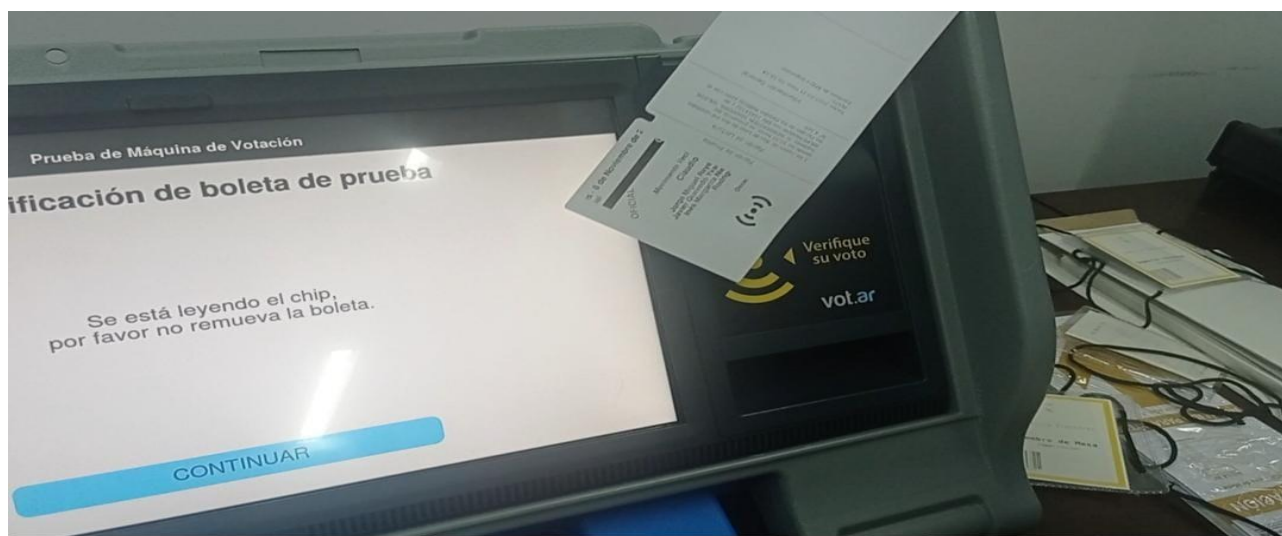
Dentro del módulo de Pruebas del Equipo se realizaron las siguientes comprobaciones:

Escritura del Chip RFID

Impresión de la papeleta de votación



Lectura del Chip RFID





AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



Las pruebas fueron satisfactorias y sin ningún contratiempo.

Resultados de la prueba:

Se comprobó el funcionamiento correcto de la impresión de la boleta electoral, así como la lectura y escritura del Chip RFID.

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.

PRUEBA 2.

PRUEBA DEL MÓDULO DE CIERRE DE MESA Y ESCRUTINIO

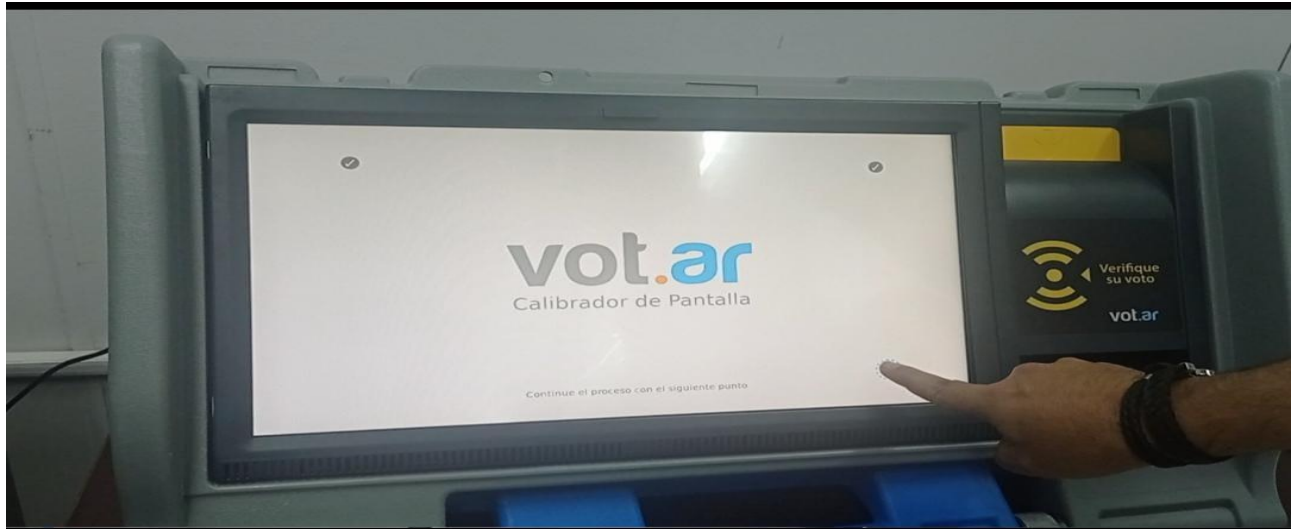
Objetivo de la Prueba

Constatar el correcto funcionamiento de las opciones del módulo de cierre de mesa y escrutinio.

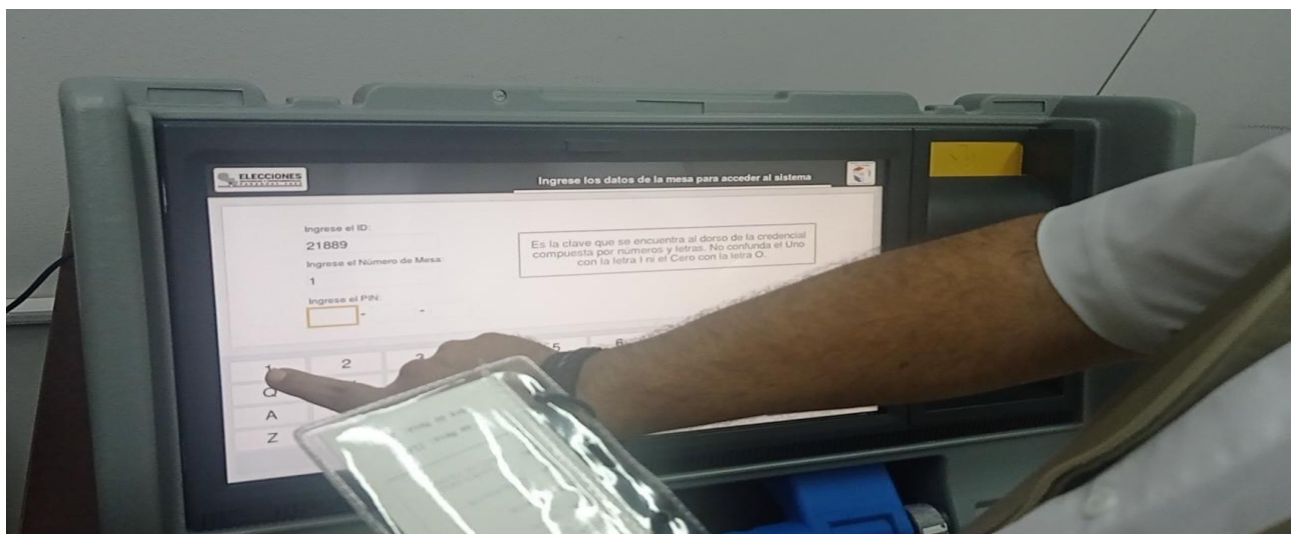
Descripción de la Prueba:

La prueba inicia con el encendido del equipo, la carga del sistema operativo y el software de votación contenidos en un disco DVD.

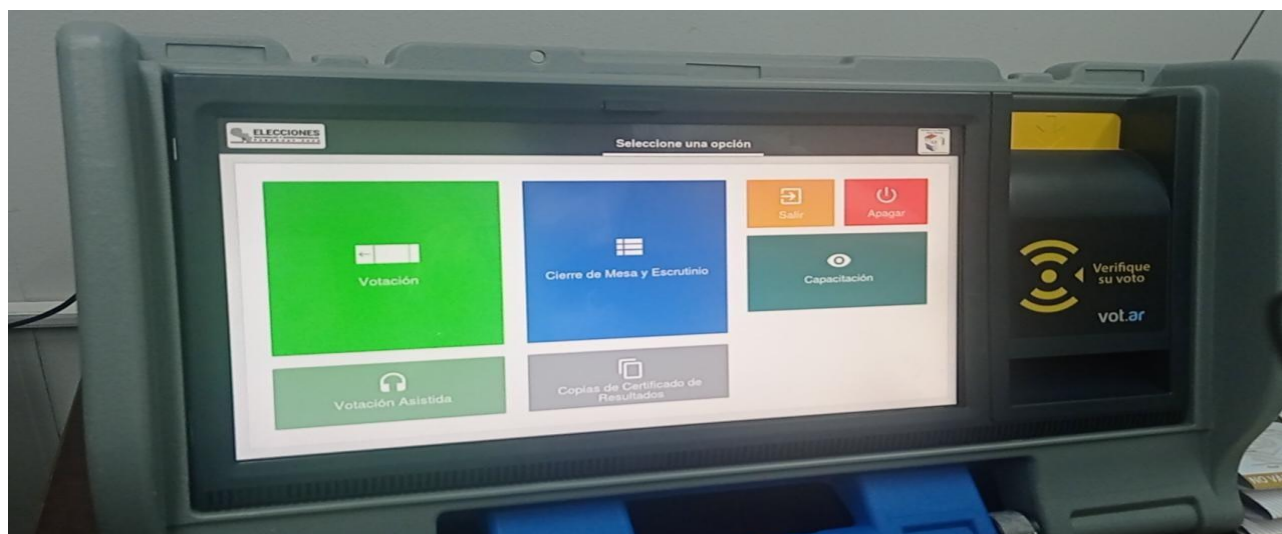
Una vez cargado el Sistema Operativo y el Software de Votación, se probó nuevamente la función de calibración de la pantalla.



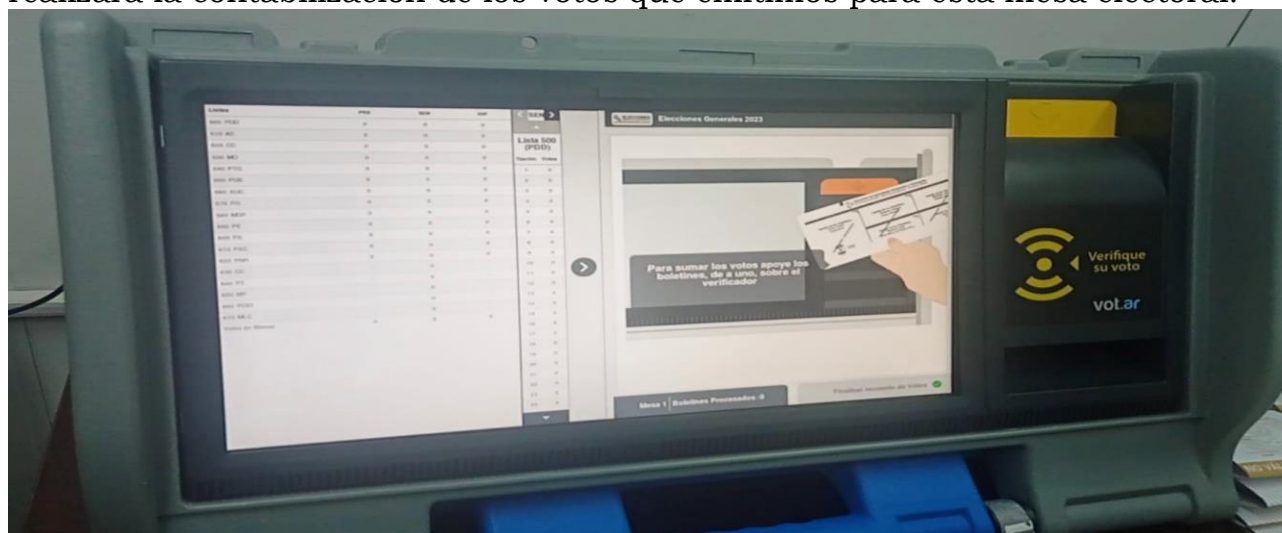
Luego se comprobó que es necesario habilitar nuevamente el sistema con la credencial de miembro de mesa proporcionada acercando el Chip para su lectura e ingresando los datos impresos en la credencial para vincular la máquina con la mesa electoral respectiva.



Luego de confirmar la información de la mesa, se habilita la pantalla con el acceso a los diferentes módulos del sistema y procedemos a seleccionar el módulo de “Cierre de Mesa y Escrutinio”.



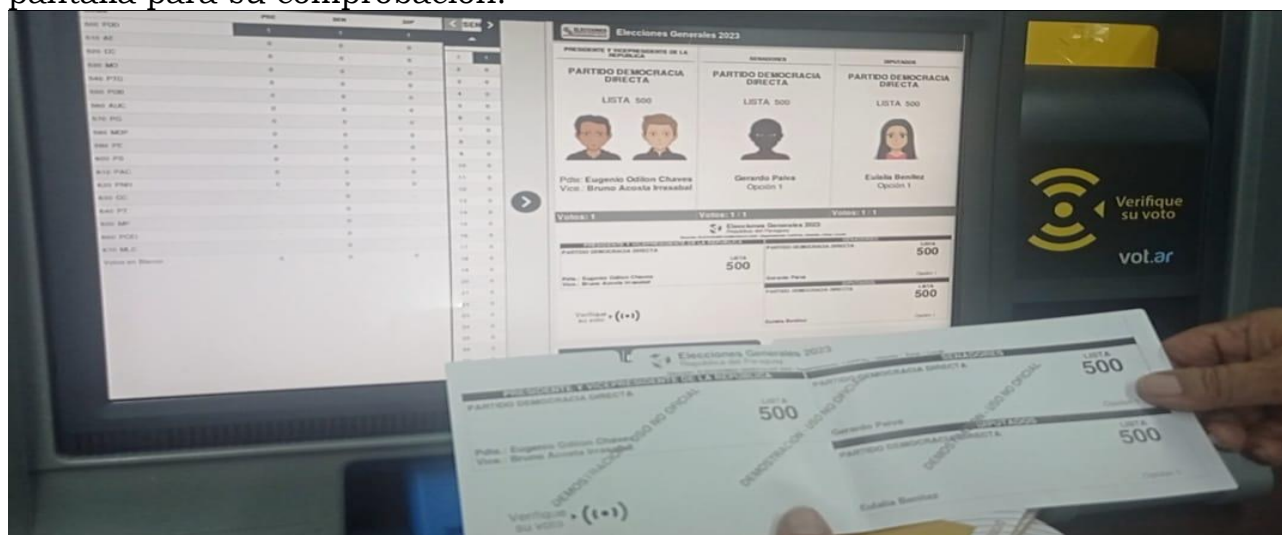
Una vez se seleccionó esta opción, el sistema presenta la interfaz en la cual se realizará la contabilización de los votos que emitimos para esta mesa electoral.



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

En esta interfaz se realizó la prueba de conteo acercando cada voto emitido al lector de RFID y constatando que este voto va sumándose al candidato seleccionado en cada una de las dignidades o categorías.

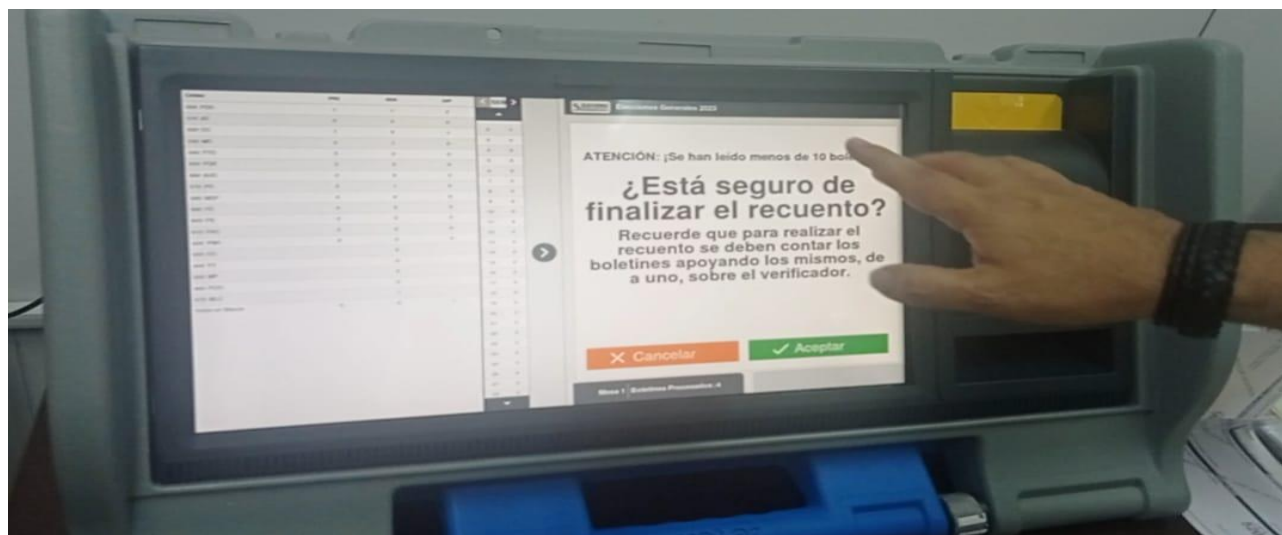
Se destaca el hecho que en cada voto contabilizado es presentado también en pantalla para su comprobación.



Se comprobó también que al pasar la misma boleta más de una vez, el sistema lo rechaza y presenta una alerta en pantalla. Además, se comprobó que este voto no sea contabilizado nuevamente.

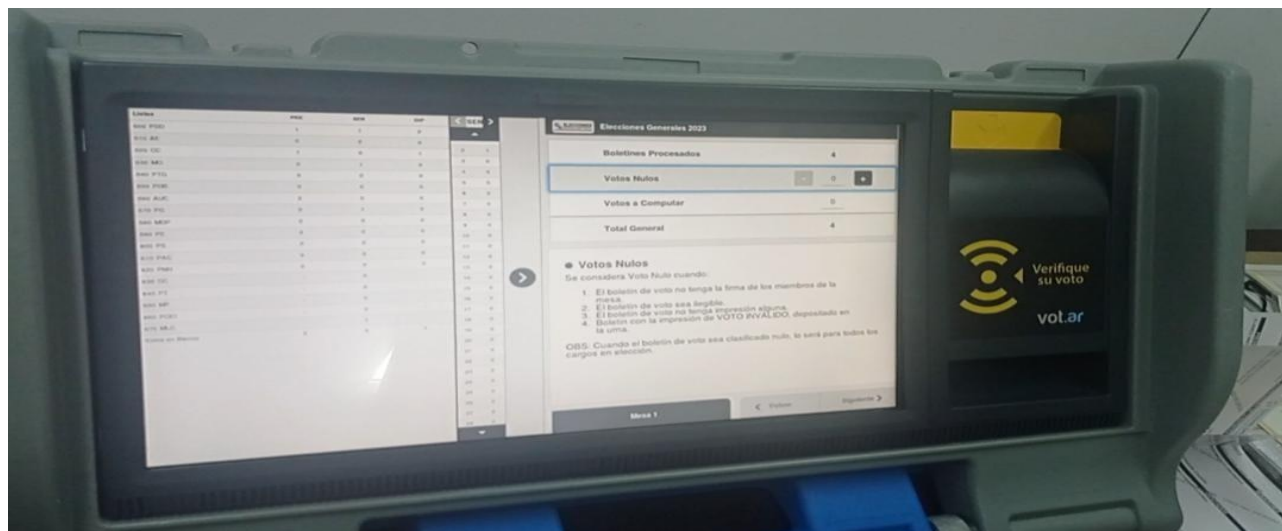


Finalmente, para terminar el conteo de votos, seleccionamos la opción “Terminar Recuento”, en este caso al tener un número menor de 10 votos, el sistema presenta una alerta antes de proceder al cierre del escrutinio. Esta es una medida de precaución para que la autoridad de mesa no cierre el proceso de escrutinio sin primero haber contabilizado todas las boletas pendientes de conteo.

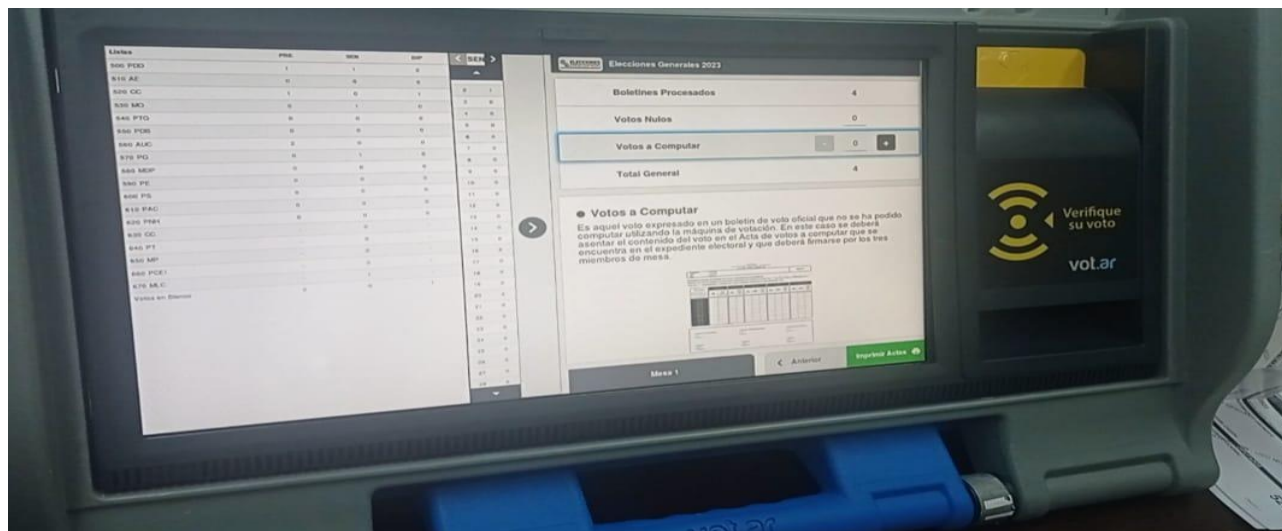


Luego el sistema presenta una pantalla en la que se nos permite registrar de manera manual, los votos nulos y votos a computar, para información de los miembros de mesa en cada opción se nos indica las causas por las cuales un voto es nulo o cuando se suma un voto a computar.

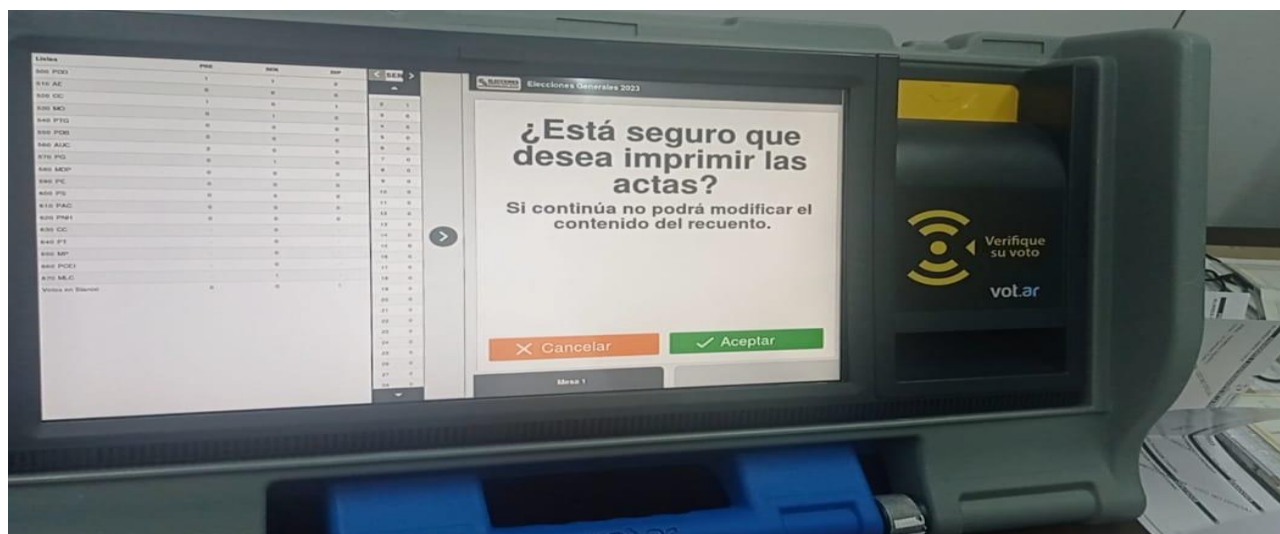
AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



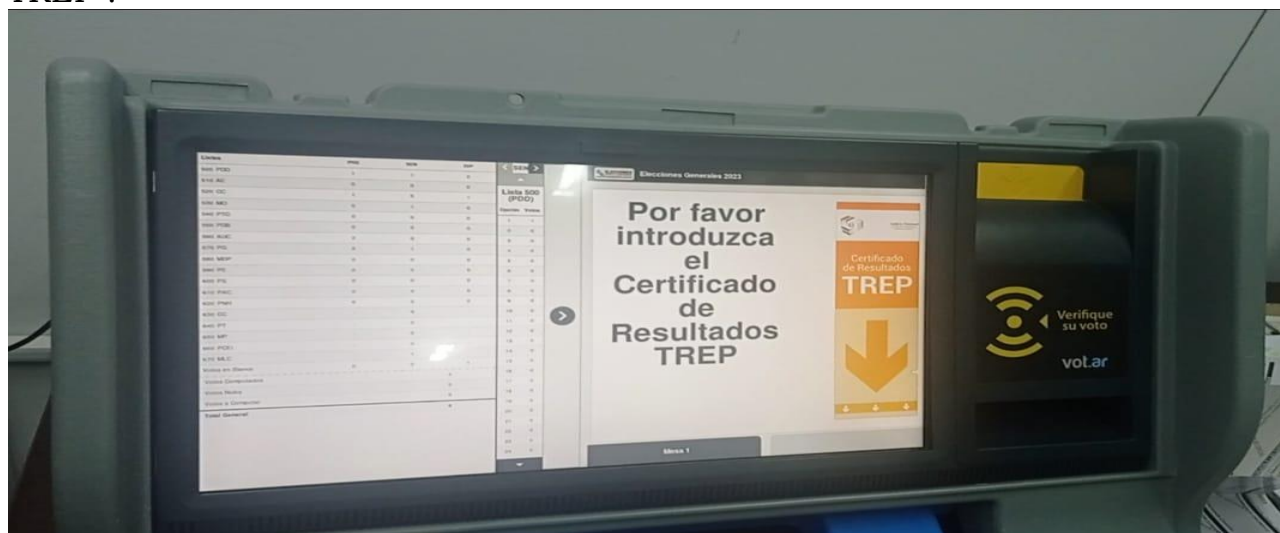
Una vez realizado este registro, se activa la opción para la impresión de actas y certificados.



Al seleccionar la opción de impresión, el sistema presenta una alerta indicando que se terminará el recuento de votos y que ya no se podrá realizar ninguna modificación al conteo realizado.



El primer certificado que el sistema imprime es el “Certificado de Resultados TREP”.



Se comprobó la impresión de un certificado por cada una de las dignidades o categorías a elegir.

Se verificó que este tipo de certificado cuenta con un Chip RFID y además se imprime un código QR que contiene los resultados de la mesa.

Se prioriza este certificado debido a que este es enviado para su transmisión en el sistema TREP, que es un sistema propio del Tribunal Supremo de Justicia Electoral.

Seguidamente el sistema procede con la impresión de las actas de escrutinio, las cuales se entregarán a los veedores de las agrupaciones políticas presentes en el escrutinio. Estas actas no poseen un Chip RFID, pero sí se imprime un código QR para una lectura rápida de los resultados del acta.

Así mismo se comprobó que se imprime un acta por cada dignidad o categoría a elegir.

Resultados de la prueba:

Se comprobó el funcionamiento correcto de cada una de las funcionalidades del módulo de “Cierre de Mesa y Escrutinio”.

Debido al alcance de la auditoría, esta prueba concluyó con la impresión de los certificados y actas de escrutinio sin validar la transmisión de los resultados que se realizan a través de los mismos con el sistema TREP.

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.

PRUEBA 3.

PRUEBA DE HABILITACIÓN DEL SISTEMA Y CREDENCIALES

Objetivo de la Prueba

Constatar la habilitación correcta del sistema mediante credenciales de acceso.

Descripción de la Prueba:

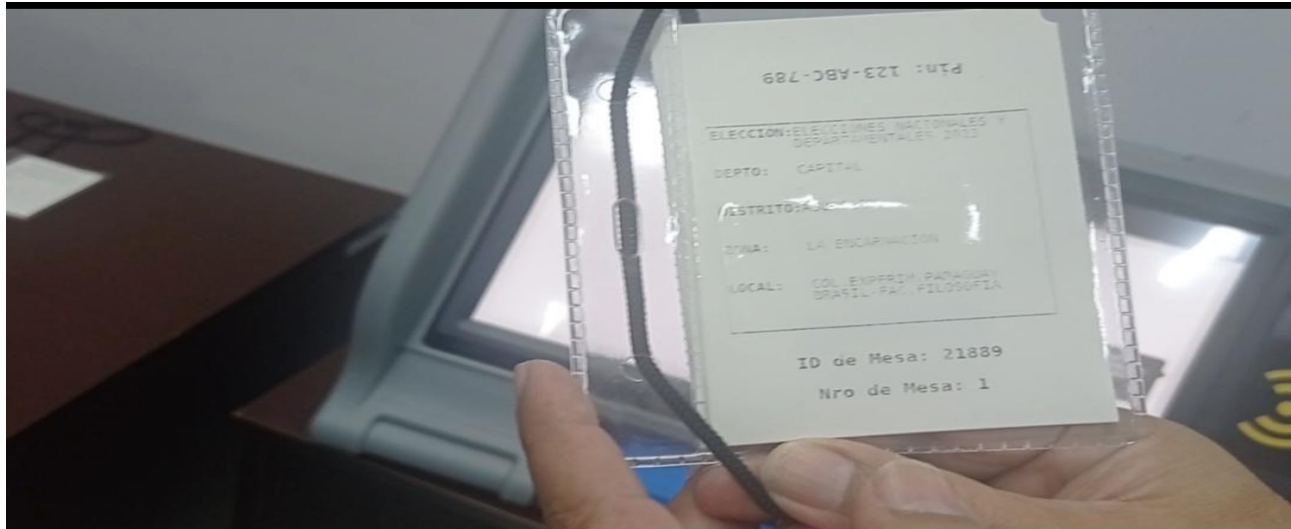
La prueba inicia con la máquina de votación electrónica ya encendida y el sistema operativo y el software de votación contenidos en el DVD ya ejecutándose en el equipo.

En este punto la máquina se encuentra a la espera de recibir la información de las credenciales de acceso.

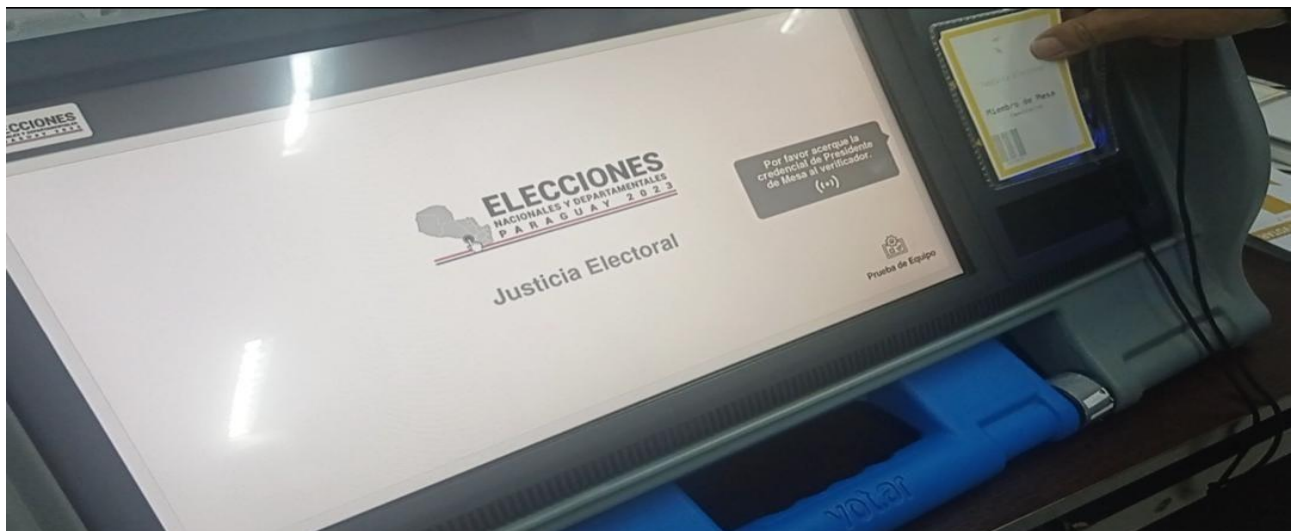


AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

Para esta prueba se nos proporcionó una credencial electrónica de miembro de mesa.

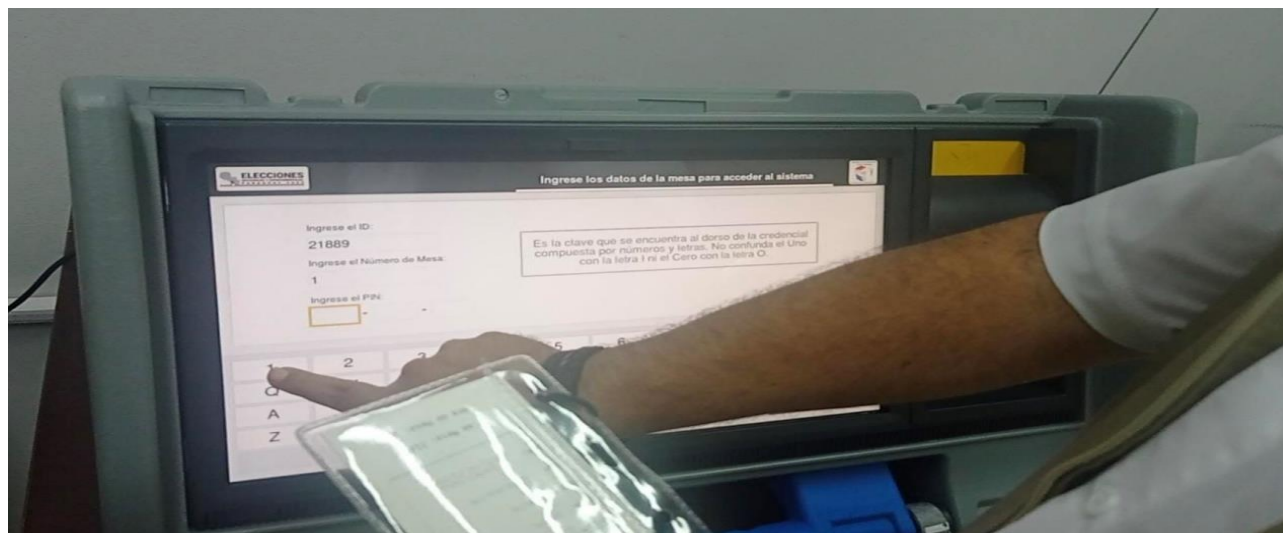


Para la iniciar la habilitación del equipo, se acercó la credencial proporcionada al lector de RFID de la máquina, con lo cual se habilita la pantalla para el ingreso de la identificación de la mesa electoral que se va a habilitar.

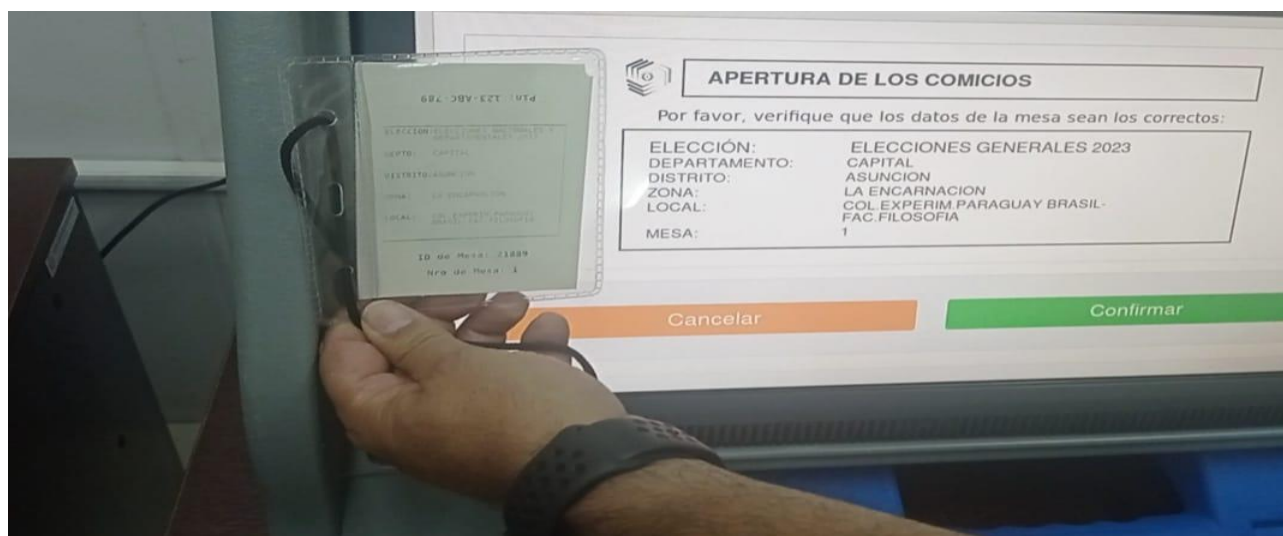


AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

Se debe registrar el id de la credencial, el número de mesa electoral y un PIN. Estos datos están impresos en la credencial.

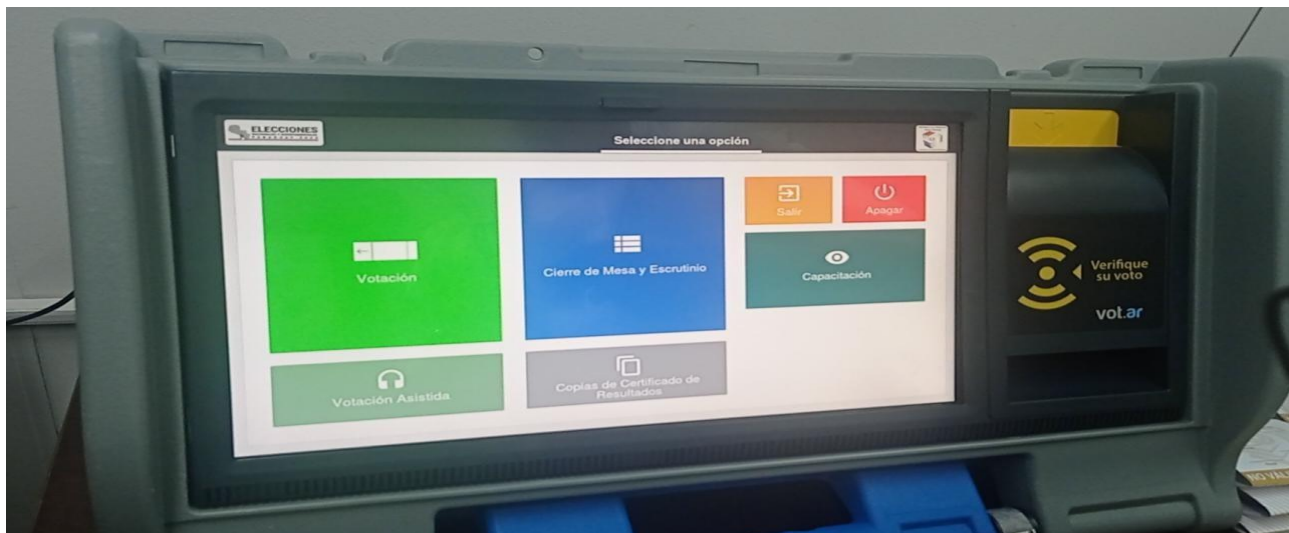


Una vez proporcionada esta información, el sistema realiza la carga de la información de la mesa electoral correspondiente y la presenta en pantalla para comprobar que los datos fueron los correctos.



Luego de confirmar la información de la mesa, se habilita la pantalla con el acceso a los siguientes módulos: Votación, Votación asistida, Cierre de mesa y escrutinio, Copia de certificado de resultados y Capacitación

Además, se presentan las opciones de “Salir” y “Apagar”.



Finalmente, el sistema queda habilitado, a la espera de la selección que realice el usuario

Resultados de la prueba:

Mediante esta prueba se comprobó que únicamente con la credencial y la información impresa en la misma, se puede habilitar el sistema y acceder a sus diferentes módulos.

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.

PRUEBA 4.

PRUEBA DEL MÓDULO DE VOTACIÓN

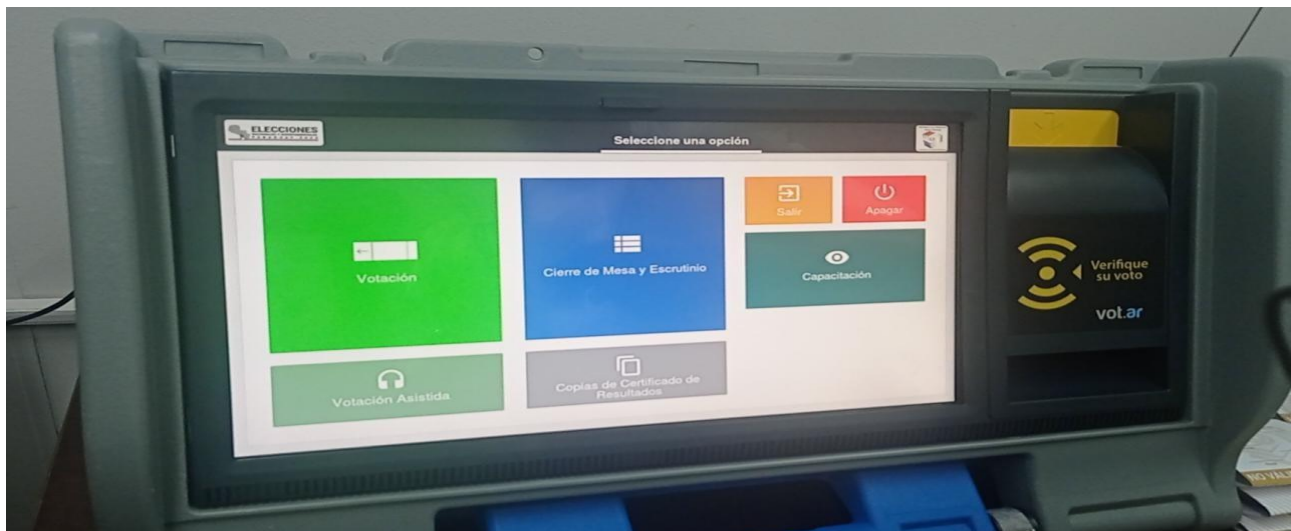
Objetivo de la Prueba

Constatar el correcto funcionamiento del módulo de votación.

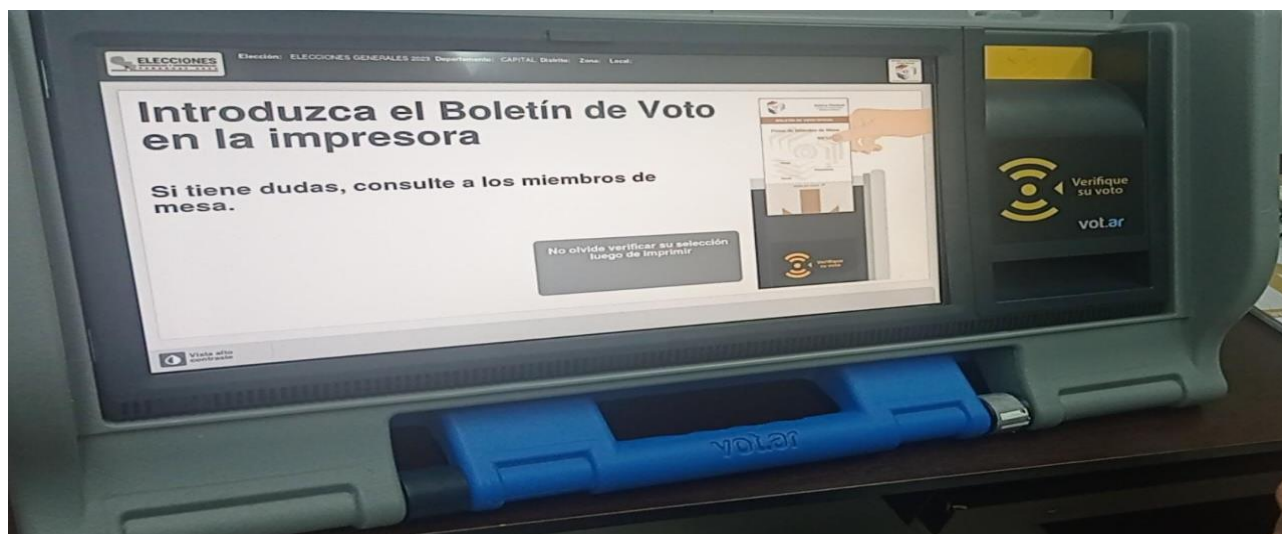
Descripción de la Prueba:

La prueba inicia con la máquina de votación encendida, el sistema operativo y el software de votación contenidos en el disco DVD ejecutándose en el equipo y el sistema habilitado para su uso, vinculando la máquina con la mesa electoral a la que pertenece mediante la credencial respectiva.

En este punto el sistema presenta una pantalla los diferentes módulos a los que se puede tener acceso.



Seleccionando el módulo de “Votación”, el sistema queda listo para recibir la votación de los electores.



Para esta prueba se nos proporcionó un paquete de boletas de votación utilizadas en capacitación, las que están sin imprimir y con el Chip RFID en blanco.

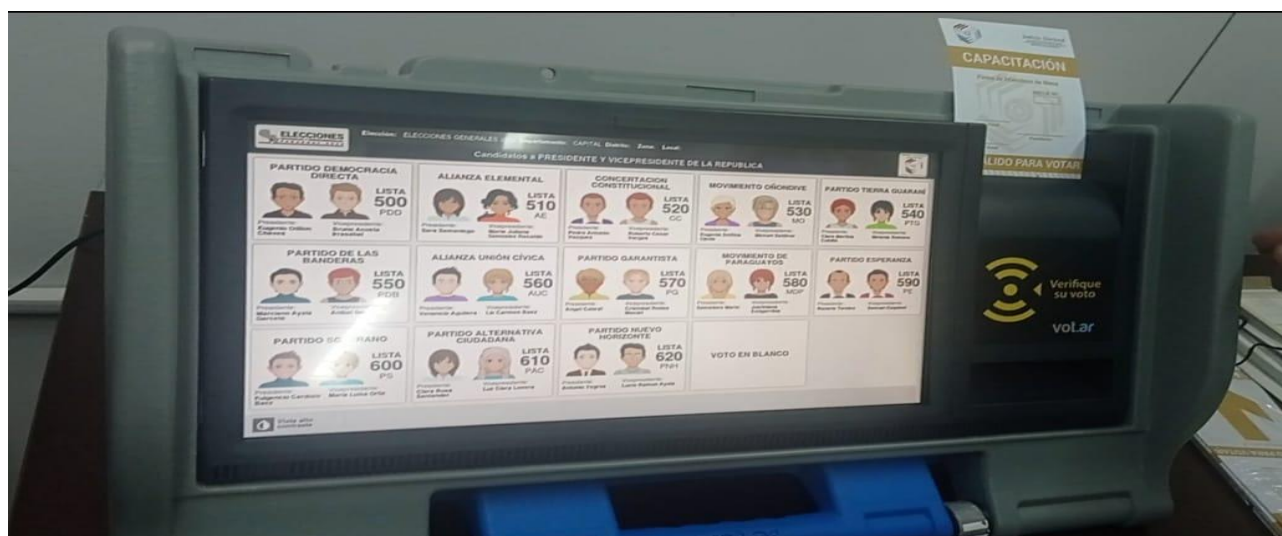
Se realizó una primera prueba insertando una boleta con un voto impreso en ella y grabado en el Chip RFID y se constató que el sistema expulsa la boleta y presenta el voto impreso en la pantalla.

AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

A continuación, se colocó una boleta de votación en blanco en la bandeja de la impresora.

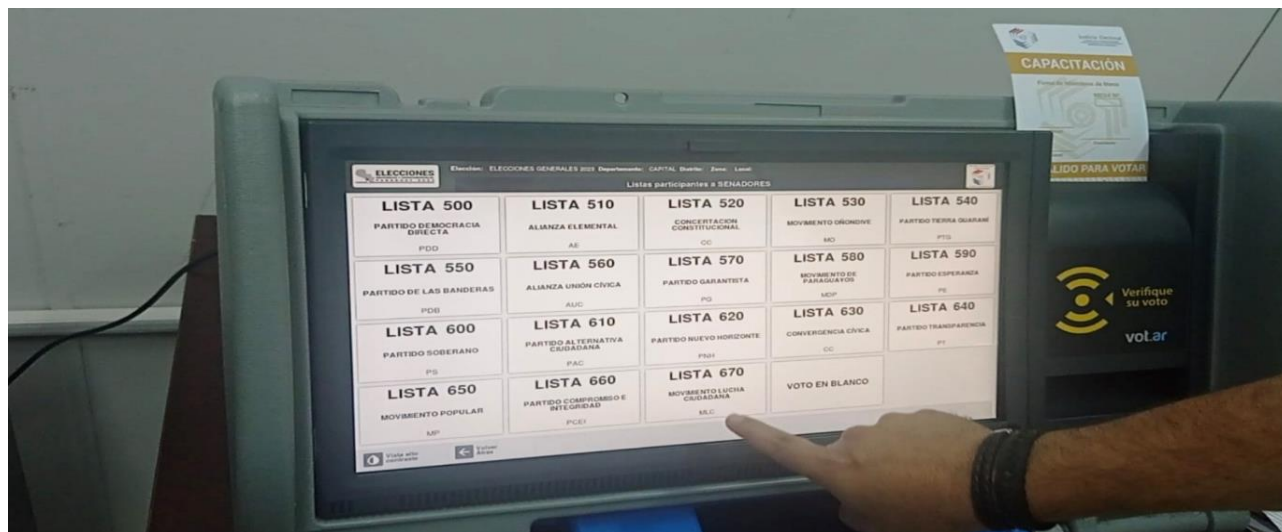


Inmediatamente el sistema presenta en pantalla a los candidatos debidamente identificados para la elección de presidente y vicepresidente de la República.

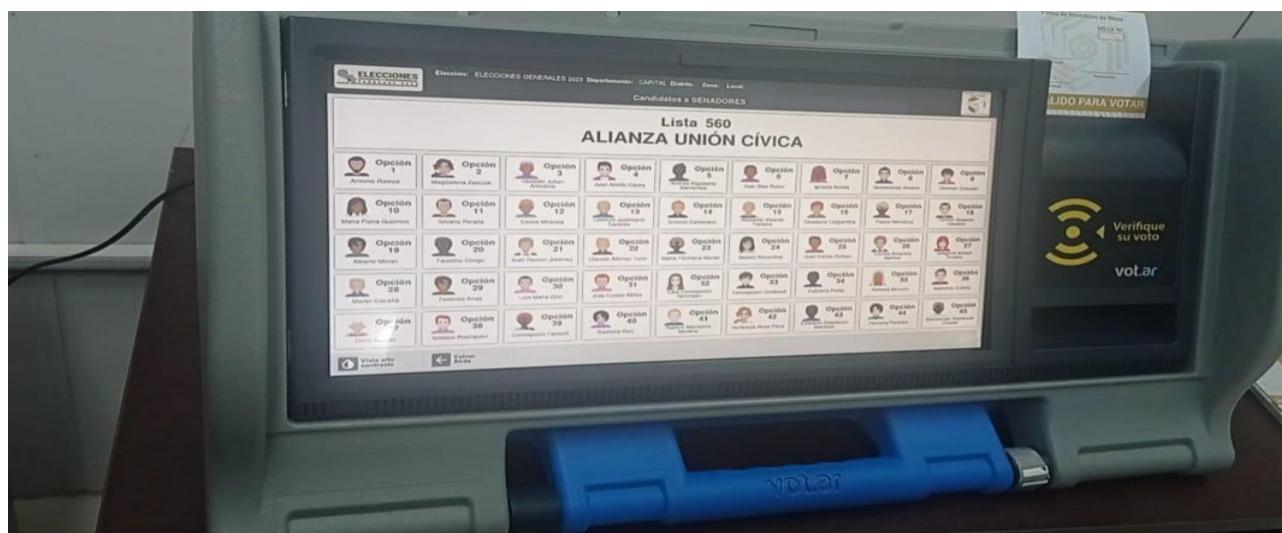


AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

Se realizó la selección de unos de los candidatos al azar; luego de esto, el sistema presenta los partidos o agrupaciones políticas participantes en la elección de senador.



Una vez seleccionada la agrupación política, el sistema presenta los candidatos de dicha agrupación para su selección.

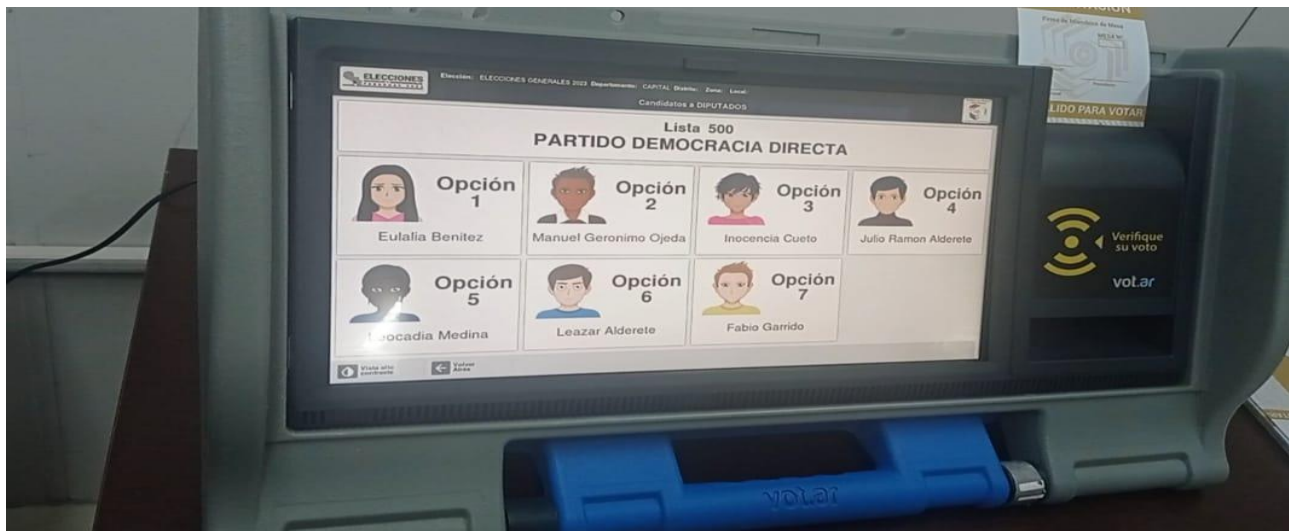


AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

Una vez realizada la selección del candidato a senador, el sistema presenta los partidos o agrupaciones políticas participantes en la elección de diputado.

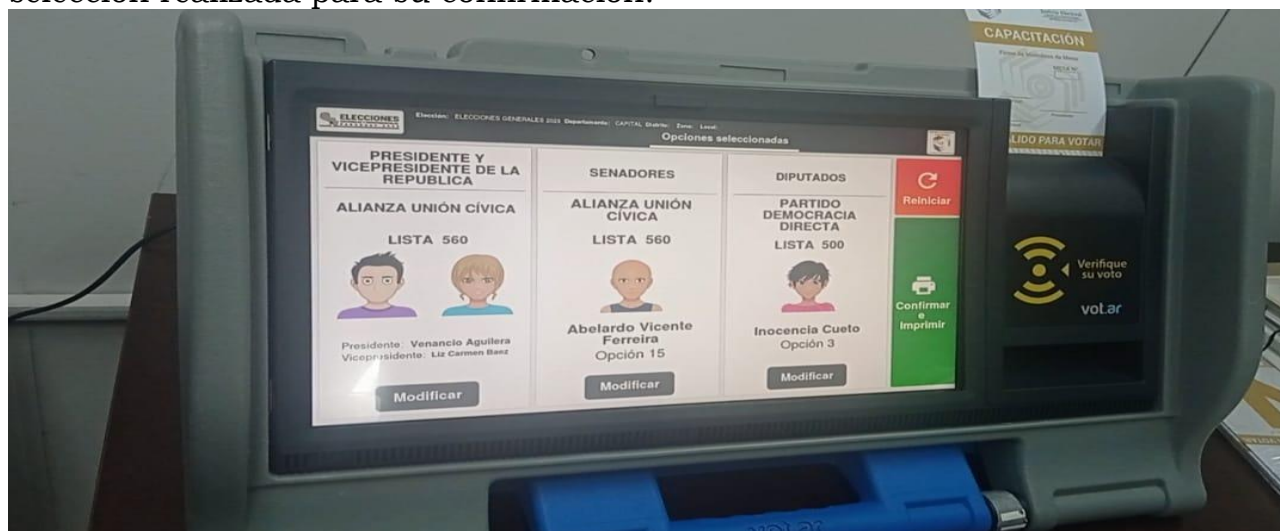


Seleccionada la agrupación política, el sistema presenta los candidatos de dicha agrupación para la selección del diputado.



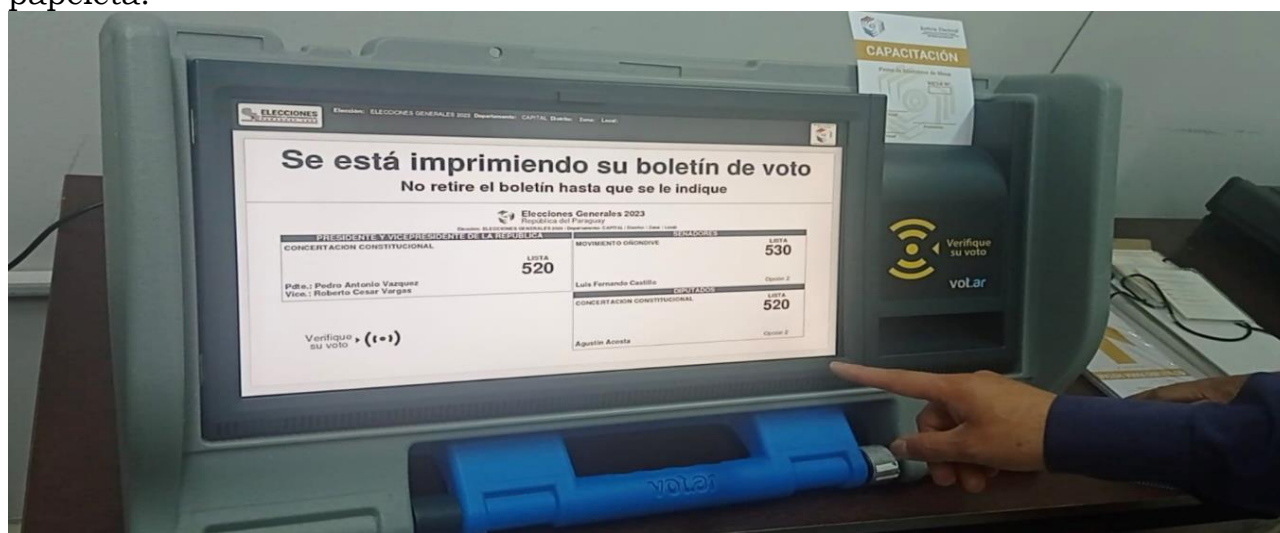
AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

Finalizada la selección de candidatos el sistema presenta una pantalla con la selección realizada para su confirmación.



Se comprobó que también es posible realizar modificaciones a la selección de candidatos las veces que el usuario lo crea conveniente hasta confirmar su elección.

Una vez confirmada la selección realizada, el sistema inició con la grabación de la información del voto realizado en el Chip RFID y la inmediata impresión de la papeleta.



Finalmente se pudo comprobar la lectura del Chip RFID al acercar la boleta al lector RFID lo que produce que se presente en pantalla la selección de candidatos que se grabó en el Chip y se pueda comprobar que es la misma información que esta impresa en la boleta.



Resultados de la prueba:

Mediante esta prueba se comprobó el funcionamiento del módulo de votación y se determinó que se puede realizar un voto únicamente con una boleta que contenga un Chip RFID en blanco. Una vez realizado el voto se comprobó que la impresión concuerda con lo grabado en el Chip.

También se pudo comprobar que el elector puede modificar su voto las veces que crea conveniente hasta quedar conforme con la selección.

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.

PRUEBA 5.

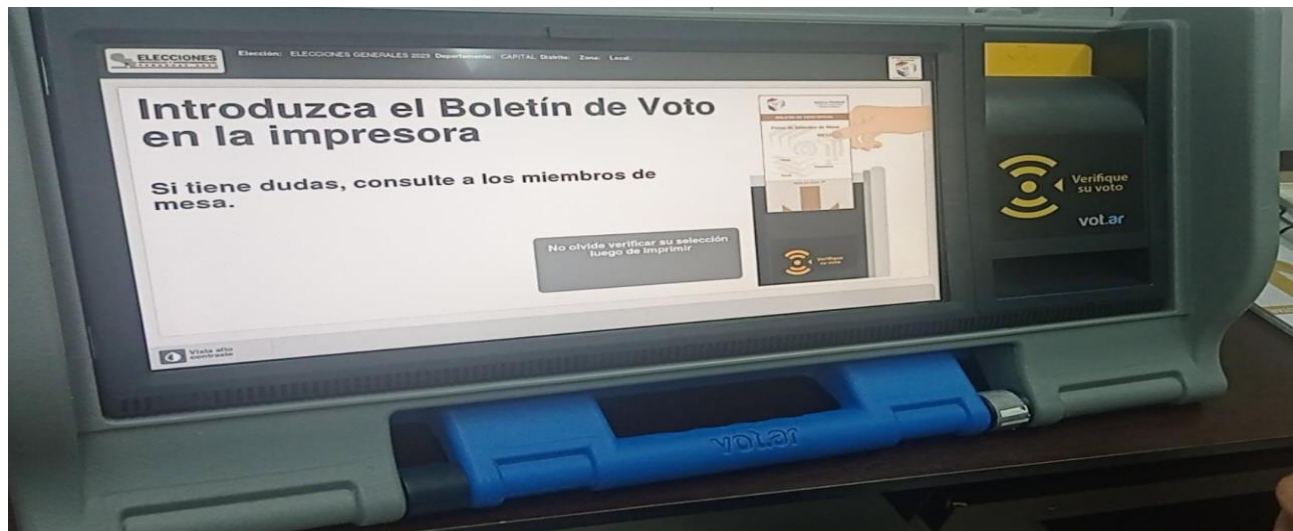
PRUEBA DEL MÓDULO DE VOTACIÓN ASISTIDA

Objetivo de la Prueba

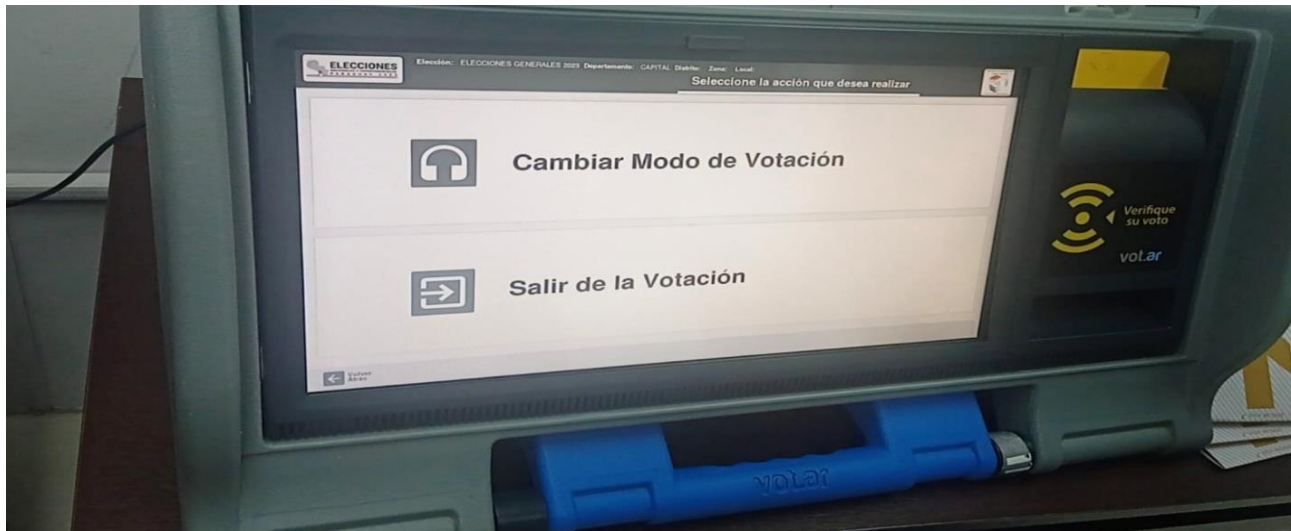
Constatar el correcto funcionamiento del módulo de votación asistida, el cual ayuda a las personas no videntes a realizar el proceso de votación.

Descripción de la Prueba:

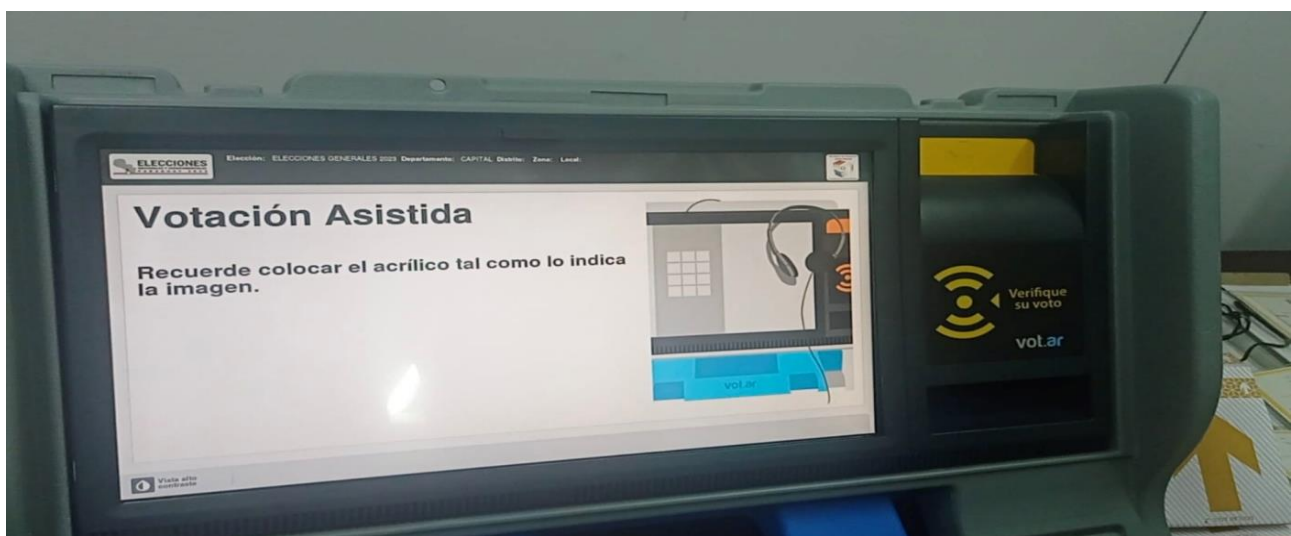
La prueba inicia con la máquina de votación encendida, el sistema operativo y el software de votación contenidos en el DVD ejecutándose en el equipo y el sistema habilitado para su uso, vinculando la máquina con la mesa electoral a la que pertenece mediante la credencial respectiva y se ha seleccionado el módulo de votación y el sistema se encuentra listo a recibir los votos de los electores. Además, se contó con una plantilla acrílica que ayuda a la persona no vidente en la selección de las opciones de votación.



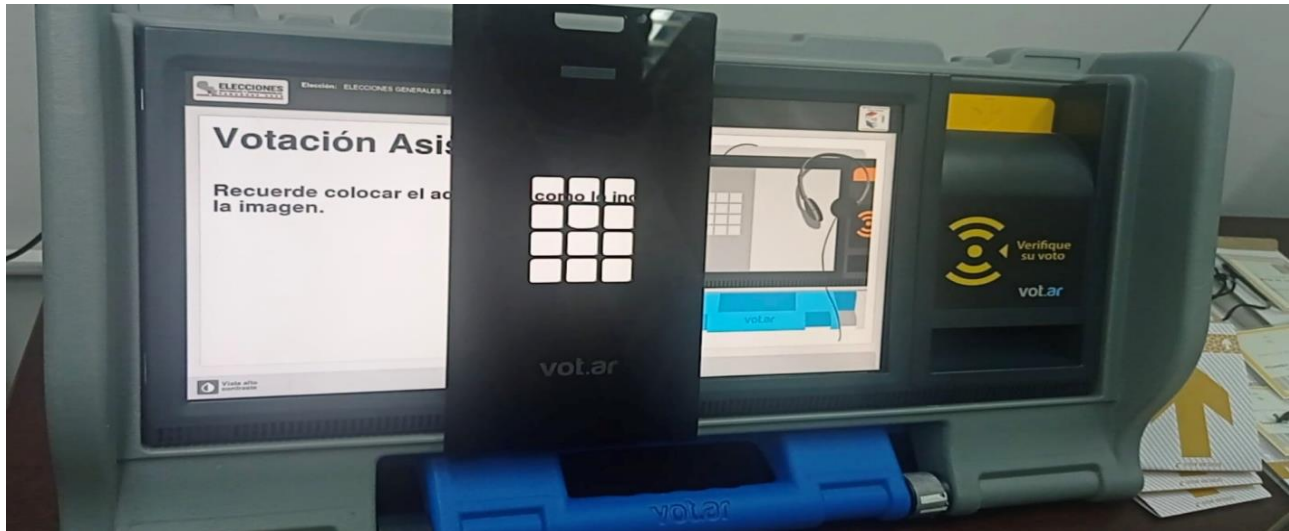
Para activar el módulo de “Votación Asistida”, es necesario acercar nuevamente la credencial de “Miembro de Mesa” al lector de RFID, lo cual activa la pantalla para la selección del modo de votación asistida.



Al seleccionar la opción “Cambiar Módulo de Votación”, se activa el módulo de votación asistida.



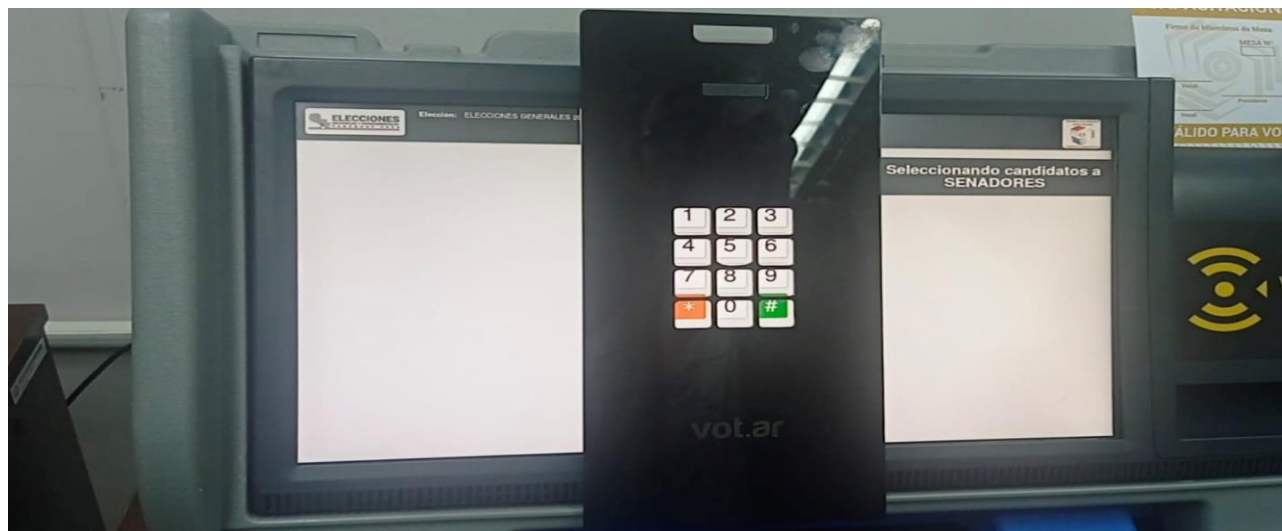
En este punto es necesario colocar elacrílico en la posición indicada en el gráfico de la pantalla y luego introducir la boleta de votación en la ranura respectiva.



Una vez colocada la boleta en la posición correcta, se presentan en pantalla un panel de números que coinciden con la plantilla acrílica y el sistema inicia la lectura de las opciones de votación la cual se escucha a través de unos audífonos proporcionados por la mesa.

En este caso cada candidatura es vinculada a un código numérico y se procedió a la selección de los candidatos de acuerdo con el código dictado por el sistema.

Para efectos de esta prueba, no se utilizaron los audífonos para que los auditores podamos escuchar cada una de las opciones dictadas por el sistema a través de los altavoces de la máquina.



Finalizada la selección de candidatos el sistema al igual que en la votación normal, también repasa las candidaturas seleccionadas y solicita al elector confirmarlas digitando la tecla numeral (#) como confirmación.

Una vez confirmada la selección de candidatos se procede con la impresión de la boleta de votación con las opciones seleccionadas.



Se verificó que el elector en este modo también puede confirmar la selección guardada en el Chip e impresa en la boleta. Para esto solamente tiene que introducir la boleta nuevamente en la ranura de la impresora y el sistema procederá con la lectura de lo que se guardó en el Chip RFID.

Resultados de la prueba:

Mediante esta prueba se comprobó el funcionamiento del módulo de votación asistida y se determinó que es factible para un elector no vidente poder realizar su proceso de votación a través de esta opción con la seguridad y confidencialidad que exige una votación electoral.

También se pudo comprobar que el elector de igual forma que en la votación normal, puede modificar su voto las veces que crea conveniente hasta quedar conforme con la selección

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.

PRUEBA 6.

PRUEBA DE CONSISTENCIA DE DATOS ALMACENADOS EN EL CHIP DE LA BOLETA DE VOTACIÓN

Objetivo de la Prueba

- Constatar el contenido del chip marca ST en los bloques del 63 a 79.
- Validar que, una vez utilizada una boleta con firma digital del fabricante, los bloques del 63 al 79 se reinician en ceros.

Descripción de la Prueba:

La prueba inicia con analizar el contenido de la hoja de datos técnicos (datasheet) del fabricante del chip ST FRID EEPROM (ST25TVcccX) en el cual se indica que los bloques del 63 al 79 son utilizados por la empresa ST para almacenar una firma digital que permita para quienes adquieran el chip poder validar su autenticidad. Esta firma es específica para cada chip porque utiliza el ID del chip para formar esa firma digital.

Descripción de la Prueba:

La prueba inicia con analizar el contenido del datasheet del fabricante del chip ST FRID EEPROM (ST25TVcccX) en el cual se indica que los bloques del 63 al 79 son utilizados por la empresa ST para almacenar una firma digital que permita para quienes adquieran el chip poder validar su autenticidad. Esta firma es específica para cada chip porque utiliza el ID del chip para formar esa firma digital.

Para esto se requirió acceder a un documento del fabricante (para el cual se requiere firmar un NDA), en el cual se indican las instrucciones que permiten acceder al contenido de los bloques del 63 al 79.

Por medio de un script de Python se implementan esas instrucciones y se puede validar el contenido, tanto en hexadecimal como en código ASCII de lo que está almacenado en forma inicial en el chip.

Estos datos pueden compararse con el contenido del chip por medio de alguna aplicación, en nuestra prueba utilizando NFC Reader en sistema operativo Android.

También se realizó la prueba con una boleta que contaba con firma digital del fabricante en los bloques del 63 al 79. En esta prueba se utilizó la boleta para realizar una votación y validar que una vez que se confirmaron las elecciones del elector, se pudo constatar en el código de la aplicación que además cada bloque es inicializado en cero antes de grabar el voto.

El contenido del voto se guarda encriptado en el chip en los bloques del 1 al 13 y que los bloques del 63 al 79 se reinician en cero.



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



Se verifica que el elector en este modo también puede confirmar la selección guardada en el Chip e impresa en la boleta, introduciendo la boleta nuevamente en la ranura de la impresora y el sistema procederá con la lectura de lo que se guardó en el chip RFID.

Resultados de la prueba:

Mediante esta prueba se comprobó el contenido de los bloques 63 al 79 de los chips del fabricante ST son los mismos según una aplicación de un tercero comparados con los del script generado con las especificaciones del fabricante.

EVALUACIÓN DE LOS PROCESOS

Durante la evaluación de los procesos del sistema, de capacitación, de soporte técnico, de carga de datos, de validación de pantallas, de aceptación y sellado de versiones, de distribución de software, de procesos en mesa antes de las elecciones, se realizó una revisión y análisis de los diferentes manuales y procedimientos involucrados en el proceso de votación electrónica, con el objetivo de conocer su existencia y alcances.

Los elementos que fueron considerados para realizar esta evaluación son los siguientes:

- Se evaluó el alcance y amplitud del manual del sistema, con el objetivo de identificar las etapas, límites, seguridad, y los participantes en el sistema.
- Se evaluó la documentación de características funcionales y no funcionales del sistema, con la finalidad de conocer los requerimientos y comportamiento del sistema de votación electrónica.
- Se evaluó el procedimiento de la carga de los datos de la elección, con el objetivo de determinar la seguridad, la calidad de los datos, y medir su eficiencia.
- Se evaluaron los procedimientos para la verificación y validación de las pantallas, mediante la utilización de la comprobación del código fuente y el análisis del sistema.
- Se evaluaron los procedimientos para la verificación de la autenticidad del software a utilizar, para determinar la existencia de un sellado del software de votación y la generación de medios o discos DVD.
- Se evaluaron los procedimientos para la distribución y personalización del software a utilizar en cada mesa de votación, con el objetivo de conocer como el software realiza este proceso y cuales son las medidas de seguridad implementadas.

- Se evaluaron los procedimientos de despliegue y repliegue de las máquinas de votación y se evaluaron los procedimientos de almacenamiento, distribución y custodia de las máquinas, con el objetivo de conocer y analizar el proceso de despliegue y repliegue de todo el material electoral, incluidas las máquinas de votación tanto en el proceso electoral como en el de capacitación.
- Se evaluó el procedimiento de soporte técnico, para conocer y analizar las funciones que debe cumplir el personal técnico del Tribunal Superior de Justicia Electoral durante los procesos de apertura de mesa, votación, cierre de mesa y escrutinio.
- Se evaluó el alcance y amplitud de los manuales de capacitación al electorado, con el objetivo de determinar las herramientas utilizadas por las partes interesadas para conocer e interactuar con el sistema y las máquinas de votación antes de realizar el sufragio oficial.
- Se evaluó el alcance y amplitud de los manuales de capacitación de las autoridades de mesa, con el objetivo de identificar y analizar las funciones que debe cumplir cada miembro de las mesas electorales.

VALIDACIÓN DEL PROCESO DE TESTEO DEL FUNCIONAMIENTO DE LAS MÁQUINAS DE VOTACIÓN ELECTRÓNICA

De acuerdo con el “Manual de Procedimientos para la Capacitación, Preparación, Distribución y Recolección de las Máquinas de Votación, Materiales, Documentos y Útiles Electorales”, el día anterior a las elecciones a las 14:00 horas, los funcionarios que actúan como Soporte Técnico de las máquinas de votación realizarán una verificación de estas en el local de votación, a fin de garantizar el buen funcionamiento para su uso durante las votaciones.

Con el fin de verificar el cumplimiento de este proceso, el equipo de auditoría en compañía del personal asignado por el Tribunal Superior de Justicia Electoral se hizo presente en el Centro de Votación en la Escuela Molinos Harineros del Paraguay, ubicada en la zona de Ita Pyta Punta en la ciudad de Asunción.



Para iniciar el proceso, la persona asignada como soporte técnico en este recinto, constató la presencia de los apoderados de las organizaciones políticas y de los miembros de mesa ante los cuales, y en presencia del personal de la Policía que resguarda el local, realizó la apertura de las 3 cajas selladas que contenían las máquinas de votación.



Se nos indicó que en este recinto electoral se instalarán dos juntas receptoras de voto las cuales ocuparian una máquina cada una, quedando la tercera máquina como un equipo de contingencia; se nos indicó también que en este recinto electoral existirá un punto de capacitación a la ciudadanía con lo cual existe una cuarta máquina que puede ser usada como una segunda contingencia en caso de necesitarla.



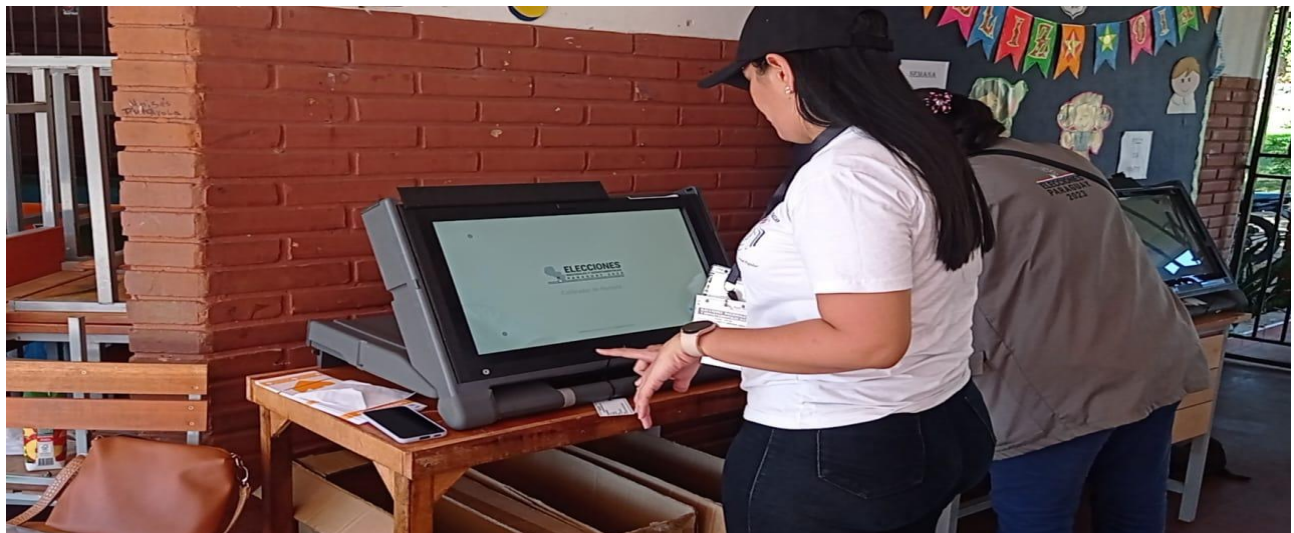
Una vez instalados los equipos, se esperó hasta las 14:00 para iniciar este proceso y así dar cumplimiento al procedimiento establecido por el Tribunal Superior de Justicia Electoral.

El proceso inició con el encendido de todos los equipos y con un disco DVD que contiene únicamente el módulo de diagnóstico de los componentes de la máquina de votación.

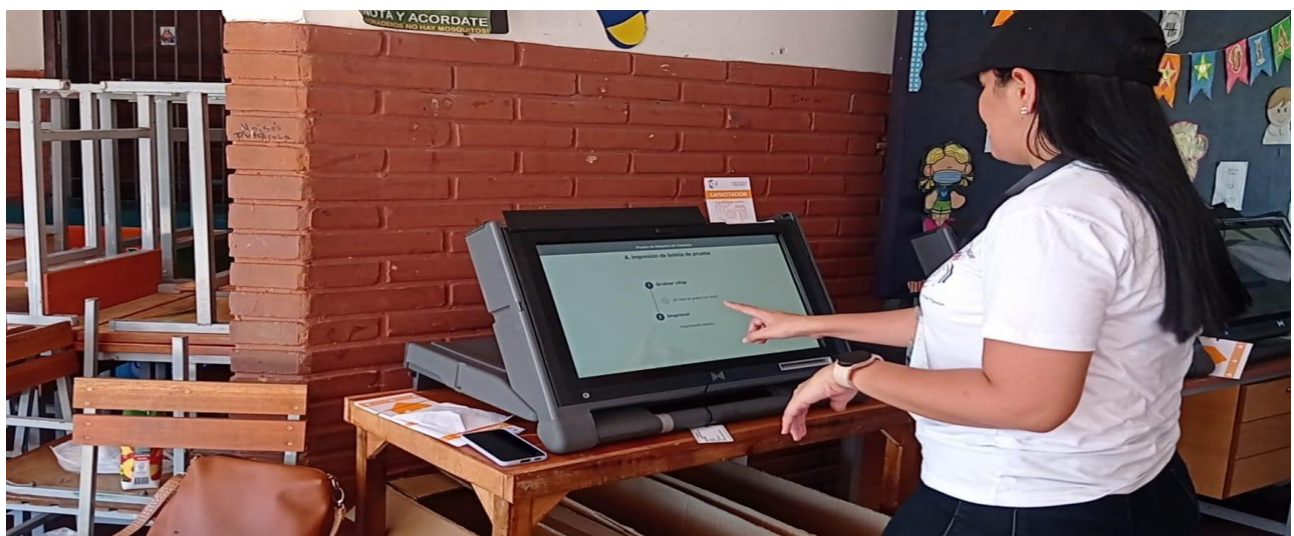


Máquina por máquina se fue realizando los test de comprobación con las siguientes pruebas:

- Calibración de la pantalla



- Grabación del chip de una boleta de prueba



- Impresión en la boleta



- Comprobación de la lectura del Chip

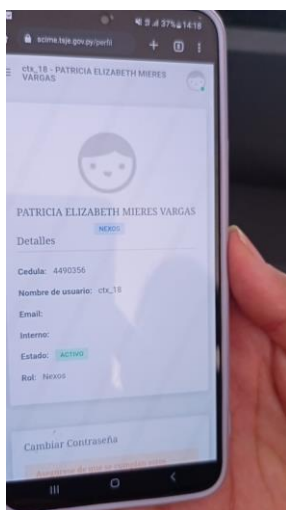


Una vez realizadas estas comprobaciones y con la aceptación de los presentes, la máquina testeada fue apagada.



Posterior a esto se realizó el mismo procedimiento con la segunda y tercera máquina teniendo como única observación que en el caso de la segunda máquina se tuvo que realizar un segundo intento de comprobación del funcionamiento del equipo ya que en una primera instancia la máquina se reinició sin completar el procedimiento de testeo.

Una vez realizada la comprobación, se tomaron los códigos de identificación de cada máquina para a través de la aplicación correspondiente, notificar al Centro de Información y Monitoreo Electoral (CIME), acerca de los resultados de las pruebas realizadas.



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

Finalizado este proceso las máquinas fueron embaladas y selladas para nuevamente ponerlas en custodia de los miembros de la policía.



OBSERVACIÓN DEL PROCESO DE SUFRAGIO

Apertura del Sufragio.

El día 30 de abril del año 2023, con el fin de verificar el cumplimiento de este proceso, el equipo de auditoría en compañía del personal asignado por el Tribunal Superior de Justicia Electoral se hizo presente en el Centro de Votación en la Universidad Católica, ubicada en la zona de Asunción con 9 mesas electorales, cada una con una máquina de votación electrónica asignada.

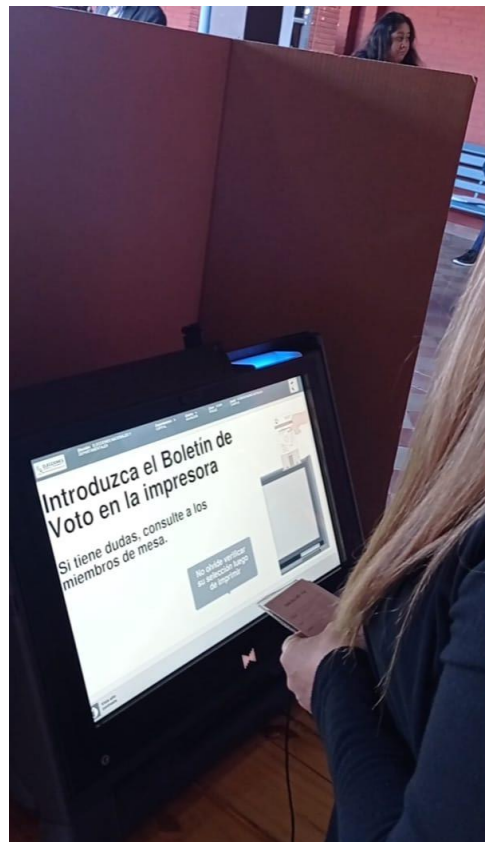
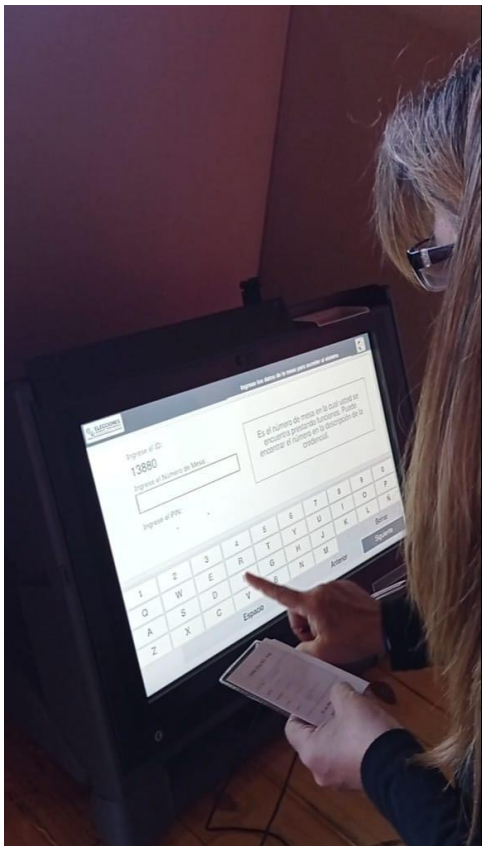


AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

Previo al inicio de la elección, los funcionarios que actúan como soporte técnico instalaron las máquinas de votación electrónica en el local de votación, y se encendieron para su uso durante el sufragio.



Para iniciar el proceso, la persona designada como presidente de la mesa ante la presencia de los otros miembros de mesa, veedores y apoderados, realizaron el proceso de apertura de la mesa, encendiendo la máquina de votación electrónica, calibrando la pantalla y utilizando su credencial y dando los datos requeridos.



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

Una vez instalados los equipos y realizada la apertura, se procede a iniciar las votaciones. Se constató por parte del equipo de auditoría que el proceso de votación transcurrió de manera normal en el inicio de la votación.



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



Luego el equipo de auditoría se trasladó al Colegio Nacional Dr. Juan José Soler situado en Villa Elisa Central para validar con los personeros del Tribunal Superior de Justicia Electoral destacados en ese lugar con 21 mesas cada una de ellas con 2 máquinas de votación. El proceso transcurrió de forma normal. Consultados los encargados de soporte de las incidencias presentadas, indicadas que se debían especialmente a errores de los votantes.

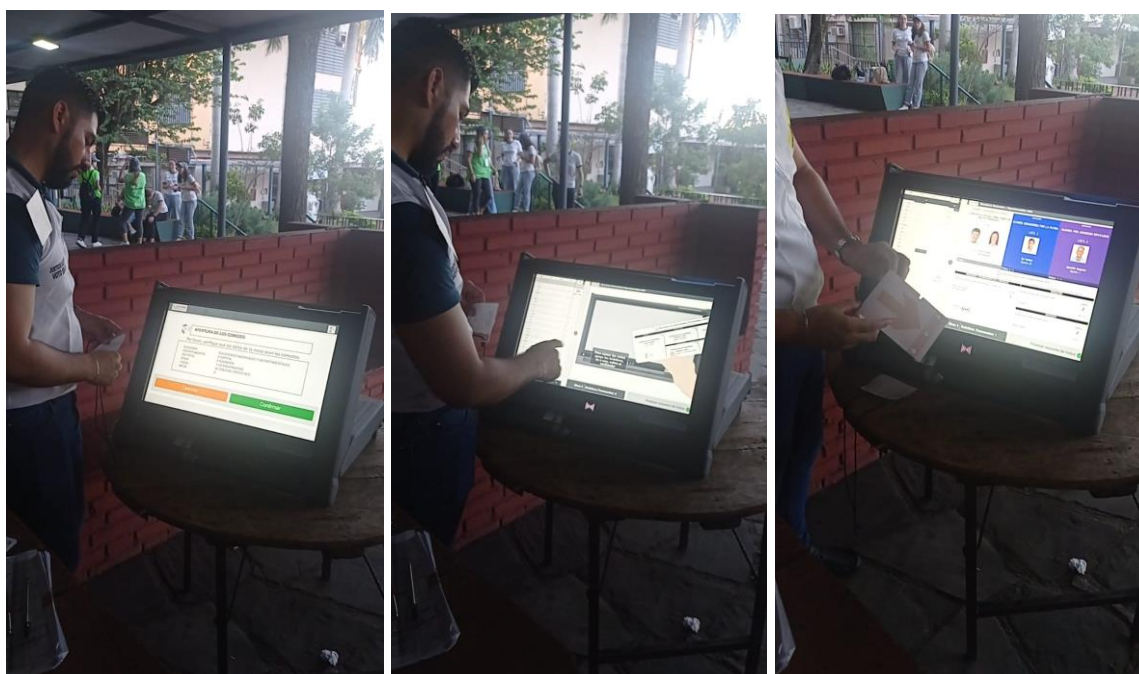


Proceso de cierre del Sufragio.

El equipo de auditoría se trasladó al Colegio Cristo Rey en la zona de Encarnación, Asunción para verificar el proceso de cierre de las mesas de votación, en este centro eran 5 mesas con 5 máquinas de votación.

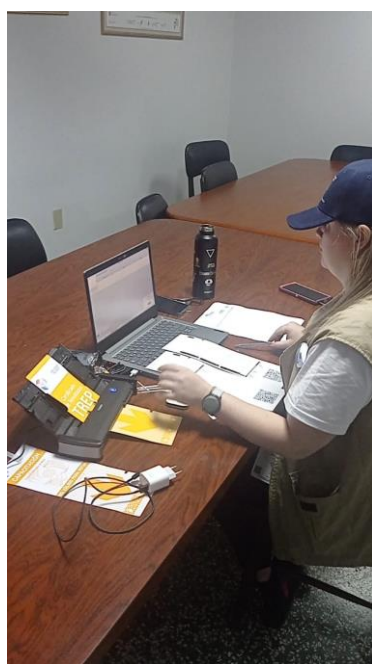
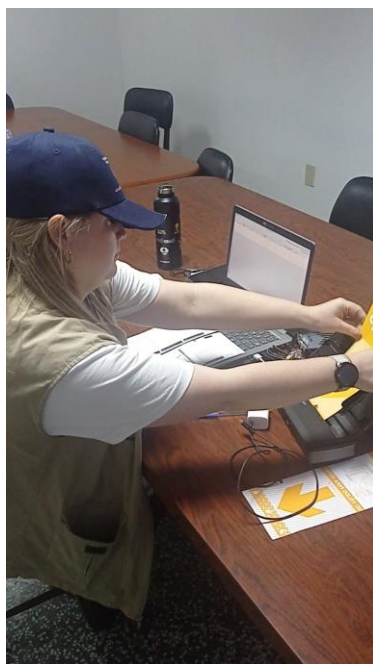


Una vez que se cerró la mesa y se procesó el último voto, la máquina de votación se cambió de modo por parte del presidente de la mesa para proceder al cierre y a la impresión de las diversas actas.



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

Una vez impresos los certificados de resultados y firmadas por los miembros de mesa, se le entregan al encargado del Centro de Votación por parte del Tribunal Superior de Justicia Electoral, quien procede a llevarlas a centro de transmisión de datos para entregarlos por medio del TREP. Además, el presidente de mesa imprime las Actas de escrutinio y por último los Certificados de Resultados TREP.



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



Se constató por parte del equipo de auditoría que la mesa 3 cumplió con todo lo dispuesto y todo el proceso de cierre se realizó de una manera adecuada.

VALIDACIÓN DEL PROCESO DE REPLIEGUE DE LAS MÁQUINAS DE VOTACIÓN ELECTRÓNICA.

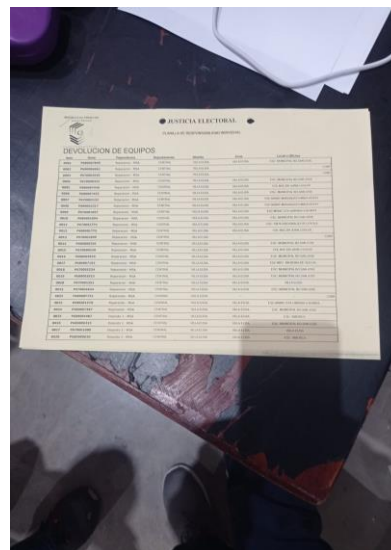
De acuerdo con el “Manual de Procedimientos para la Capacitación Preparación, Distribución y Recolección de las Máquinas de Votación, Materiales, Documentos y Útiles Electorales”, indica que una vez terminado el escrutinio e impresos los certificados del TREP y las actas electorales, los integrantes de la mesa con el apoyo del soporte técnico, procederán a extraer el disco DVD, el cual pondrán en el sobre N° 5 (vuelta) con la credencial electrónica del presidente de mesa, apagarán la máquina de votación y los entregara al soporte técnico designado para el repliegue respectivo.

En este proceso de repliegue son los coordinadores departamentales, los encargados de reunir todas las máquinas de votación y trasladarlas hacia el depósito establecido previamente por el Tribunal Superior de Justicia Electoral.

El depósito de máquinas de votación está ubicado en el distrito Fernando de la Mora en la Ciudad de Asunción. El equipo de auditoría realizó una visita al depósito de máquinas de votación para validar el proceso de repliegue.

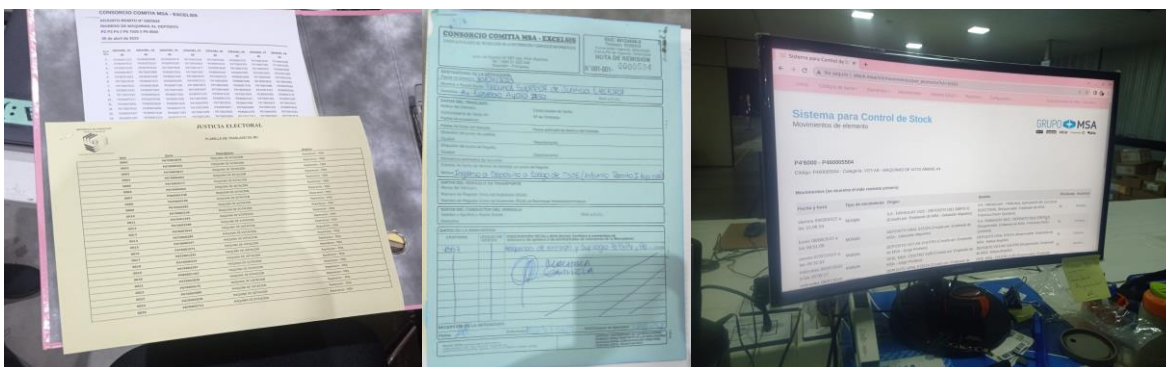


Este proceso inicia con la recepción de los equipos por parte del personal del Tribunal Superior de Justicia Electoral, quienes, a través de la lectura del código de barras de identificación de cada máquina, realiza su ingreso registrándolo en el Sistema de Recepción y Salida de Máquinas. Por temas logísticos este ingreso es realizado en grupos de hasta 48 equipos luego de lo cual es impreso un reporte del número de equipos registrados.



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

Una vez registradas las máquinas de votación en el sistema del Tribunal Superior de Justicia Electoral, estas son entregadas al personal de la empresa proveedora Grupo MSA con el reporte impreso en su ingreso. El personal de la empresa a su vez realiza un segundo ingreso de los equipos en su propio sistema de inventarios del cual generan un segundo reporte que es entregado al personal del Tribunal Superior de Justicia Electoral para el cruce y comprobación de la información.



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023

El personal técnico de la empresa Grupo MSA una vez registrado los equipos en su sistema, procede a la revisión técnica de las máquinas. En este proceso, se hace una verificación física de los equipos para detectar golpes o trizaduras, además, se procede a realizar una verificación de los componentes utilizando el disco DVD con el Sistema de Verificación.



Los equipos que tienen que ser reparados son marcados y separados para su ingreso en el taller, y los equipos con trizaduras o daños mayores, son reportados al Tribunal Superior de Justicia Electoral para los trámites pertinentes de acuerdo con el contrato con la empresa Grupo MSA.



CAPÍTULO IV

CONCLUSIONES FINALES

AUDITORÍA DE LA SEGURIDAD

- **Evaluar los controles para arranque seguro de las máquinas de votación.**

Durante el análisis realizado, se han podido identificar que las máquinas de votación realizan un conjunto de validaciones en el proceso de arranque que garantizan que solo se pueda iniciar la máquina con un medio de arranque autorizado. Esto asegura que cualquier intento de iniciar la máquina con un medio no autorizado, como una unidad de DVD, CD, USB o un disco duro externo, sea bloqueado.

Además, se ha llevado a cabo varias pruebas en el disco DVD que contiene el sistema de votación, las cuales han permitido comprobar que este realiza validaciones en el proceso de arranque para garantizar que solo se permita iniciar en las máquinas de votación utilizadas para el proceso. El proceso de modificación de la imagen del disco DVD para hacer que su ejecución pueda realizarse en un computador de propósito general es de elevada complejidad y requeriría la inclusión de equipamiento que emule la funcionalidad de la máquina de votación.

- **Evaluar los controles y niveles de aseguramiento del sistema operativo.**

La máquina de votación utiliza una versión reducida de Ubuntu 20.04, en la cual se realizaron pruebas para identificar configuraciones o paquetes vulnerables. Los resultados demostraron que el sistema operativo se encuentra debidamente asegurado, ya que no se identificaron potenciales brechas de seguridad. No obstante, es importante mencionar que, debido a las restricciones de acceso a la shell impuestas por el aseguramiento del sistema operativo, no fue posible

obtener detalles adicionales sobre el bastionado del sistema. Cabe destacar que las restricciones de acceso a la línea de comando, es una medida de seguridad implementada en el sistema operativo, la cual no se pudo omitir durante las pruebas realizadas.

- **Evaluar la confidencialidad de la información del elector durante todo el proceso.**

Durante las pruebas realizadas se comprobó que, para leer la información de las boletas, se requiere que el lector esté a una distancia de 4 cm. Además, se utilizó un dispositivo de propósito específico para llevar a cabo auditorías que involucren tecnologías como RFID. Cabe destacar que no se realizaron pruebas con antenas de gran tamaño, amplificadores de señal u otro equipo similar, ya que se considera que la probabilidad de que alguien instale este tipo de equipos en los lugares de votación sin ser detectado por el personal de la entidad electoral o la fuerza pública es muy baja.

Por otro lado, se constató que, incluso si se lee el contenido de las boletas a distancia, el contenido de estas se encuentra cifrado mediante el algoritmo AES. En consecuencia, aún en el caso improbable de que se pudiera acceder a la información de las boletas mediante equipos no autorizados, el contenido seguiría estando protegido por este cifrado.

- **Evaluar los controles de integridad que garantizan la inalterabilidad de la votación.**

Durante las pruebas realizadas, se intentó modificar el contenido de las boletas sin éxito. Esto se debe a tres factores clave: en primer lugar, el contenido de las boletas se almacena de manera cifrada utilizando el algoritmo AES. En segundo lugar, la llave de cifrado es única para cada mesa y el Vector de Inicialización (IV) es único para cada boleta. En tercer lugar, una vez que se escribe en las boletas, estas se ponen en modo de solo lectura, estos tres factores juntos generan una gran dificultad para llevar a cabo la alteración de los resultados.

Es importante destacar que para lograr una modificación masiva que afecte el resultado de la elección, la dificultad se eleva aún más, porque habría que omitir

los tres factores clave mencionados previamente, en cada una de las mesas. En consecuencia, se considera que el sistema cuenta con niveles de seguridad adecuados para garantizar la integridad de los resultados electorales.

- **Evaluar los controles para garantizar la disponibilidad del sistema de votación durante toda la jornada electoral.**

En las pruebas realizadas se ha podido comprobar que las máquinas de votación utilizadas no dependen de las mesas de votación, lo que significa que estas no almacenan información relacionada con la elección que las vincule a una ubicación específica. Esto permite que cualquier máquina de votación pueda ser inicializada para reemplazar a otra que esté defectuosa o dañada, lo que aumenta significativamente la disponibilidad del sistema, ya que no se limita a un solo reemplazo.

Además, se ha identificado que las máquinas de votación cuentan con dos baterías y un conector eléctrico, lo que asegura un respaldo eléctrico que contribuye a la alta disponibilidad del sistema de votación. Esta característica garantiza que el sistema esté siempre funcionando, incluso en caso de una interrupción inesperada del suministro eléctrico.

Por lo tanto, la combinación de la posibilidad de múltiples reemplazos de máquinas de votación y el respaldo eléctrico asegurado por las baterías y el conector eléctrico, hacen que el sistema de votación sea altamente disponible y pueda funcionar de manera continua durante toda la jornada electoral.

- **Realizar análisis de vulnerabilidades.**

Durante el análisis de vulnerabilidades del código de la aplicación, se utilizaron más de 200 reglas que permiten identificar omisiones a las buenas prácticas de desarrollo seguro, con el objetivo de prevenir posibles vulnerabilidades en la aplicación. Los resultados demostraron que solo se identificó una vulnerabilidad, la cual no representa un riesgo significativo para el sistema debido a la naturaleza de este y las interfaces de acceso limitadas para la operación de la máquina de votación por parte del votante.

El análisis de vulnerabilidades realizado incluyó una revisión exhaustiva de los paquetes de software y librerías que forman parte del sistema operativo, específicamente se examinaron 610 paquetes y en las versiones instaladas no se encontraron vulnerabilidades reportadas hasta el momento de la realización del ejercicio.

- **Realizar análisis de penetración utilizando como referencia OWASP Desktop App Security, entre otras.**

Se realizaron pruebas de intrusión sobre el software y el hardware de la máquina de votación, para el caso del hardware las pruebas se concentraron en hacer que la máquina interactúe con hardware externo no autorizado, obtener control de la máquina de votación a través de puertos de red, o un método de interacción distinto a los provistos por el mismo sistema, como por ejemplo una línea de comandos, terminal físico o similares. No fue posible obtener un acceso distinto al provisto por la interfaz de votación.

Para las pruebas del software, se entregó al equipo consultor acceso al código fuente de toda la aplicación, se pudo comprobar que este no guarda datos sensibles o información que permita obtener algún tipo de acceso no autorizado a la máquina de votación, además de que se pudo analizar los procedimientos de cifrado que, por el proceso de votación y las consideraciones de la implementación de este, mantiene una elevada postura de seguridad.

- **Realizar análisis de código fuente mediante ejecución de pruebas de código estático y dinámico.**

Se llevó a cabo una evaluación exhaustiva del código de la aplicación utilizando tanto métodos automatizados como manuales, y no se encontraron vulnerabilidades relacionadas con malas prácticas de desarrollo, uso de funciones inseguras o similares.

- **Realizar Pruebas de caja gris.**

Las pruebas de caja gris fueron realizadas en la máquina de votación electrónica, tanto en el software como en el hardware, con el fin de identificar posibles vulnerabilidades y debilidades del sistema. Se llevaron a cabo pruebas de intrusión, análisis de vulnerabilidades, evaluación de controles y niveles de aseguramiento del sistema operativo y análisis del código de la aplicación en modalidad automatizada y manual. A partir de estos análisis se pudo comprobar que el sistema presenta un alto nivel de seguridad y que se ha seguido buenas prácticas de desarrollo seguro. Se identificó una sola vulnerabilidad en la aplicación, la cual no representa un riesgo significativo para la integridad del sistema.

Después de las pruebas realizadas se puede concluir que el sistema de votación electrónica usado en la fase de sufragio, por el Tribunal Superior de Justicia Electoral de la República de Paraguay, cuenta con una elevada postura de seguridad, se recomienda agregar al alcance de un próximo ejercicio la fase de generación de credenciales, considerando que estos documentos permiten obtener la llave de cifrado de los datos que se almacenan en las boletas, así como también la inicialización de una máquina de votación.

AUDITORÍA DEL HARDWARE

- **Evaluar el diseño y construcción para las condiciones particulares de exigencia del proceso electoral.**
 1. La arquitectura de los dos modelos de máquina de votación examinados durante el trabajo de campo, corresponden a la construcción de un equipo propietario, basado en el diseño de hardware específico del fabricante para estas máquinas en particular, prescindiendo por completo de dispositivos periféricos comerciales, lo que permite un mayor control sobre la construcción de las terminales de votación, incrementa el nivel de seguridad y disminuye el riesgo de la introducción de equipos ilegítimos.
 2. Los equipos analizados cuentan con controles de arranque por medio de la personalización de la interfaz unificada de firmware extensible (UEFI por sus siglas en inglés), esta característica ofrece un mayor nivel de seguridad en el proceso de arranque del sistema operativo, dado que en este nivel de personalización se introducen llaves privadas que se utilizan para identificar el dispositivo desde el cual la máquina de votación iniciará el sistema operativo. Es decir, mediante este tipo de llaves digitales personalizadas en la UEFI se controla que la terminal de votación inicie únicamente con el sistema operativo que reside en los discos DVD que están firmados con esta llave. Cualquier otro DVD de arranque distinto a los firmados es rechazado por el equipo al momento del arranque.
 3. Debido a las características anteriores, las terminales de votación funcionan únicamente con la versión de sistema operativo que ha sido preparada para ese fin y aprobada por el TSJE, lo que a su vez constituye un control para evitar en un recinto electoral se pueda realizar un cambio del software de votación en el equipo.

4. El control de seguridad de las máquinas de votación se hace en conjunto con componentes de hardware y de software, permitiendo que se tenga un nivel de confianza en el momento de realizar el voto.
 5. El diseño de la terminal de votación incorpora diversas medidas de seguridad, como los Jammers para impedir la lectura a distancia del RFID, también las técnicas de protección que impide que se cargue cualquier software, esto garantiza su fiabilidad en el proceso electoral. Además, se han utilizado componentes de alta calidad (componentes electrónicos como chips de radiofrecuencia, controles de carga el MCU, también el procesador de marca líder Intel y componentes electrónicos pasivos como capacitores de aluminio con polímero) que permiten para asegurar su durabilidad y correcto funcionamiento. Se ha tenido en cuenta cada detalle en el proceso de fabricación y se han aplicado estándares según la IEC (International Electrotechnical Commission) e IPC (Association Connecting Electronics Industries) para asegurar la durabilidad y confiabilidad del equipo en el largo plazo. Todo ello, combinado con la implementación de medidas de seguridad físicas y tecnológicas, hacen de la terminal de votación un equipo altamente fiable para el proceso electoral.
- **Evaluar una operación aislada de cualquier tipo de conectividad con el exterior durante el proceso de votación.**
 1. Se evaluaron ambos modelos de máquinas de votación en relación con su acceso a puertos USB o de red, sin embargo, no se evidenció envío de datos a través del puerto de red. Según se muestra en la arquitectura, en el modelo más reciente (P6), los puertos USB y de red están completamente desconectados, mientras que en el modelo P4, aunque los puertos USB tienen carga eléctrica (únicamente los pines Vcc y GND), los datos del puerto están apagados por completo, lo que impide el acceso al software o al equipo en caso de conectar cualquier dispositivo, adicionalmente el puerto Ethernet está completamente deshabilitado, por lo tanto no se genera conexión de ningún tipo hacia o desde el exterior de la máquina de votación ante el intento de conectarlo a una red.

- **Evaluar la garantía de voto secreto, sin almacenar información relacionada con el voto de cada elector.**

1. El hardware utilizado en las elecciones en Paraguay es un equipo diseñado específicamente para la votación con la boleta única electrónica y cuenta con medidas de seguridad diseñadas para ese fin. En este sentido, cabe resaltar que el equipo no dispone de ningún tipo de almacenamiento para guardar información de votación, lo que asegura la confidencialidad y privacidad del proceso. Asimismo, el equipo no tiene una asignada fecha y hora, evitando cualquier tipo de registro de la actividad que pudiera comprometer la privacidad del votante.
2. En el proceso de votación, se genera una única copia del voto del ciudadano, la cual se imprime en el reverso de la boleta de votación y se almacena en un chip RFID. Es importante destacar que esta copia en el chip RFID es de solo lectura, lo que significa que no se puede modificar ni alterar de ninguna manera. La posibilidad de verificar que la información impresa en la boleta sea igual a la información digital del chip es una característica importante de las terminales de votación utilizadas en el proceso electoral.

- **Evaluar la garantía de integridad (no alteración) de la información de votos registrados electrónicamente durante todo el proceso electoral.**

1. El equipo no cuenta con conectividad externa, ni alámbrica ni inalámbrica, lo que impide la posibilidad de enviar datos desde o hacia la terminal de forma remota, lo que reduce el riesgo de manipulación externa de votos.
2. Durante el trabajo de campo en el cual se realizaron diversas pruebas y la revisión de los componentes de la máquina de votación, se evidencia que no cuentan con dispositivos de almacenamiento de información permanente, por tanto, los datos relativos a cada voto no se almacenan en las máquinas, sino que se almacenan únicamente en el chip RFID de la boleta de votación. Además, los Chips RFID utilizados operan bajo la norma ISO 15693, por lo que cuentan con un comando de bloqueo contra

escritura, bloqueo que no es reversible. Este comando se activa inmediatamente después de la rutina de grabación y verificación de escritura de voto, la cual se realiza en la terminal antes de expulsar la boleta de votación. Esta garantiza que el chip quede de solo lectura después de haberlo grabado, haciendo imposible su modificación posterior. Esta característica está presente tanto en las boletas de votación que utilizan los electores como en las boletas que registran la información para el TREP.

- **Evaluar las Condiciones para la continuidad de la operación durante toda la jornada electoral.**
 1. Entre las numerosas especificaciones de la terminal de votación, es importante destacar que el equipo cuenta con un sistema de respaldo energético propio, gracias a la incorporación de un grupo de baterías de alta capacidad. En pruebas realizadas por la TSJE y Grupo MSA, se ha constatado que la terminal de votación puede tener una autonomía de más de 12 horas con actividad de votación continua, incluso en condiciones ambientales de alta temperatura. Esta característica resulta esencial para garantizar la continuidad y fiabilidad del proceso electoral, asegurando que el equipo no se vea afectado por cortes de energía o fallas en el suministro eléctrico.
 2. Otra característica importante del terminal de votación es la fuente de alimentación esta certificada con IQC/CE y tiene normaliza de fabricación con ROHS, esto garantiza que este componente no vaya a fallar. Además, la terminal de votación está equipada con un cable de alimentación de hasta 8 metros de longitud, lo que permite su instalación en zonas atípicas donde la toma de corriente pueda estar lejos del lugar donde se necesita instalar la terminal. Esta característica resulta muy útil en contextos en los que se necesita flexibilidad en la instalación del equipo y se garantiza el correcto funcionamiento de este en cualquier situación. La terminal de votación al ser un equipo autónomo, sin conectividad, sin las capacidades

de almacenar información y sustituible, no representa un factor sensible para la continuidad de la operación durante el proceso electoral.

- **Evaluar el registro electrónico utilizado no admita lectura a distancia.**

1. Las medidas de seguridad implementadas en el equipo de votación garantizan que las boletas de votación no puedan ser interceptadas en las mesas de votación. Para lograr esto, se han utilizado varias técnicas y herramientas, entre las que se destacan las jaulas de Faraday y los Jammers. La jaula de Faraday es un dispositivo que se utiliza para bloquear las señales electromagnéticas. En el contexto de las elecciones, se utiliza para proteger el chip de la boleta de votación de interferencias externas. Las jaulas de Faraday se han instalado en las máquinas de votación para garantizar que el chip de la boleta no pueda ser leído o interceptado por dispositivos externos. Por otro lado, los Jammers son dispositivos que se utilizan para bloquear señales de radiofrecuencia. En las mesas de votación, se utilizan Jammers para evitar que dispositivos externos puedan enviar señales al chip de la boleta y alterar el proceso de votación. Estos dispositivos garantizan que nadie pueda acceder al chip de la boleta desde corta o larga distancia antes de que se escriba en él. En conjunto, estas medidas de seguridad garantizan que el proceso de votación sea seguro y confidencial. La implementación de jaulas de Faraday y Jammers impide cualquier intento de alteración o interceptación de las boletas de votación, lo que garantiza la integridad y transparencia del proceso electoral.
2. Además de las medidas de seguridad implementadas en las máquinas de votación, existen características adicionales que protegen el chip RFID fuera de la máquina de votación. Una de estas características es el uso de la misma boleta de votación para bloquear el acceso a la señal de manera cercana. Para lograr esto, la boleta de votación se debe doblar de una manera específica y alinear el doblez que la placa coincida con el chip RFID, lo que bloquea completamente la señal y evita que sea interceptada

por dispositivos no autorizados en un rango cercano. De esta manera, se garantiza la integridad y confidencialidad de los datos almacenados en el chip RFID. De esta manera, se garantiza que el proceso de votación sea justo, transparente y confiable para todos los ciudadanos participantes.

3. Tras realizar diversas pruebas, se ha concluido que los dispositivos portátiles de lecto-escritura RFID no cuentan con la suficiente potencia para leer o escribir el chip de la boleta a una distancia mayor de un centímetro. Además, una vez que se ha escrito la información en el chip de la boleta, no es posible reescribir la misma mediante ningún comando de escritura descrito en la norma ISO 15693. Por otro lado, para poder leer el chip de la boleta a una distancia de un metro, se requiere de una antena grande y muy visible, así como de equipos especializados de alta potencia. En caso de que se logre la lectura a distancia, los datos se encuentran cifrados, lo que garantiza la privacidad del voto. En resumen, se puede afirmar que los dispositivos portátiles RFID no representan una amenaza para la seguridad del voto, ya que no cuentan con la potencia suficiente para leer o escribir el chip a distancia y la información se encuentra cifrada para garantizar el secreto del voto.

AUDITORÍA DEL SOFTWARE

- **Evaluar que los procedimientos de diseño, desarrollo y versionado son adecuados.**

Se usan metodologías ágiles adaptadas como Scrum para manejar el proceso de desarrollo del software. Los documentos MT-7002 Catálogo de software BUE y MN-5000 Sistema de Boleta Única Electrónica explican las metodologías utilizadas por la empresa desarrolladora. Estas metodologías siguen los estándares de la industria y mejores prácticas para el proceso de desarrollo de software.

- **Evaluar que los aplicativos desarrollados se encuentren individualizados e identificados en un catálogo que permite validar su integridad.**

Se cuenta con un documento (MT-7002 Catálogo de software BUE) de todos los componentes de software que muestran cada aplicación de forma individualizada. A través de este documento, se pudo constatar que el aplicativo está organizado de forma modular y se encuentran individualizados e identificados claramente cada uno de esos componentes.

- **Evaluar los esquemas y estándares de seguridad utilizados.**

Estos esquemas y estándares se describen en el documento MT-7007 Seguridad informática sistema BUE. Se utilizan en el sistema diversos materiales que tienen presencia de seguridad, tales como las credenciales de autoridad de mesa y técnico, que cuentan con chip RFID. El DVD es solo de lectura y utiliza Secure Boot como elemento para asegurar que solo los discos adecuados puedan utilizarse para encender los equipos. El software a través de métodos de encriptación permite el manejo de los datos en forma segura. Además, el uso de llaves públicas y privadas para firmar las aplicaciones asegura un alto nivel de seguridad. Las boletas de

votación cuentan con chips RFID y con el estándar utilizado solo son grabadas una vez. Las actas también cuentan con un chip RFID. Los esquemas y estándares de seguridad utilizados por la empresa, se consideran estándares de la industria de software y son adecuados para este tipo de aplicación.

- **Evaluar que las capacidades de parametrización se adecúan a los requerimientos.**

El software es altamente configurable, se adecúa a los requerimientos según la definición en el Formulario de Datos de Entrada (documento MT-7009 Parametrización, personalización y autenticidad de SW BUE). Este formulario de entrada refleja lo indicado en el Pliego de la contratación y sirve para determinar los requerimientos que deben incluirse o cambiarse, todo lo cual es gestionado a lo interno de la empresa desarrolladora por medio de un sistema de tickets. Se pudo constatar que la parametrización del sistema permite cumplir con todos los requerimientos para la elección.

- **Evaluar que se realice una adecuada gestión y control de cambios.**

Mediante una adaptación de una metodología ágil, usando herramientas como Jira y Confluence, se puede indicar que se siguen las mejores prácticas de la industria. El documento MT-7002 Catálogo de Software BUE describe la gestión del proceso de desarrollo que realiza la empresa. Se ha constatado que se usan metodologías adecuadas según los estándares de la industria para el proceso de desarrollo en la gestión y control de cambios.

- **Evaluar los procesos de control de calidad y pruebas.**

Se tienen planes de pruebas acordes a los requerimientos de la elección. En el documento MN-2001 Manual de testing sistema BUE, se puede observar un detalle de las pruebas iniciales, de integración, de estrés, de usabilidad y accesibilidad, intensivas que se han realizado. Además, los procesos de presentación a los partidos políticos, tanto de hardware como software permitieron validar el funcionamiento de la máquina de votación. Las pruebas realizadas en la presente auditoría permiten concluir que los resultados obtenidos fueron exitosos en todas las categorías de pruebas evaluadas.

- **Evaluar que los casos de uso estén completos, detallados y acordes a las necesidades del proceso; y Evaluar que los casos de prueba sean exhaustivos y estén acordes a los casos de uso.**

Se validó la existencia de los casos de uso en el documento MT-7002 Catálogo de Software BUE. La revisión realizada permite concluir que los casos de uso son detallados, pero no están ajustados a los requerimientos de este proceso electoral. En consecuencia, los casos de prueba no están acordes a los casos de uso. Este desfase no representa un riesgo para la elección y que permite que el proceso electoral se lleve a cabo en forma normal.

- **Evaluar el análisis de los sistemas desde una perspectiva de desarrollo de software, de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.**

En el documento MT-7002 Catálogo de software BUE se puede ver la descripción de los componentes de software de las aplicaciones de: voto, fiscales (que se corre para validación del escrutinio) y el simulador web. La empresa utiliza máquinas de votación especialmente construidas para el desarrollo y pruebas del software, lo cual asegura la calidad y seguridad de los aplicativos. Además, como parte de las pruebas de la auditoría de

seguridad, se realizó un análisis de código fuente (Análisis de código estático y dinámico) cuyos resultados se describen en las pruebas y conclusiones de seguridad, donde no se evidencia ningún riesgo para la elección en esta materia.

- **Evaluar la integridad y la consistencia de los datos, de la información transmitida desde las máquinas de votación a las boletas de votación.**

La información transmitida desde las máquinas de votación a las boletas de votación es segura y cifrada. La boleta cuenta con una placa metálica que al doblar la boleta permite bloquear la lectura a distancia de la memoria del chip. La máquina de votación cuenta con un mecanismo denominado jaula de Faraday que permite proteger los datos que se van a almacenar en el chip RFID. La escogencia del votante se guarda en la memoria del chip RFID y se bloquea de acuerdo con el estándar 15693 en forma permanente, para que esta no pueda ser modificada. El documento MT-7007 Seguridad informática sistema BUE describe los procesos realizados para asegurar la integridad, consistencia y confidencialidad de los datos, lo cual fue constatado en la presente auditoría.

Sobre el código fuente: se revisaron los códigos fuentes de la aplicación almacenados en el DVD de capacitación suministrado al equipo auditor, se pudo constatar que se usan estándares de codificación de Python como PEP-8 y que los programas fuentes se almacenan en un repositorio de GitLab alojado en los servidores en la empresa proveedora del software que permite un control de cambios y control de acceso. Estos repositorios solicitan autenticación y registran autor del cambio, fecha y hora. Esta información está suministrada en el documento MT-7002 Catálogo de software BUE. Además, se puede concluir que el código refleja una definición modular de acuerdo con las mejores prácticas.

- **Evaluación de la información contenida en el chip ST**

Sobre el contenido del chip de la marca ST, su Ficha Técnica indica que este chip tiene grabado una firma digital generada por TruST25 (un conjunto de software y procedimientos) para probar el origen del chip en la detección de clonación. El equipo de auditoría pudo constatar a través de la APP “NFC TAG INFO”, que los chips ST contienen información en los bloques 63 al 79.

En reunión con el equipo técnico de la empresa MSA, se verificó que, a través del sistema de votación, el contenido completo del chip es inicializado en cero previo a grabar el voto en el chip, lo cual asegura que cualquier información inicial que existiera en los chips es anulada y que no exista más información que el voto generado por el ciudadano al momento del voto.

AUDITORÍA DE LOS PROCESOS

- **Evaluar el alcance y amplitud del manual del sistema.**

Los documentos “Manual de soporte técnico”, “Manual de Procedimientos para capacitación, preparación, distribución y recolección de las máquinas de votación, materiales, documentos y útiles electorales” y “Manual De Funciones de Miembros de Mesa Receptora de Votos Y Agentes Electorales”, detallan de manera precisa las distintas funcionalidades del sistema de votación, así como las distintas maneras con las que el usuario puede interactuar con la máquina de votación para su uso correcto.

- **Evaluar la documentación de características funcionales y no funcionales del sistema.**

Los documentos Manual de soporte técnico” y “Manual De Funciones de Miembros de Mesa Receptora de Votos Y Agentes Electorales” describen a detalle las características funcionales del sistema. La empresa proveedora además proporcionó el documento “MN-5000- Sistema de Boleta Única Electrónica”, en el cual se describe las características no funcionales del sistema de votación.

- **Evaluar los procedimientos para la carga de los datos de la elección.**

Conforme a la explicación realizada por la empresa proveedora y por el director de Tecnología del Tribunal Superior de Justicia Electoral, este proceso es realizado de manera simple y segura mediante el intercambio de archivos a través de servicios FTP seguros y con formatos preestablecidos entre la empresa y el órgano electoral. Este procedimiento esta descrito en el documento “Procesos Tecnológicos DTIC 2023” en su página 53 en el que se describe los pasos a seguir para el intercambio de datos electorales necesarios para los ajustes del software de votación y capacitación.

- **Evaluar los procedimientos para la verificación y validación de las pantallas.**

La empresa proveedora desarrolla una versión especial de software para que las organizaciones políticas puedan revisar las interfaces finales, incluidas las que tienen las imágenes de los candidatos que se presentarán en el software de votación oficial. Este acto denominado “Auditoría de pantallas”, es organizado por el ente electoral y consta dentro de las actividades del calendario electoral. Al ser una versión especial del software, no existe riesgo de alteración del software oficial manteniendo la integridad de la elección. Este proceso se encuentra descrito a detalle dentro del documento “Procesos tecnológicos DTIC 2023”.

- **Evaluar los procedimientos para la verificación de la autenticidad del software a utilizar.**

Existe un procedimiento para la generación del hash para el sellado del software de votación y la generación de medios – discos Master, denominado “Generación y control de calidad de medios ópticos y credenciales electrónicas a ser utilizados en las máquinas de votación”, organizado por el Tribunal Superior de Justicia y consta dentro de las actividades del calendario electoral. Al ser un acto público con la participación de las organizaciones políticas en el que a través de herramientas tecnológicas se revisa los últimos cambios realizados en el software oficial y se hace un sellado del sistema a través de la generación de un hash de este, brinda la transparencia y seguridad que se requiere en estos casos. Este proceso se encuentra descrito dentro del documento “Procesos tecnológicos DTIC 2023”.

- **Evaluar los procedimientos para la distribución y personalización del software a utilizar en cada mesa de votación.**

Existe un software único que es ejecutado en todas las máquinas de votación utilizadas en el proceso electoral. La personalización para su utilización en las distintas mesas de votación, se lo realiza a través de las credenciales con las cuales se identifica e inicializa cada una de las máquinas de votación. En el documento “Procesos tecnológicos DTIC 2023” se detalla el “Procedimiento de Generación de Medios ópticos Oficiales”, el cual describe la creación de las

credenciales utilizadas por el sistema de votación y en el documento “Manual de Procedimientos para capacitación, preparación, distribución y recolección de las máquinas de votación, materiales, documentos y útiles electorales” se registra el procedimiento para la distribución de las credenciales oficiales. Estos documentos explican claramente el manejo transparente que se le da a este aspecto tan importante de las credenciales.

- **Evaluar los procedimientos de despliegue y repliegue de las máquinas de votación y Evaluar los procedimientos de almacenamiento, distribución y custodia de las máquinas.**

Los procedimientos de despliegue y repliegue de las máquinas de votación así como su almacenamiento y custodia es un aspecto que es tratado a detalle en el documento “Manual de Procedimientos para capacitación, preparación, distribución y recolección de las máquinas de votación, materiales, documentos y útiles electorales”, en el que se describe a detalle el proceso de despliegue y repliegue de todo el material electoral, incluidas las máquinas de votación tanto en el proceso electoral como en el de capacitación. Esto se pudo constatar en la visita realizada al centro de distribución en la que de manera conjunta el personal del Tribunal Superior de Justicia Electoral y el personal de la empresa proveedora realizan de manera coordinada, estricta y ordenada los procesos de despliegue y repliegue de las máquinas de votación.

En la visita realizada al centro de distribución, también se pudo constatar las condiciones óptimas de almacenamiento de los equipos y la seguridad que tienen las instalaciones provistas por el personal de las fuerzas armadas en trabajo conjunto con el personal de seguridad del ente electoral.

- **Evaluar los Procedimientos de Soporte Técnico.**

Estos se encuentran bien definidos y documentados en el “Manual de Soporte Técnico” que describe a detalle las funciones que debe cumplir el personal técnico del Tribunal Superior de Justicia Electoral durante los procesos de apertura de mesa, votación, cierre de mesa y escrutinio. Además, existen los manuales de la máquina p4 y p6 en los que se explica el manejo a detalle de cada uno de los modelos de máquinas de votación utilizadas en el proceso electoral. También se pudo constatar que la empresa proveedora tiene personal de soporte técnico que pone a punto los equipos en el centro de distribución, siendo un apoyo técnico importante para el normal desenvolvimiento del proceso electoral.

- **Evaluar el alcance y amplitud de los manuales de capacitación al electorado.**

Se constató que se elaboró varios materiales de capacitación como manuales, simuladores, aplicaciones móviles, y otros. Esto juntamente con las campañas de capacitación realizadas han permitido que el elector tenga un conocimiento previo del proceso de votación y ha facilitado el proceso de votación ya que pudieron conocer e interactuar con el sistema y las máquinas de votación antes de realizar el sufragio oficial.

- **Evaluar el alcance y amplitud de los manuales de capacitación de las autoridades de mesa.**

El documento “Manual de Funciones Miembros de Mesa Receptora de Votos y Agentes Electorales” describe las funciones que debe cumplir a detalle los miembros de las mesas electorales. También se crearon videos de capacitación en el que se indica las funciones que deben cumplir los miembros de mesa y su interacción con la máquina de votación lo que facilita y hace más eficaz la participación de los miembros de las mesas electorales tanto en el proceso de votación como en los procesos de cierre de mesa y escrutinio.

- **Evaluar el proceso de testeo de las máquinas de votación electrónica**

El proceso de testeo de las máquinas de votación se realizó de manera normal y la persona de soporte técnico del Tribunal Superior de Justicia Electoral conocía a perfección el procedimiento.

- **Evaluar el proceso de sufragio con las máquinas de votación electrónica**

EL proceso de sufragio se realizó de manera normal, en algunas mesas se observó grandes filas, pero esto se debió al tiempo que tardaban algunas personas en la realización del voto, principalmente personas de la tercera edad. También se tuvo conocimiento que a nivel nacional fallaron alrededor de 75 máquinas de votación, las cuales fueron reemplazadas con las máquinas de contingencia, lo que no tuvo ninguna injerencia en el proceso.

- **Evaluar el proceso de repliegue de las máquinas de votación electrónica**

Se pudo validar que el proceso de repliegue luego de realizadas las elecciones se efectuó con total normalidad y que el personal tanto del Tribunal Superior de Justicia Electoral como de la empresa proveedora conocen y ejecutan uno a uno los pasos establecidos en este procedimiento de repliegue de acuerdo con lo planificado por el órgano electoral.



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



Asunción, Paraguay, 04 de mayo de 2023.

Carlos Roberto Silva
Auditor Líder

Jorge Ignacio Moya Polanco
Especialista en Seguridad Informática

José Feghali Jabr
Especialista en Electrónica y
Arquitectura de Computadoras

Marcelo Olivo Pila
Especialista en Implementación de
Sistemas informáticos Electorales y
Producción de Software.

Jeff Schmidt Peralta
Especialista en Producción de
de Software e Ingeniería de
Computadoras



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



ANEXOS

SECURITY ASSESSMENT - MAQUINA DE
VOTACION ELECTRÓNICA VOT-AR

TRIBUNAL SUPERIOR DE JUSTICIA ELECTORAL -
REPÚBLICA DEL PARAGUAY

COD: OS-ELEC-2023-01
04 de abril de 2023

Aviso de Confidencialidad

La información contenida en el presente documento es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de este documento no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este documento por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

Índice general

1. Informe Ejecutivo	2
1.1 Resumen de Vulnerabilidades	2
2 Alcance y Contexto del Análisis	3
2.1 Datos de la Aplicación	3
2.3 Metodología	3
3 Resultado de Pruebas y Narrativa	4
3.1 Arquitectura de la aplicación:	4
3.2 Análisis Estático	4
3.2.1 Otros hallazgos	7
3.3 Análisis Dinámico	8
3.3.1 Instalación en Sistema Operativo	8
3.3.2 Ejecución del sistema de elecciones en VM	10
3.3.3 Escaneo de Vulnerabilidades	12
3.4 Pruebas de Hardware	15
3.4.1 Evaluar una operación aislada de cualquier tipo de conectividad con el exterior durante el proceso de votación	15
3.4.2 Evaluar la garantía de voto secreto, sin almacenar información rela- cionada con el voto de cada elector	18
3.4.3 Evaluar la garantía de integridad (no alteración) de la información de votos registrados electrónicamente durante todo el proceso electoral	19
3.4.4 Verificar boot desde DVD de arranque de Windows / Linux.	21
3.5 Análisis de RFID	22
3.5.2 Cifrado de contenido de boleta	25
3.5.3 Distancia de Lectura	26
4. Remediación	28
5. Conclusiones	28

1. Informe Ejecutivo

Esta actividad fue realizada entre el 27 y el 30 de marzo de 2023. Los objetivos del análisis fueron los siguientes:

- Evaluar los controles para arranque seguro de las máquinas de votación.
- Evaluar los controles y niveles de aseguramiento del sistema operativo.
- Evaluar la confidencialidad de la información del elector durante todo el proceso.
- Evaluar los controles de integridad que garantizan la inalterabilidad de la votación.
- Evaluar los controles para garantizar la disponibilidad del sistema de votación durante toda la jornada electoral.
- Realizar análisis de vulnerabilidades.
- Realizar análisis de penetración utilizando como referencia OWASP Desktop App Security, entre otras.
- Realizar análisis de código fuente mediante ejecución de pruebas de código estático y dinámico.

Este análisis se realizó en modo de caja gris, se proporcionó el código fuente de la aplicación, credenciales para inicialización de la máquina de votación, liveDVD usado para el arranque de la máquina de votación. No se proporcionaron accesos de línea de comandos o la posibilidad de interactuar con la máquina de votación a través de métodos distintos a la interface de votación.

En el escenario previamente descrito, y en el periodo de análisis, no se logró obtener acceso no autorizado a la máquina de votación, ni la ejecución de acciones que representen un potencial riesgo de alteración de la votación u omisiones de las reglas del proceso de sufragio.

Este es un resultado positivo en términos de seguridad del sistema de votación electrónica, ya que se demostró la capacidad de resistir ataques en un escenario controlado, donde se proporcionaron varios recursos para la realización de las pruebas. Sin embargo, es importante tener en cuenta que este tipo de análisis representa una fotografía en el punto de la ejecución del ejercicio, y la identificación de vulnerabilidades está en constante cambio. Por lo tanto, se recomienda mantener la revisión y actualización periódica de los controles y medidas de seguridad implementados en el sistema de votación electrónica para garantizar la integridad y confidencialidad del proceso de sufragio.

1.1 Resumen de Vulnerabilidades

Vulnerabilidad	Detalle	Severidad	Remediación
Escape automático en los motores de plantillas deshabilitado	Referirse al punto 3.2	Baja	Referirse al punto 4, ítem 1

2 Alcance y Contexto del Análisis

2.1 Datos de la Aplicación

- **Sistema Operativo:** GNU/Linux modificado, base Ubuntu 20.04 LTS.
- **Kernel:** 5.4.0-100-generic
- **Lenguaje de programación del sistema:** Python3
- **Líneas de Código:**

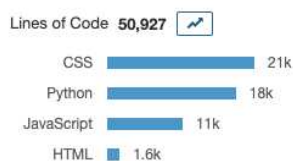


Figura 1: Detalle de líneas de código:

2.3 Metodología

La metodología utilizada para el presente análisis es PTES (Penetration Testing Execution Standard), que es un estándar para la realización de pruebas de penetración que proporciona una guía completa y detallada de los procesos, técnicas y herramientas que se utilizan en este tipo de pruebas. La metodología PTES se divide en siete fases: Pre-Explotación, Recopilación de Información, Detección de Vulnerabilidades, Explotación, Post-Explotación, Análisis y Presentación del Informe. Esta metodología se enfoca en proporcionar un enfoque sistemático y estandarizado para llevar a cabo pruebas de penetración efectivas y confiables.

3 Resultado de Pruebas y Narrativa

3.1 Arquitectura de la aplicación:

La aplicación analizada está desarrollada en el lenguaje de programación Python, utiliza las librerías GTK y webkit para renderizar los archivos javascript. El acceso al sistema es a través de un liveDVD que arranca el sistema operativo en memoria, la máquina de votación donde inicia el sistema operativo no dispone de dispositivos de almacenamiento persistente.

3.2 Análisis Estático

En el análisis automatizado de código estático realizado, se obtuvo el siguiente resultado:

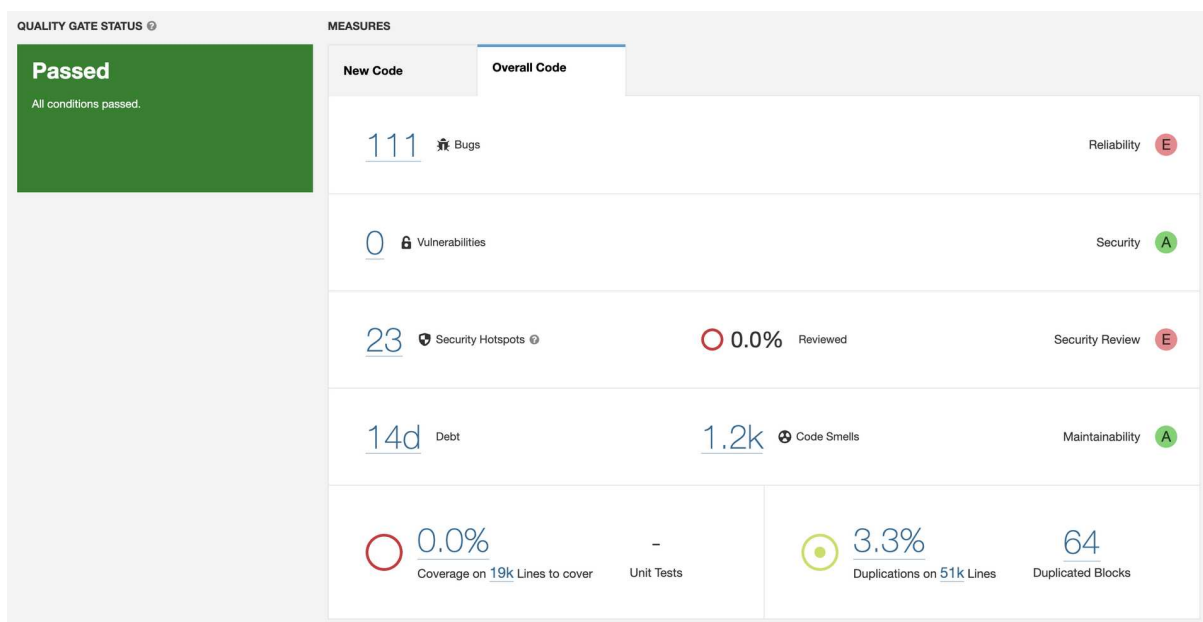


Figura 2: Resultado de análisis de código estático.

No se identificaron vulnerabilidades relacionadas al código.

Sin embargo el software alerta de 23 advertencias que deben ser revisadas de manera manual.

De los 23 hallazgos, se pudo identificar 1 de ellos podría permitir la ejecución de XSS (Cross Site Scripting).

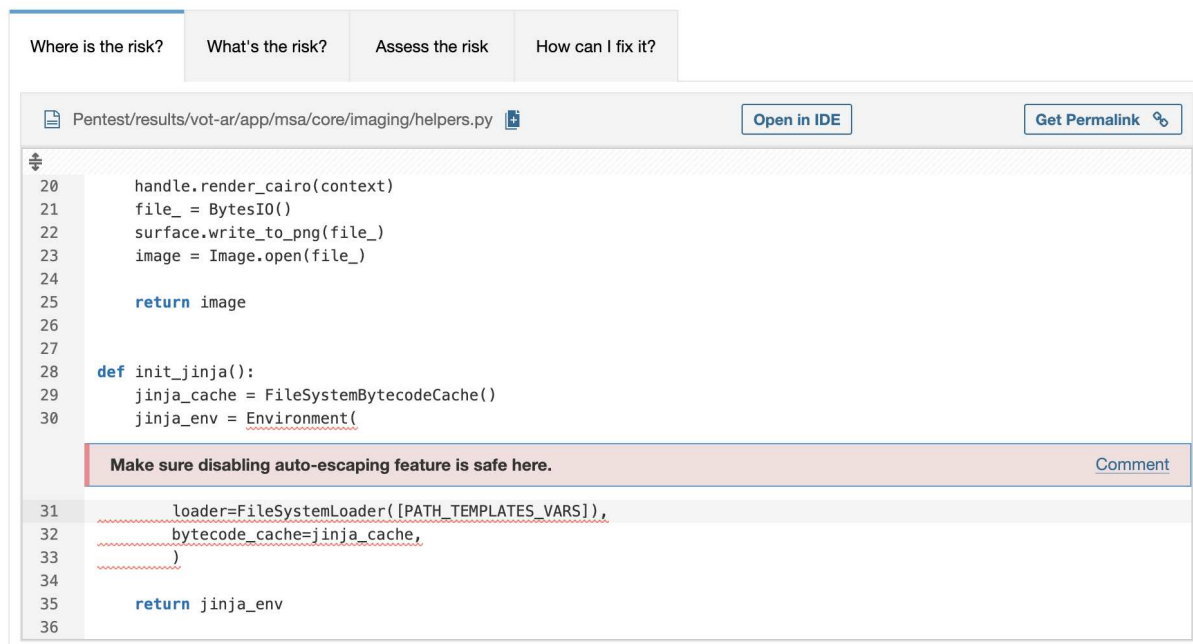


Figura 3: Código con vulnerabilidad.

El archivo donde se presenta la vulnerabilidad es `app/msa/core/imaging/helpers.py`, la herramienta informa que la funcionalidad auto-escape no está habilitado.

El auto-escape es una función de seguridad en los sistemas de plantillas que escapa automáticamente caracteres especiales en las cadenas de entrada para evitar la inyección de código, como la inyección de scripts en el lado del cliente (Cross-Site Scripting o XSS). Cuando el auto-escape está habilitado, los caracteres potencialmente peligrosos, como `<`, `>`, `&`, `'` y `"`, se convierten en sus equivalentes seguros (por ejemplo, `<`, `>`, `&`, `'`, y `"` respectivamente).

Aquí hay un ejemplo de cómo se vería el auto-escape en acción:

Entrada sin escapar:

```
1 <script>alert("XSS")</script>
```

Entrada auto-escapada:

```
1 &lt;script&gt;alert("XSS")&lt;/script&gt;
```

Si se deshabilita el auto-escape en un entorno donde se manejan datos no confiables (por ejemplo, datos de entrada proporcionados por usuarios), podría permitir a un atacante inyectar código malicioso en la aplicación, si la aplicación estuviera disponible para su interacción en un navegador web o una interface similar. A pesar de esta vulnerabilidad, no se considera que represente un riesgo significativo para la integridad del sistema o el proceso de votación en sí. La razón principal

por la que esta vulnerabilidad no representa una amenaza importante se debe a la naturaleza del sistema y las interfaces de acceso limitadas que tiene el votante para interactuar con la máquina de votación. El diseño del sistema asegura que los votantes tengan acceso restringido a las funcionalidades y componentes críticos del sistema, lo que reduce la posibilidad de explotación de esta vulnerabilidad.

Además, se analizaron las 22 advertencias restantes, de las 23 reportadas por el software y se pudo comprobar que son falsos positivos, o no representan un riesgo a la seguridad de la aplicación:

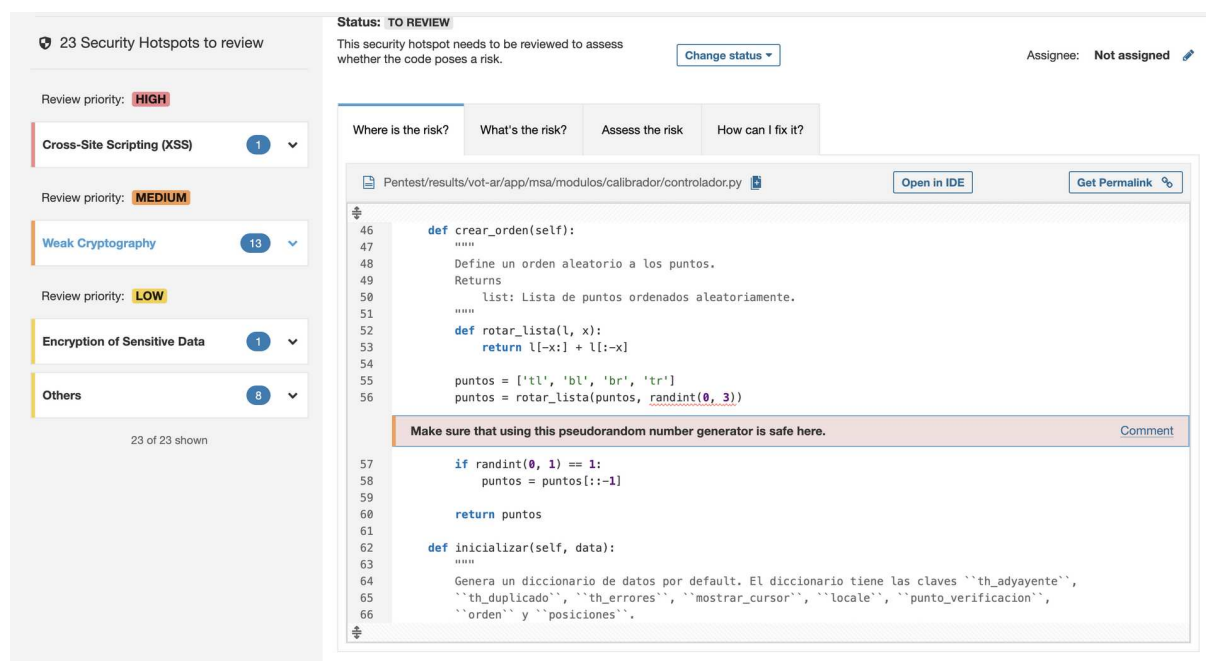


Figura 4: Falso positivo.

Por ejemplo, 13 de las advertencias, indica que se está usando un número pseudorandómico, pero analizando el código, este número es usado para la generación de los puntos para la calibración de la pantalla, por lo que no se considera un riesgo para la seguridad.

Existen otras advertencias que sugieren un análisis de la confidencialidad de los archivos, que son colocados en directorios de libre acceso para todos los usuarios del sistema operativo, como es el caso del directorio /tmp, en el caso de que estos archivos que son generados por el sistema guarden información confidencial, no deberían usar este directorio para ser escritos.

Este es el caso de:

- /tmp/%s_logstash.db
- /tmp/resultados_test_boletas.csv
- /tmp/TemplatesImpresion.json

- /tmp/TemplatesMap.json
- /tmp/downstream

Considerando la naturaleza del equipo, no se considera una vulnerabilidad, sin embargo se sugiere su análisis. Esta configuración se encuentra en el archivo `/app/msa/core/logging/settings.py` como se puede ver en la imagen a continuación.

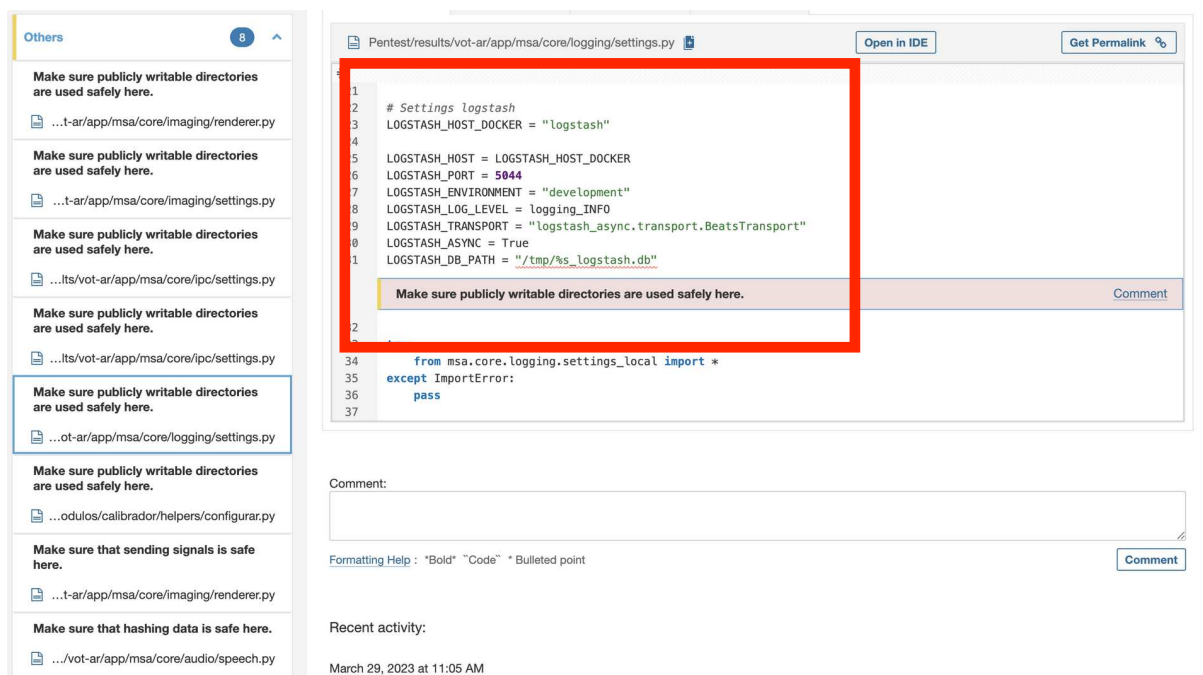


Figura 5: Alerta relacionada con la escritura en directorios de acceso público.

3.2.1 Otros hallazgos

En el análisis realizado, se encontraron 111 errores en el código relacionado a las buenas prácticas de desarrollo, de los cuales 5 son considerados bloqueantes, es decir, que deberían ser solucionados previos a un paso a producción. Sin embargo, cabe destacar que el principal enfoque de este análisis ha sido evaluar la seguridad del software y no profundizar en estos errores de desarrollo.

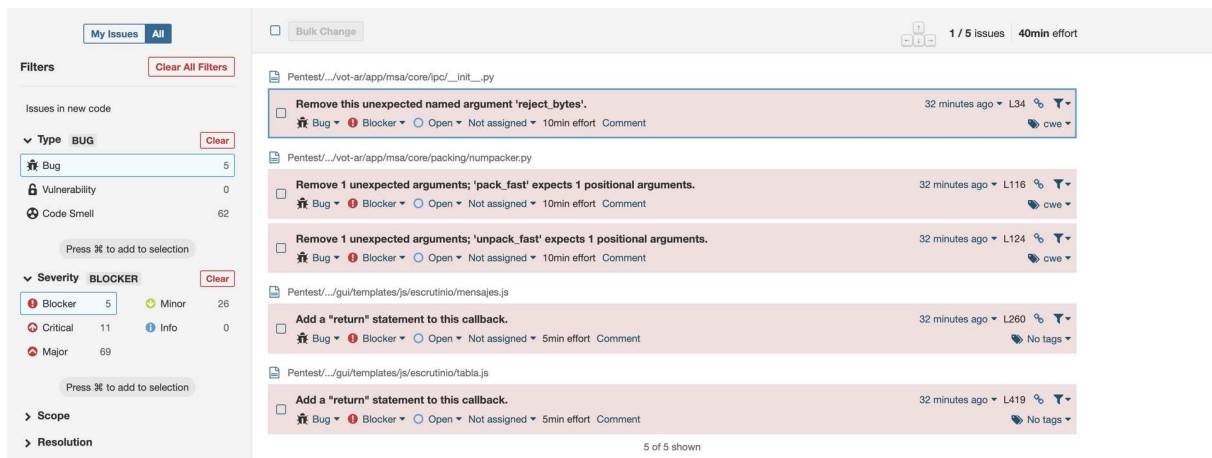


Figura 6: Otros hallazgos.

3.3 Análisis Dinámico

Para crear un entorno de prueba con el LiveDVD proporcionado se realizaron las siguientes acciones:

3.3.1 Instalación en Sistema Operativo

Se instaló Ubuntu 20.04 y luego el software que está en el archivo filesystem.manifest:

```
1 accountsservice adduser alsa-base alsa-utils base-files base-passwd bash bind9-
  dnsutils bind9-libs bsdmaintools bsdtails bubblewrap busybox-initramfs busybox-
  static casper coreutils cpio cpp cpp-9 dash dbus dbus-x11 dconf-gsettings-
  backend dconf-service debconf debianutils diffutils discover discover-data
  distro-info-data dmsetup dosfstools dpkg e2fsprogs ed eject fdisk file finalrd
  findutils fontconfig fontconfig-config fonts-dejavu-core fonts-ubuntu gcc-10-
  base gcc-9-base gettext-base gir1.2-atk-1.0 gir1.2-atspi-2.0 gir1.2-freedesktop
  gir1.2-gdkpixbuf-2.0 gir1.2-glib-2.0 gir1.2-gtk-3.0 gir1.2-harfbuzz-0.0 gir1.2-
  javascriptcoregtk-4.0 gir1.2-pango-1.0 gir1.2-rsvg-2.0 gir1.2-soup-2.4 gir1.2-
  webkit2-4.0 glib-networking glib-networking-common glib-networking-services gpgv
  grep grub-common gsettings-desktop-schemas gsfonts gstreamer1.0-plugins-base
  gstreamer1.0-plugins-good gtk-update-icon-cache gzip hicolor-icon-theme hostname
  hunspell-en-us icu-devtools info init init-system-helpers initramfs-tools
  initramfs-tools-bin initramfs-tools-core install-info iso-codes keyboard-
  configuration klibc-utils kmod language-pack-es language-pack-es-base libaa1
```

```
1 libaccountsservice0 libacl1 libapparmor1 libapt-pkg6.0 libargon2-1 libasound2
  libasound2-data libaspell15 libatk-bridge2.0-0 libatk-bridge2.0-dev libatk1.0-0
  libatk1.0-data libatk1.0-dev libatomic1 libatopology2 libatspi2.0-0 libatspi2.0-
  dev libattr1 libaudit-common libaudit1 libavahi-client3 libavahi-common-data
  libavahi-common3 libavc1394-0 libblkid-dev libblkid1 libbrotli-dev libbrotli1
  libbsd0 libbz2-1.0 libc-bin libc6 libcaca0 libcairo-gobject2 libcairo-script-
  interpreter2 libcairo2 libcairo2-dev libcanberra0 libcap-ng0 libcap2 libcap2-bin
  libcdparanoia0 libcolord2 libcom-err2 libcrypt-dev libcrypt1 libcryptsetup12
  libcups2 libdatrie-dev libdatrie1 libdb5.3 libdbus-1-3 libdbus-1-dev libdconf1
  libdebconfclient0 libdevmapper1.02.1 libdiscover2 libdpkg-perl libdrm-amdgpu1
```

```
libdrm-common libdrm-intel1 libdrm-nouveau2 libdrm-radeon1 libdrm2 libdv4
libedit2 libefiboot1 libefivar1 libegl-dev libegl-mesa0 libegl1 libegl1-mesa-dev
libelf1 libenchant-2-2 libepoxy-dev libepoxy0 libevdev2 libexpat1 libexpat1-dev
libext2fs2 libffi-dev libffi7 libfftw3-single3 libflac8 libfontconfig1
libfontconfig1-dev libfontenc1 libfreetype-dev libfreetype6 libfreetype6-dev
libfribidi-dev libfribidi0 libfuse2 libgbm1 libgcc-s1 libgcr20 libgdbm-
compat4 libgdbm6 libgdk-pixbuf2.0-0 libgdk-pixbuf2.0-bin libgdk-pixbuf2.0-common
libgdk-pixbuf2.0-dev libgirepository-1.0-1 libgl-dev libgl1 libgl1-mesa-dev
libgl1-mesa-dri libglapi-mesa libgles-dev libgles1 libgles2 libglvnd0
libglvnd0-bin libglvnd0-data libglvnd0-dev libglvnd0-dev-bin libglvnd-dev
libglvnd0 libglx-dev libglx-mesa0 libglx0 libgmp10 libgnutls30 libgpg-error0
libgpm2 libgraphite2-3 libgraphite2-
```

```
1 dev libgssapi-krb5-2 libgstreamer-glib1.0-0 libgstreamer-plugins-base1.0-0
libgstreamer-plugins-good1.0-0 libgstreamer1.0-0 libgtk-3-0 libgtk-3-common
libgtk-3-dev libgudev-1.0-0 libharfbuzz-dev libharfbuzz-gobject0 libharfbuzz-
icu0 libharfbuzz0b libhogweed5 libhunspell1-1.7-0 libhyphen0 libice-dev libice6
libicu-dev libicu66 libidn2-0 libiec61883-0 libinput-bin libinput10 libip4tc2
libip6tc2 libisl22 libjack-jackd2-0 libjavascriptcoregtk-4.0-18
libjavascriptcoregtk-4.0-bin libjavascriptcoregtk-4.0-dev libjbig0 libjpeg-
turbo8 libjpeg8 libjson-c4 libjson-glib-1.0-0 libjson-glib-1.0-common
libk5crypto3 libkeyutils1 libklibc libkmod2 libkrb5-3 libkrb5support0 liblcms2-2
libl1vm12 liblmbd0 liblocale-gettext-perl libltdl7 liblz4-1 liblzma5 liblzo2-2
libmagic-mgc libmagic1 libmaxminddb0 libmnl0 libmount-dev libmount1 libmp3lame0
libmpc3 libmpdec2 libmpfr6 libmpeg123-0 libmtddev1 libncurses6 libncursesw6
libnetfilter-conntrack3 libnettle7 libnewt0.52 libnftnl1 libnftnl1 libnl
-3-200 libnl-genl-3-200 libogg0 libopengl-dev libopengl0 libopenjp2-7 libopus0
liborc-0.4-0 libp11-kit0 libpam-modules libpam-modules-bin libpam-runtime libpam-
systemd libpam0g libpango-1.0-0 libpango1.0-dev libpangocairo-1.0-0 libpangoft2
-1.0-0 libpangoxft-1.0-0 libparted2 libpci3 libpciaccess0 libpcre16-3 libpcre2
-16-0 libpcre2-32-0 libpcre2-8-0 libpcre2-dev libpcre2-posix2 libpcre3 libpcre3-
dev libpcre32-3 libpcrecpp0v5 libperl5.30 libpipeline1 libpixman-1-0 libpixman
-1-dev libplymouth5 libpng-dev libpng16-16 libpolkit-gobject-1-0 libpopt0
libproxy1v5 libpsl-dev libpsl5 libpthread-stubs0-dev libpython3-stdlib
libpython3.8 libpython3.8-minimal libpython3.8-stdlib libqrencode4 libraw1394-11
libreadline3 librest-0.7-0 librsvg2-2 librsvg2-common libsamplerate0
libseccomp2 libsecret-1-0 libsecret-common libselinux1 libselinux1-dev
libsemanage-common libsemanage1 libensors-config libensors5 libsepol1
libsepol1-dev libshout3 libslang2 libsm-dev libsm6 libsmartcols1 libsoup-gnome2
.4-1 libsoup2.4-1 libsoup2.4-dev libspice1 libsqlite3-0 libsqlite3-dev libss2
libssl1.1 libstartup-notification0 libstdc++6 libsystemd0 libtag1v5 libtag1v5-
vanilla libtalloc2 libtasn1-6 libtdb1 libtevent0 libtext-
```

```
1 iconv-perl libthai-data libthai-dev libthai0 libtheora0 libtiff5 libtinfo6
libtvolame0 libuchardet0 libudev1 libunistring2 libunwind8 libusb-0.1-4 libusb
-1.0-0 libuuid1 libuv1 libv4l-0 libv4lconvert0 libvisual-0.4-0 libvorbis0a
libvorbisenc2 libvorbisfile3 libvpx6 libvulkan1 libwacom-common libwacom2
libwavpack1 libwayland-bin libwayland-client0 libwayland-cursor0 libwayland-dev
libwayland-egl1 libwayland-server0 libwbclient0 libwebkit2gtk-4.0-37
libwebkit2gtk-4.0-37-gtk2 libwebkit2gtk-4.0-dev libwebkit2gtk-4.0-doc libwebp6
libwebpdemux2 libwnck-3-0 libwnck-3-common libwoff1 libx11-6 libx11-data libx11-
dev libx11-xcb1 libxatracker2 libxau-dev libxau6 libxaw7 libxcb-dri2-0 libxcb-
dri3-0 libxcb-glx0 libxcb-present0 libxcb-render0 libxcb-render0-dev libxcb-shm0
libxcb-shm0-dev libxcb-sync1 libxcb-util1 libxcb-xfixes0 libxcb1 libxcb1-dev
libxcbcomposite-dev libxcbcomposite1 libxcursor-dev libxcursor1 libxdamage-dev
libxdamage1 libxdmcp-dev libxdmcp6 libxext-dev libxext6 libxfce4ui-2-0
libxfce4ui-common libxfce4util-common libxfce4util7 libxfconf-0-3 libxfce4-dev
libxfce4ui3 libxfont2 libxft-dev libxft2 libxi-dev libxi6 libxinerama-dev
libxinerama1 libxkbcommon-dev libxkbcommon0 libxkbfile1 libxml2 libxml2-dev
libxmu6 libxmuu1 libxpm4 libxpresent1 libxrandr-dev libxrandr2 libxrender-dev
libxrender1 libxres1 libxshmfence1 libxslt1.1 libxss1 libxtable1 libxtables12
libxtst-dev libxtst6 libxvmc1 libxxf86vm1 libyaml-0-2 libzstd1 linux-base linux-
image-5.4.0-100-generic linux-modules-5.4.0-100-generic linux-modules-extra
```

```
-5.4.0-100-generic linux-sound-base locales login logrotate logsave lsb-base lsb-  
-release lshw lsof ltrace lupin-casper lz4 mawk mime-support mount ncurses-base  
ncurses -
```

```
1 bin openssl pango1.0-tools passwd pci.ids pciutils perl perl-base perl-modules-5.30  
pkg-config plymouth plymouth-label psmisc python3 python3-apport python3-blinker  
python3-cairo python3-certifi python3-cffi-backend python3-chardet python3-  
cryptography python3-dbus python3-distro python3-distutils python3-entrypoints  
python3-gi python3-gi-cairo python3-httplib2 python3-idna python3-jwt python3-  
keyring python3-launchpadlib python3-lazr.restfulclient python3-lazr.uri python3-  
lib2to3 python3-minimal python3-oauthlib python3-pkg-resources python3-problem-  
report python3-requests python3-requests-unixsocket python3-secretstorage  
python3-simplejson python3-six python3-urllib3 python3-wadllib python3-yaml  
python3.8 python3.8-minimal qrencode readline-common sed sensible-utils shared-  
mime-info sound-theme-freedesktop strace sudo systemd systemd-sysv systemd-  
timesyncd sysvinit-utils tar time tzdata ubuntu-standard ucf udev usb.ids  
usbutils user-setup util-linux uuid-dev uuid-runtime wayland-protocols x11-  
common x11-xkb-utils x11-xserver-utils x11proto-core-dev x11proto-dev x11proto-  
input-dev x11proto-randr-dev x11proto-record-dev x11proto-xext-dev x11proto-  
xinerama-dev xdg-dbus-proxy xfconf xfw4 xinput xkb-data xorg-sgml-doctools  
xserver-common xserver-xorg xserver-xorg-core xserver-xorg-input-all xserver-  
xorg-input-libinput xserver-xorg-video-intel xserver-xorg-video-vmware xtrans-  
dev xxd xz-utils zlib1g zlib1g-dev
```

Se llevaron a cabo los pasos necesarios para instalar las librerías requeridas con el objetivo de ejecutar la aplicación en el ambiente de pruebas. No obstante, no fue posible hacer que la aplicación funcione correctamente debido a diferencias en el hardware del entorno de pruebas en comparación con el hardware específico de una máquina de votación real.

El software de la máquina de votación realiza varias comprobaciones de hardware antes de iniciar el sistema operativo, lo que dificulta su ejecución en un entorno que no cuente con el hardware adecuado. Estas comprobaciones pueden incluir la verificación de componentes específicos, como lectores de tags, pantallas táctiles o módulos de seguridad, que pueden no estar presentes en el ambiente de pruebas.

3.3.2 Ejecución del sistema de elecciones en VM

Se realizó la modificación de la imagen del DVD que se utiliza como LiveDVD de arranque para las máquinas de votación para que permita realizar la instalación en VMware como máquina virtual.

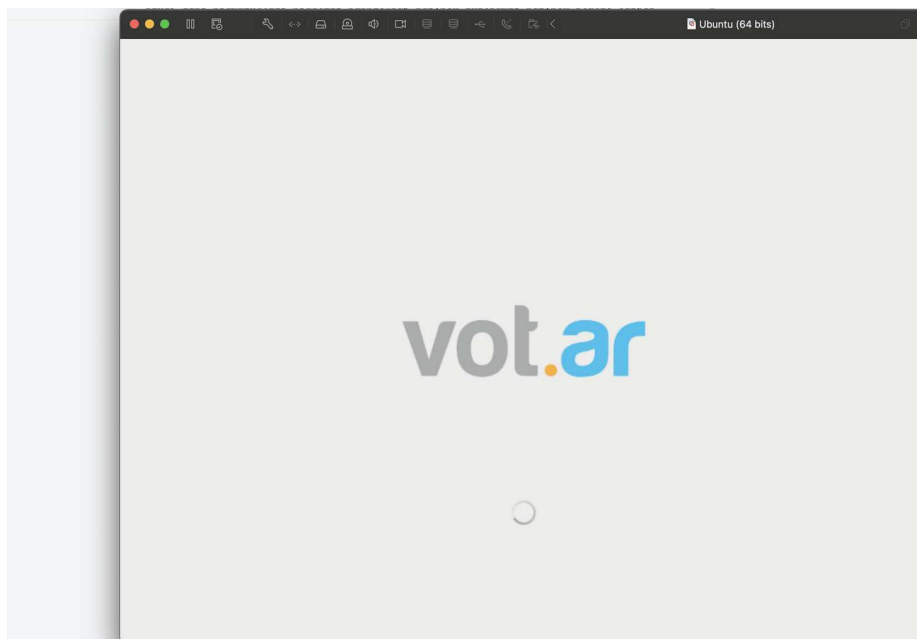


Figura 7: Sistema de votación iniciando en Máquina Virtual.

El liveDVD arranca con un conjunto de errores relacionados a la integridad del medio.

```
[ 24.515462] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 25.569636] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x80700 phys_seg 1 prio class 0
[ 25.613096] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 25.627584] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 25.650921] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 26.604134] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 27.724928] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x80700 phys_seg 1 prio class 0
[ 27.764911] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 27.776427] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 27.802156] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 28.848971] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x80700 phys_seg 1 prio class 0
[ 28.869069] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 28.904981] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 28.926774] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 29.976168] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 31.029425] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x80700 phys_seg 1 prio class 0
[ 31.073439] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 31.089912] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 31.115471] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 32.150347] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 33.205647] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x80700 phys_seg 1 prio class 0
[ 33.249077] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 33.264710] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 33.288069] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 34.323230] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 35.369084] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x80700 phys_seg 1 prio class 0
[ 35.409002] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 35.424907] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 35.450250] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 36.480689] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
mount: mounting /dev/sr0 on /cdrom failed: Input/output error
[ 37.537048] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x80700 phys_seg 1 prio class 0
[ 37.577667] blk_update_request: I/O error, dev sr0, sector 121075712 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 0
[ 37.594827] Buffer I/O error on dev sr0, logical block 30268928, async page read
[ 37.618986] FAT-fs (sr0): logical sector size too small for device (logical sector size = 512)
```

Figura 8: Errores al ejecutar el liveDVD modificado.

3.3.3 Escaneo de Vulnerabilidades

Se pudo identificar que el kernel que ejecuta el liveDVD es la versión 5.4.0-100 como se puede ver a continuación:

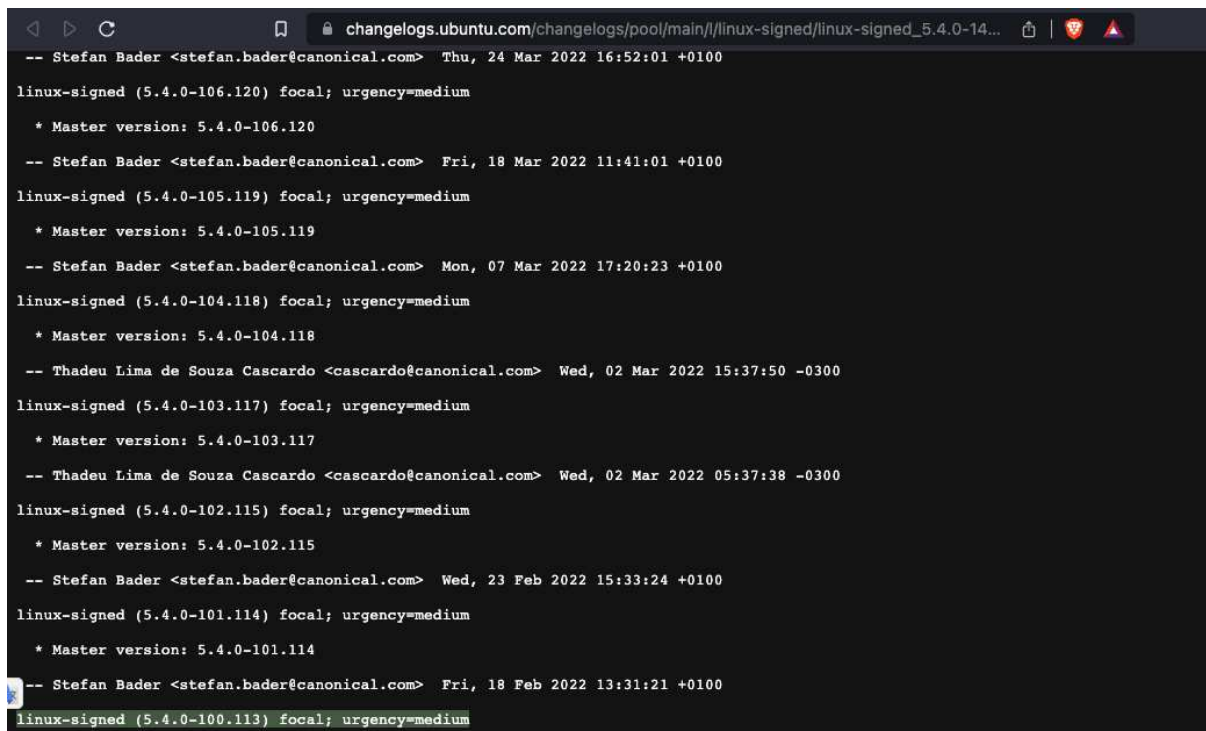
```
/Volumes/Vot-Ar/casper_floss (0.147s)
strings vmlinuz |grep 5.4
5.4.0-100-generic (buildd@lcy02-amd64-002) #113-Ubuntu SMP Thu Feb 3 18:43:29 UTC 2022
5'40K
TYd5@a
:2!5Y4
5$41
ZP5@a
05.4
```

Figura 9: Identificación de versión de Kernel.

Teniendo en cuenta que no se pudo obtener acceso a la línea de comandos del sistema operativo debido a las restricciones de seguridad impuestas por el software, se realizaron varios intentos para omitir estos controles. Sin embargo, después de no tener éxito en eludir estas restricciones, se decidió optar por un enfoque alternativo para evaluar la seguridad del sistema.

Se llevó a cabo una búsqueda manual de vulnerabilidades relacionadas con la versión del Kernel del sistema operativo utilizado en la máquina de votación. Este enfoque consistió en revisar las vulnerabilidades conocidas y documentadas que pudieran afectar al Kernel en cuestión.

Luego de realizar esta investigación, se pudo verificar, a través de la imagen proporcionada (no incluida en el texto), que la versión del Kernel que se ejecuta en la máquina de votación no presenta vulnerabilidades conocidas. Esto indica que, al menos en lo que respecta al Kernel del sistema operativo, la máquina de votación parece estar protegida contra ataques y explotaciones conocidas.



```
-- Stefan Bader <stefan.bader@canonical.com> Thu, 24 Mar 2022 16:52:01 +0100
linux-signed (5.4.0-106.120) focal; urgency=medium
  * Master version: 5.4.0-106.120
-- Stefan Bader <stefan.bader@canonical.com> Fri, 18 Mar 2022 11:41:01 +0100
linux-signed (5.4.0-105.119) focal; urgency=medium
  * Master version: 5.4.0-105.119
-- Stefan Bader <stefan.bader@canonical.com> Mon, 07 Mar 2022 17:20:23 +0100
linux-signed (5.4.0-104.118) focal; urgency=medium
  * Master version: 5.4.0-104.118
-- Thadeu Lima de Souza Cascardo <cascardo@canonical.com> Wed, 02 Mar 2022 15:37:50 -0300
linux-signed (5.4.0-103.117) focal; urgency=medium
  * Master version: 5.4.0-103.117
-- Thadeu Lima de Souza Cascardo <cascardo@canonical.com> Wed, 02 Mar 2022 05:37:38 -0300
linux-signed (5.4.0-102.115) focal; urgency=medium
  * Master version: 5.4.0-102.115
-- Stefan Bader <stefan.bader@canonical.com> Wed, 23 Feb 2022 15:33:24 +0100
linux-signed (5.4.0-101.114) focal; urgency=medium
  * Master version: 5.4.0-101.114
-- Stefan Bader <stefan.bader@canonical.com> Fri, 18 Feb 2022 13:31:21 +0100
linux-signed (5.4.0-100.113) focal; urgency=medium
```

Figura 10: Registro de cambios de la versión de Kernel.

Para la identificación de vulnerabilidades en los paquetes de software instalados en el Sistema Operativo que utiliza la máquina de votación se realizó el siguiente procedimiento:

1. En base al archivo filesystem.manifest se pudo obtener las versiones de todos los paquetes que se incluyen en el liveDVD el detalle de paquetes está en el punto 3.3.1.
2. Para realizar una búsqueda automatizada se usó el software BurpSuite, de tal manera de que en el sitio <https://www.cvedetails.com/> se inserte como valor de búsqueda cada uno de los paquetes que contine el liveDVD como se puede ver a continuación:

Request ^	Payload	Status	Error	Timeout	Length	Comment
2	adduser 3.118ubuntu2	200	☐	☐	10791	
3	alsa-base 1.0.25+dfsg-0ubu...	200	☐	☐	10791	
4	alsa-utils 1.2.2-1ubuntu2.1	200	☐	☐	10791	
5	base-files 11ubuntu5	200	☐	☐	10791	
6	base-passwd 3.5.47	200	☐	☐	10791	
7	bash 5.0-6ubuntu1	200	☐	☐	10791	
8	bind9-dnsutils 1:9.16.1-0ubu...	200	☐	☐	10791	
9	bind9-libs 1:9.16.1-0ubuntu2...	200	☐	☐	10791	
10	bsdmainutils 11.1.2ubuntu3	200	☐	☐	10791	
11	bsdutils 1:2.34-0.1ubuntu9	200	☐	☐	10791	
12	bubblewrap 0.4.0-1ubuntu4	200	☐	☐	10791	
13	busybox-initramfs 1:1.30.1-4...	200	☐	☐	10791	
14	busybox-static 1:1.30.1-4ub...	200	☐	☐	10791	
15	casper 1.445.3	200	☐	☐	10791	
16	coreutils 8.30-3ubuntu2	200	☐	☐	10791	

Request

Response

Pretty

Raw

Hex

Render

CVE Details

The ultimate security vulnerability datasource

[Log In](#)
[Register](#)
[Take a third party risk management course for FREE](#)

[Switch to https://](#)
[Home](#)

Browse :
[Vendors](#)
[Products](#)
[Vulnerabilities By Date](#)
[Vulnerabilities By Type](#)

Reports :
[CVSS Score Report](#)

No Results

Search for coreutils 8.30-3ubuntu2 on Google

Vulnerability Feeds & Widgets^{New}

ENHANCED BY Google

Figura 11: Consultas de vulnerabilidades en CVE Details.

3. El mismo ejercicio se realizó con el sitio vulmon.com

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	22443	
1	accountsservice 0.6.55-0ubu...	200	☐	☐	24161	
2	adduser 3.118ubuntu2	200	☐	☐	22336	
3	alsa-base 1.0.25+dfsg-0ubu...	200	☐	☐	22408	
4	alsa-utils 1.2.2-1ubuntu2.1	200	☐	☐	22385	
5	base-files 11ubuntu5	200	☐	☐	22336	
6	base-passwd 3.5.47	200	☐	☐	22322	
7	bash 5.0-6ubuntu1	200	☐	☐	22315	
8	bind9-dnswriter 1:9.16.1-0ubu...	200	☐	☐	22443	
9	bind9-libs 1:9.16.1-0ubuntu2...	200	☐	☐	22415	
10	bsdmainutils 11.1.2ubuntu3	200	☐	☐	22378	
11	bsdutils 1:2.34-0.1ubuntu9	200	☐	☐	22380	
12	bubblewrap 0.4.0-1ubuntu4	200	☐	☐	22371	
13	busybox-initramfs 1:1.30.1-4...	200	☐	☐	22457	

Request	Response
Pretty	Raw Hex Render

	Vulmon	Recent Vulnerabilities	Research Posts	Trends	Blog	About	Contact	Vulmon Alerts
--	---------------	------------------------	----------------	--------	------	-------	---------	---------------

☒ By Relevance
 ☐ By Risk Score
 ☐ By Publish Date
 ☐ By Recent Activity

bind9-dnswriter 1:9.16.1-0ubuntu2.12 vulnerabilities and exploits (subscribe to this query)

CVSSv3
RECOMMENDATIONS:
 CVE-2023-26822

Figura 12: Consultas de vulnerabilidades en Vulmon.

No se obtuvieron vulnerabilidades reportadas en los paquetes incluidos en el Sistema Operativo de la máquina de votación. Con este procedimiento se emuló lo que hace un software de análisis de vulnerabilidades, ya que este, identifica el software presente, las versiones y en su base de datos mapea las vulnerabilidades correspondientes al software en la versión identificada.

3.4 Pruebas de Hardware

Se realizaron varias pruebas de hardware, con una orientación al cumplimiento de los objetivos de la auditoría.

3.4.1 Evaluar una operación aislada de cualquier tipo de conectividad con el exterior durante el proceso de votación

- Identificación visual de puertos de conexión físicos que permitan transmisión de datos.



Figura 13: Puertos en la máquina P4.



Figura 14: Puertos en la máquina P5

En los dos equipos se identificó puertos USB y un puerto de red.

En el caso del equipo P4, se pudo comprobar que el puerto USB se encuentra energizado, se realizó una prueba para determinar si había la posibilidad de cerrar la aplicación y acceder a la línea de comandos usando fuerza bruta de combinación de teclas. No se obtuvo un resultado exitoso.

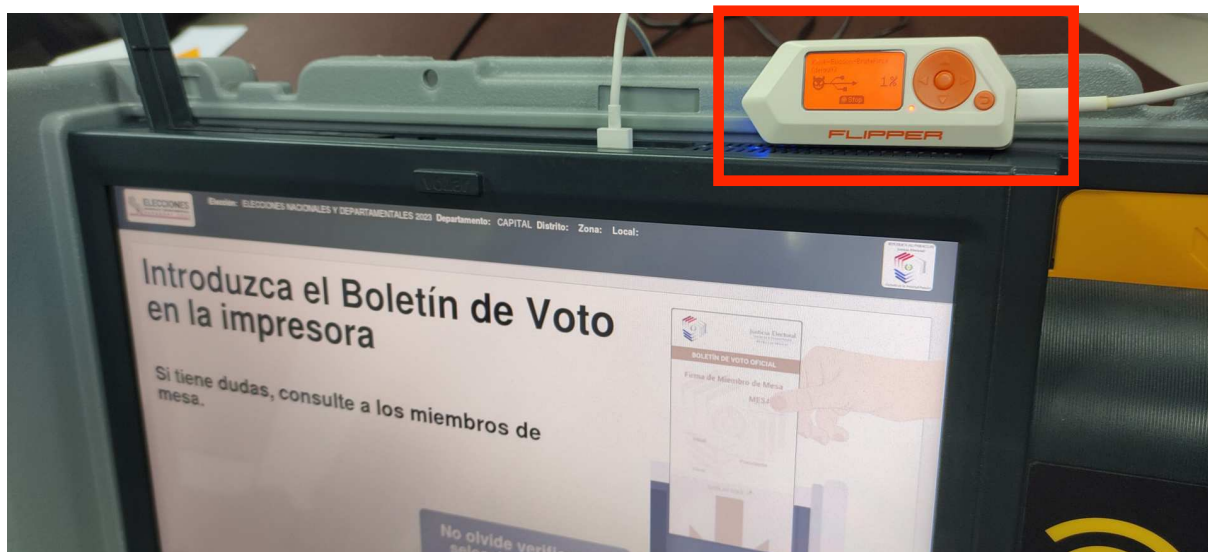


Figura 15: Prueba del puerto USB en equipo P4.

En el equipo P6 se pudo comprobar que el puerto USB está deshabilitado de manera física, el puerto no está energizado y el dispositivo de prueba no detecta conexión como se puede ver a continuación.

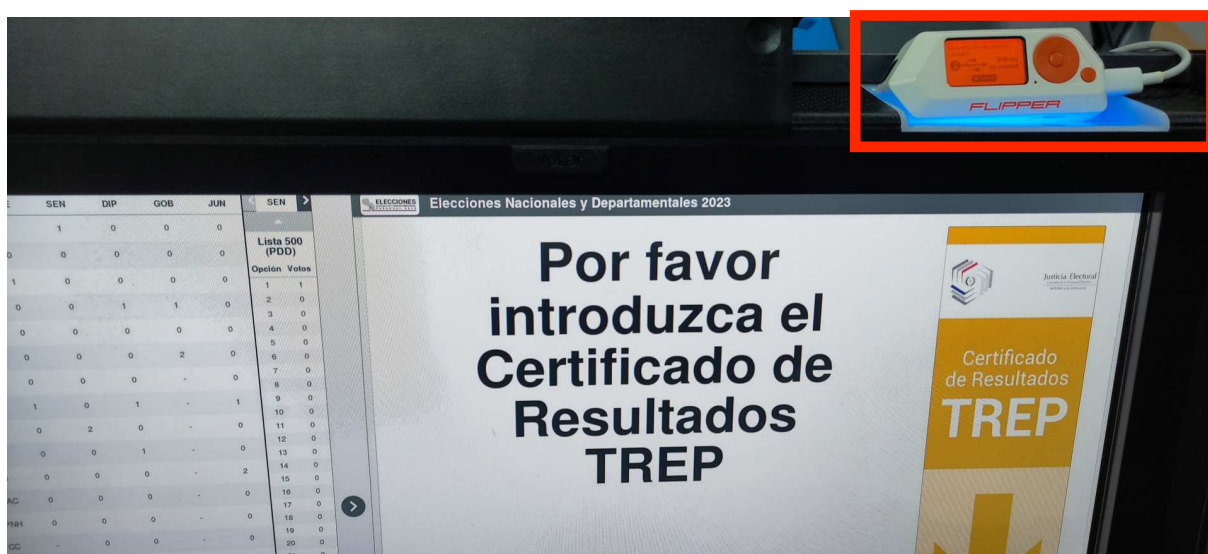


Figura 16: Prueba del puerto USB en equipo P6.

En ambos casos se realizó la ejecución de un ataque de fuerza bruta con un dispositivo badUSB, sin obtener ejecución de los payloads en ninguna de las máquinas evaluadas.

También se identificó el puerto de red en las dos máquinas evaluadas, para identificar posibles

conexiones a través de este puerto se utilizó un sniffer de red conectado a la máquina de votación.



Figura 17: Puerto de red P6.



Figura 18: Puerto de red P4

Se pudo evidenciar que en las máquinas P4 y P6 los puertos de red no se activan al conectar el cable de red. Se probó conectando un sniffer y conectando directamente a un puerto del switch.

No existe otro tipo de puerto en la máquina de votación que permita algún tipo de conexión o transferencia de datos.

3.4.2 Evaluar la garantía de voto secreto, sin almacenar información relacionada con el voto de cada elector

En las pruebas realizadas, se pudo hacer un análisis visual de las placas principales de los dos equipos, no se identificaron dispositivos de almacenamiento persistente.

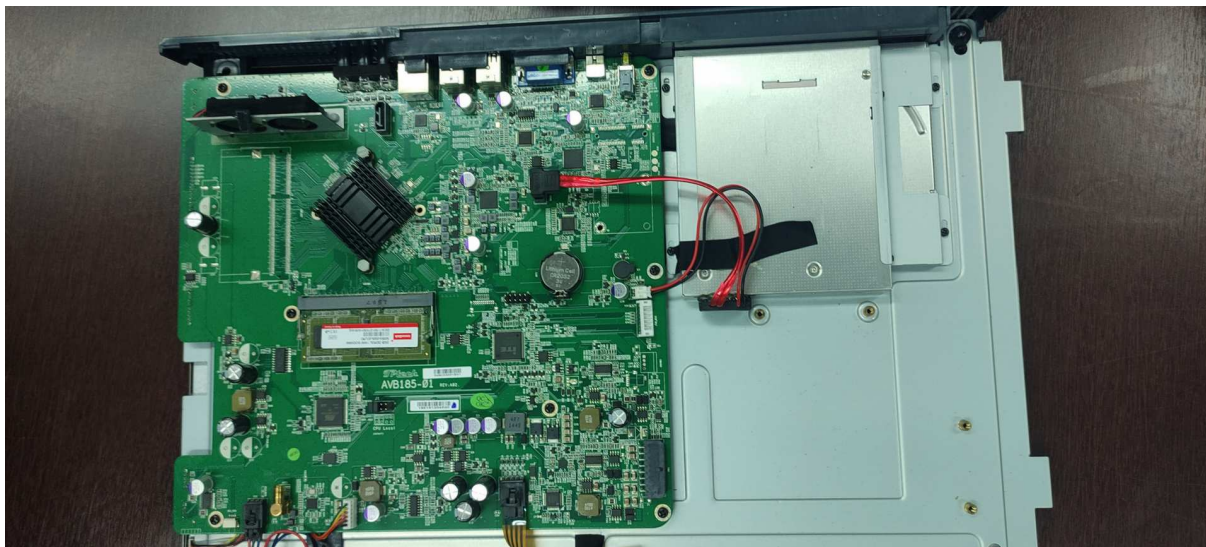


Figura 19: Placa principal de P4.

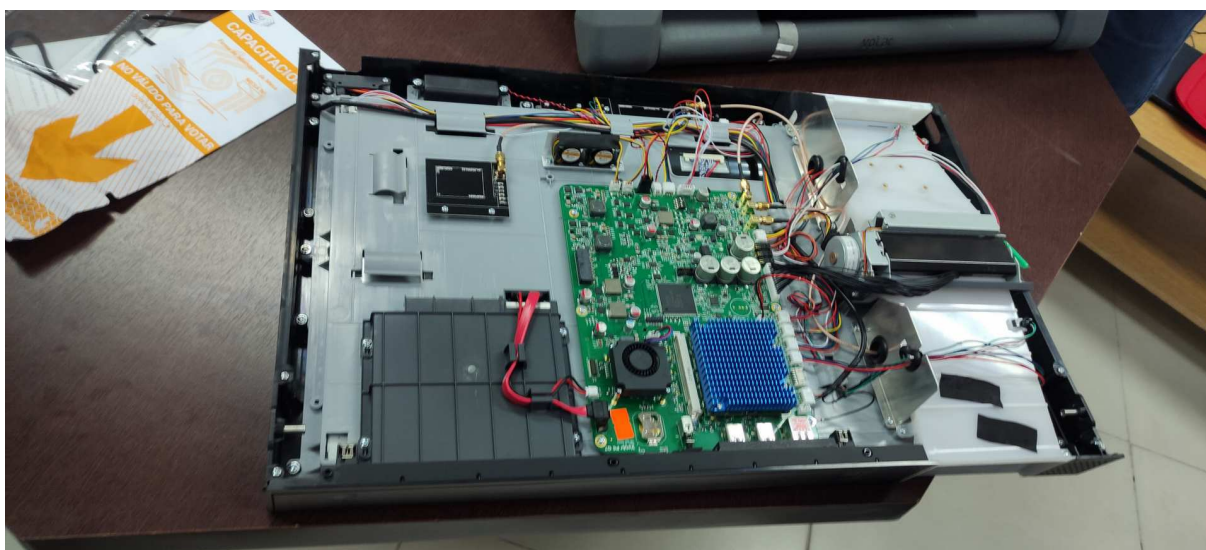


Figura 20: Placa principal de P6.

3.4.3 Evaluar la garantía de integridad (no alteración) de la información de votos registrados electrónicamente durante todo el proceso electoral

- Capturar contenido de TAG DATA de las boletas, verificar si es posible replicar.

Fue posible leer las boletas con un dispositivo de lectura RFID, y posteriormente se pudo replicar sin embargo solo el equipo P4 leyó el contenido replicado a través del dispositivo.

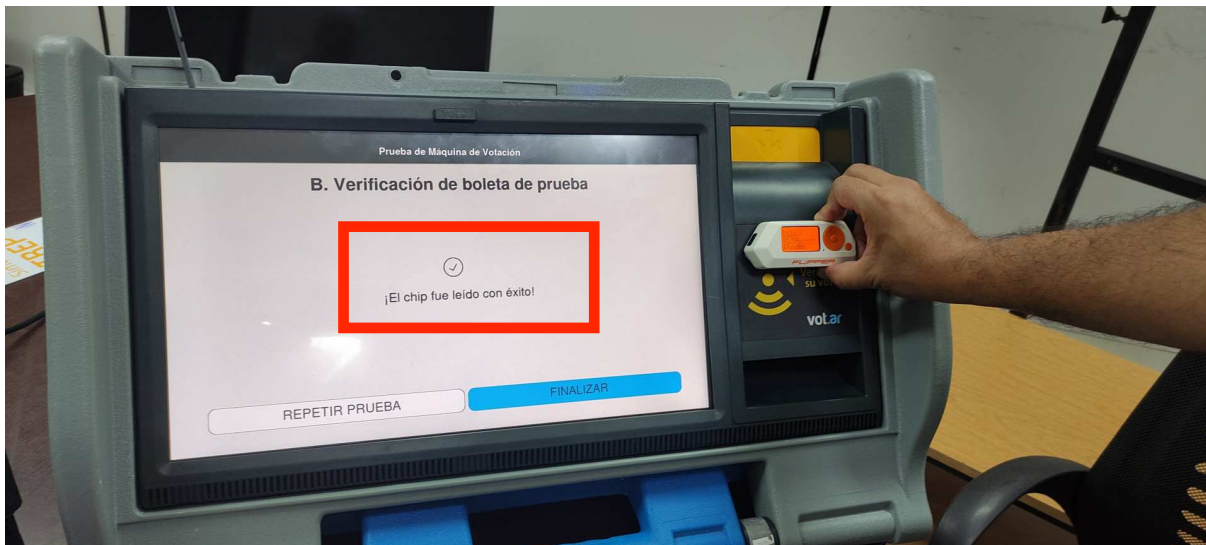


Figura 21: Lectura de información replicada en P4.

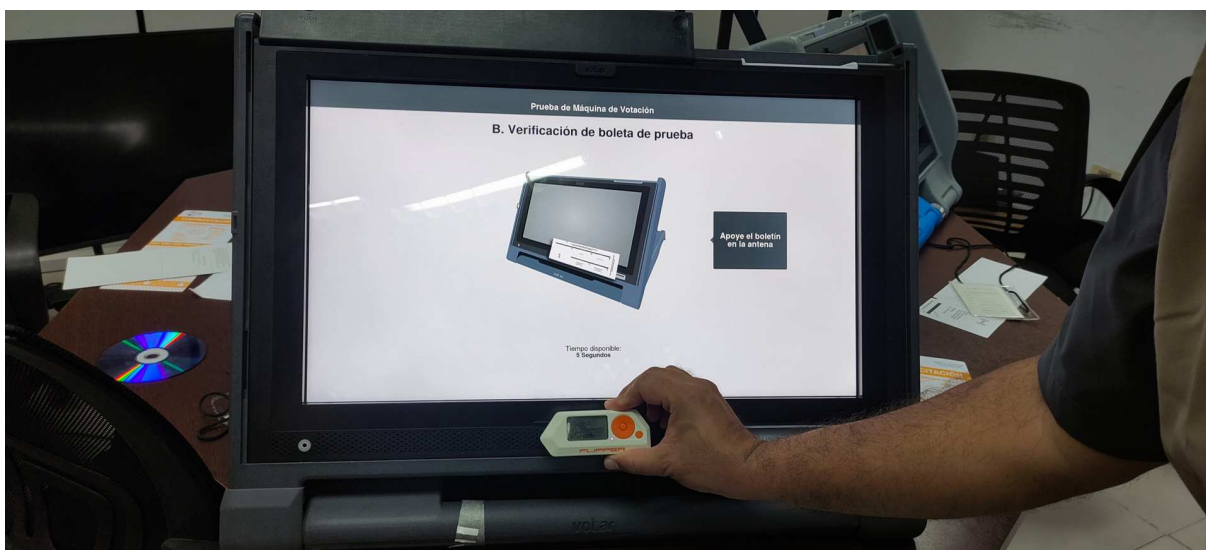


Figura 22: Lectura de información replicada en P6.

De la misma manera que se replicó los datos de las boletas, se modificó el contenido de la data del tag de la boleta por contenido aleatorio, no se obtuvo ninguna respuesta por parte de las máquinas al momento de acercar al lector el equipo de replicación.

Se intentó modificar el contenido de las boletas electorales sin éxito, lo que demuestra la efectividad de las medidas de seguridad implementadas en el sistema de votación. Esta protección se debe a tres factores clave:

- El contenido de las boletas se almacena de manera cifrada utilizando el algoritmo AES, lo que dificulta el acceso no autorizado a la información.
- La llave de cifrado es única para cada mesa electoral, y el Vector de Inicialización (IV) es único para cada boleta, lo que incrementa la seguridad y evita la reutilización de llaves y vectores.
- Una vez que se escribe en las boletas, estas se ponen en modo de solo lectura, lo que impide la modificación posterior del contenido almacenado.

Estos tres factores en conjunto generan un alto nivel de dificultad para alterar los resultados electorales. Además, para llevar a cabo una modificación masiva que afecte el resultado de la elección, la dificultad se eleva aún más, ya que sería necesario sortear estos tres factores clave en cada una de las mesas electorales.

3.4.4 Verificar boot desde DVD de arranque de Windows / Linux.

Se pudo verificar que ninguna de las máquinas tiene como opción configurada en primera prioridad de arranque las unidades usb, para la prueba se insertó una unidad usb y se reinició la máquina sin el DVD de arranque del sistema de votación, las máquinas se quedaron esperando una unidad de arranque válida.

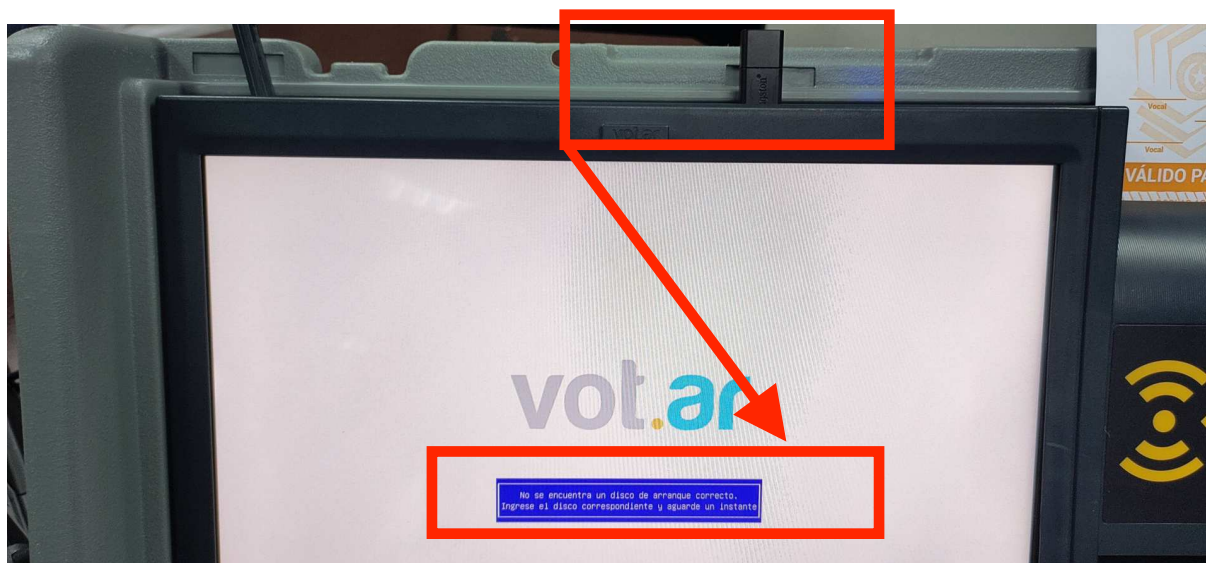


Figura 23: Arranque desde USB.

La segunda prueba fue, con un DVD de arranque de una versión de Linux Debian, la máquina detectó que no es un disco autorizado y no arrancó.

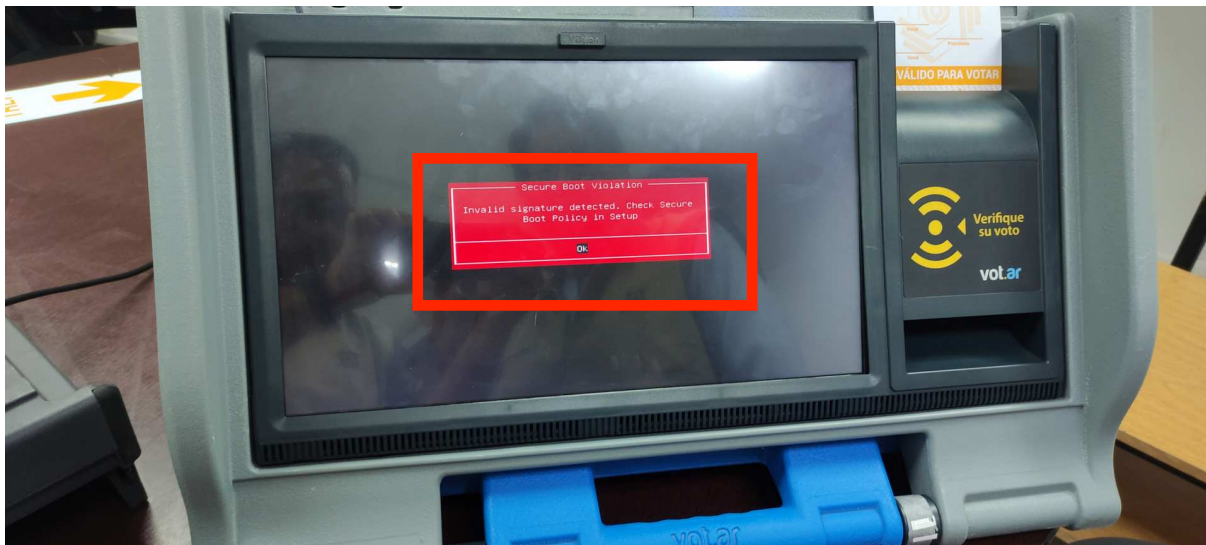


Figura 24: Arranque desde disco no autorizado en P4.

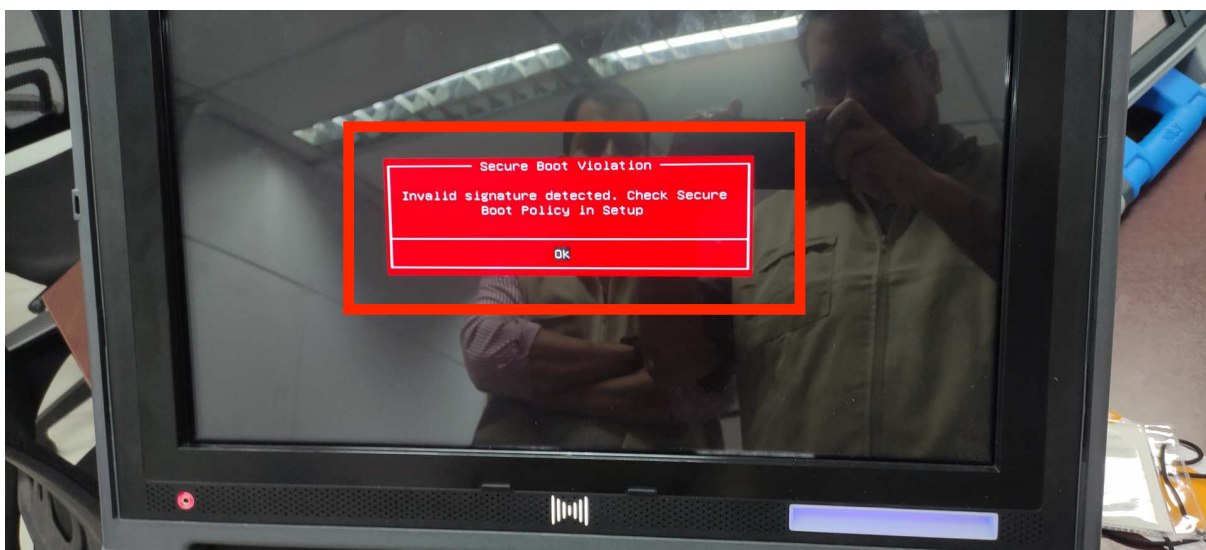


Figura 25: Arranque desde disco no autorizado en P6.

3.5 Análisis de RFID

Como parte del ejercicio se realizó un análisis de la data que se lee de las papeletas en distintas etapas del proceso:

Datos de Tag RFID antes de votación:

```
1 Filetype: Flipper NFC device
```

```

2  Version: 3
3  # Nfc device type can be UID, Mifare Ultralight, Mifare Classic or ISO15693
4  Device type: ISO15693
5  # UID is common for all formats
6  UID: E0 04 01 50 AD 66 A3 AC
7  # Data Storage Format Identifier
8  DSFID: 00
9  # Application Family Identifier
10 AFI: 00
11 IC Reference: 01
12 # Number of memory blocks, usually 0 to 256
13 Block Count: 28
14 # Size of a single memory block, usually 4
15 Block Size: 04
16 Data Content: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00
17 # Subtype of this card (0 = ISO15693, 1 = SLIX, 2 = SLIX-S, 3 = SLIX-L, 4 = SLIX2)
18 Subtype: 01
19 # SLIX specific data
20 PasswordEAS: 00 00 00 00

```

Datos de Tag RFID después de votación:

```

1 Filetype: Flipper NFC device
2 Version: 3
3 # Nfc device type can be UID, Mifare Ultralight, Mifare Classic or ISO15693
4 Device type: ISO15693
5 # UID is common for all formats
6 UID: E0 04 01 50 AD 66 9B BC
7 # Data Storage Format Identifier
8 DSFID: 00
9 # Application Family Identifier
10 AFI: 00
11 IC Reference: 01
12 # Number of memory blocks, usually 0 to 256
13 Block Count: 28
14 # Size of a single memory block, usually 4
15 Block Size: 04
16 Data Content: 1C 01 00 25 1D D0 D8 4D CC 70 3C 57 1F 64 C3 B9 19 3F 51 DD 36 CC D0 2
    F 14 E5 DA 98 33 96 36 B4 3F DA D6 CD 20 D7 E0 B0 47 22 BC 02 94 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
17 # Subtype of this card (0 = ISO15693, 1 = SLIX, 2 = SLIX-S, 3 = SLIX-L, 4 = SLIX2)
18 Subtype: 01
19 # SLIX specific data
20 PasswordEAS: 00 00 00 00

```

Datos de un Acta:

```
1 Filetype: Flipper NFC device
2 Version: 3
3 # Nfc device type can be UID, Mifare Ultralight, Mifare Classic or ISO15693
4 Device type: ISO15693
5 # UID is common for all formats
6 UID: E0 02 08 03 C6 CA 19 8D
7 # Data Storage Format Identifier
8 DSFID: 00
9 # Application Family Identifier
10 AFI: 00
```

```
11 IC Reference: 08
12 # Number of memory blocks, usually 0 to 256
13 Block Count: 80
14 # Size of a single memory block, usually 4
15 Block Size: 04
16 Data Content: 1C 04 00 20 99 C1 72 60 00 00 00 00 5B 52 72 E3 03 78 9C D3 3A D0 D8
    C0 80 00 2C 48 6C 06 26 38 2B 56 05 00 4A F8 02 73 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00
17 # Subtype of this card (0 = ISO15693, 1 = SLIX, 2 = SLIX-S, 3 = SLIX-L, 4 = SLIX2)
18 Subtype: 00
19 # End of ISO15693 parameters
```

Esta información describe las especificaciones técnicas y características de un dispositivo NFC compatible con el estándar ISO 15693, que tiene 28 bloques de memoria, cada uno con un tamaño de 4 bytes y que contiene una serie de datos específicos almacenados en él.

El detalle a continuación:

Device type: ISO15693: se refiere al tipo de dispositivo NFC que es compatible con el estándar ISO 15693. Este estándar define las características y especificaciones técnicas de los sistemas de identificación por radiofrecuencia (RFID) de alta frecuencia que operan en la banda de frecuencia de 13,56 MHz.

UID: es el Identificador Único del Dispositivo, que es un número único de 8 bytes que identifica de manera exclusiva al dispositivo NFC.

DSFID: es el Identificador de Formato de Almacenamiento de Datos, que es un número de 1 byte que identifica el formato de almacenamiento de datos en el dispositivo NFC.

AFI: es el Identificador de Familia de Aplicación, que es un número de 1 byte que identifica la familia de aplicaciones a la que pertenece el dispositivo NFC.

IC Reference: es una referencia del circuito integrado que se utiliza en el dispositivo.

Block Count: es el número de bloques de memoria disponibles en el dispositivo NFC.

Block Size: es el tamaño de cada bloque de memoria en bytes.

Data Content: es el contenido de los datos almacenados en el dispositivo NFC.

Subtype: se refiere al subtipo de la tarjeta, que en este caso es 01 y significa que es una tarjeta SLIX.

Password EAS: se refiere a la contraseña de seguridad del dispositivo NFC para el Sistema de Antenas Electrónicas (EAS).

3.5.2 Cifrado de contenido de boleta

Para determinar si los datos que se almacenan en las boletas están cifrados se analizó el código

Cifrado del voto:

```
def encriptar_voto(aes_key, serial_number, data):
    """Funcion de alto nivel para encriptar un voto.

    Argumentos:
    aes_key -- un stream de 16 bytes con la clave de encriptación.
    serial_number -- un stream de 8 bytes con el serial_number del tag.
    data -- el stream de bytes que queremos encriptar.
    """
    ret = data
    # si no queremos encriptar el voto devolvemos los datos que nos mandaron
    if ENCRYPTAR_VOTO:
        # El vector tiene que tener 12 bytes así que le agregamos 4 bytes como
        # padding
        init_vector = serial_number + PADDING_SERIAL
        gcm_tag, data_encryptada = encriptar(aes_key, init_vector, data)
        # armamos un container de construct para armar el voto con el formato
        # correcto
        contenedor = Container(gcm_tag=gcm_tag, len_datos=len(data_encryptada),
                               datos=data_encryptada)
        ret = struct_voto.build(contenedor)
    return ret
```

Figura 26: Cifrado de voto.

El algoritmo que se usa es AES:

IV es el ID de tag + Padding

Padding es PADDING_SERIAL: [b"\x00\x00\x00\x00"]

Para obtener la llave AES se utiliza esta función:

```
msa > core > crypto > __init__.py > desencriptar_credencial
123
124
125 def desencriptar_credencial(mesa, pin, credencial):
126     # generamos el vector de inicializacion
127     init_vector = unhexlify(credencial.serial) + PADDING_SERIAL
128     # parseamos la credencial con construct
129     datos = struct_credencial.parse(credencial.datos)
130     # derivamos la clave
131     clave = derivar_clave(pin, datos.salt)
132     # devolvemos la key de la mesa
133     key = desencriptar(clave, init_vector, datos.gcm_tag, datos.datos, mesa)
134     return key
```

Figura 27: Obtención AES Key.

La función `desencriptar_credencial` toma tres argumentos: mesa, pin y credencial. La función devuelve la key de la mesa, que se desencripta a partir de la credencial, utilizando un pin y otros datos.

El proceso de desencriptación comienza generando un `init_vector`, que es una combinación del número de serie de la credencial y un relleno (`PADDING_SERIAL`). Luego se parsea la credencial utilizando la biblioteca `construct`. La biblioteca `construct` es una herramienta de Python para definir y analizar estructuras de datos binarios.

Se deriva una clave a partir del pin y los datos de salt. Luego se utiliza esta clave para desencriptar la key de la mesa. El `init_vector`, el `gcm_tag` y los datos de datos también se utilizan en el proceso de desencriptación.

Finalmente, se devuelve la key de la mesa, esta key es utilizada para cifrar el voto, y corresponde a cada mesa, no se utiliza una sola key para todas las mesas.

Además en el punto anterior se pueden ver contenidos de ejemplo de una boleta, en ellos se identifica un contenido en hexadecimal, que haciendo una decodificación no muestra caracteres imprimibles. Prueba de que el contenido está cifrado.

3.5.3 Distancia de Lectura

Con un dispositivo especializado para lectura de etiquetas RFID se realizó varias pruebas, en las que se puede ver que, el dispositivo debe estar a una distancia de 4 cm aproximadamente para poder leer el contenido de una boleta.

Cabe destacar que no se realizaron pruebas con antenas de gran tamaño, amplificadores de señal u otro equipo similar, ya que se considera que la probabilidad de que alguien instale este tipo de equipos en los lugares de votación sin ser detectado por el personal de la entidad electoral o la fuerza pública es muy baja.

Por otro lado, se constató que, incluso si se lee el contenido de las boletas a distancia, el contenido de estas se encuentra cifrado mediante el algoritmo AES. En consecuencia, aún en el caso improbable de que se pudiera acceder a la información de las boletas mediante equipos no autorizados, el contenido seguiría estando protegido por este cifrado.

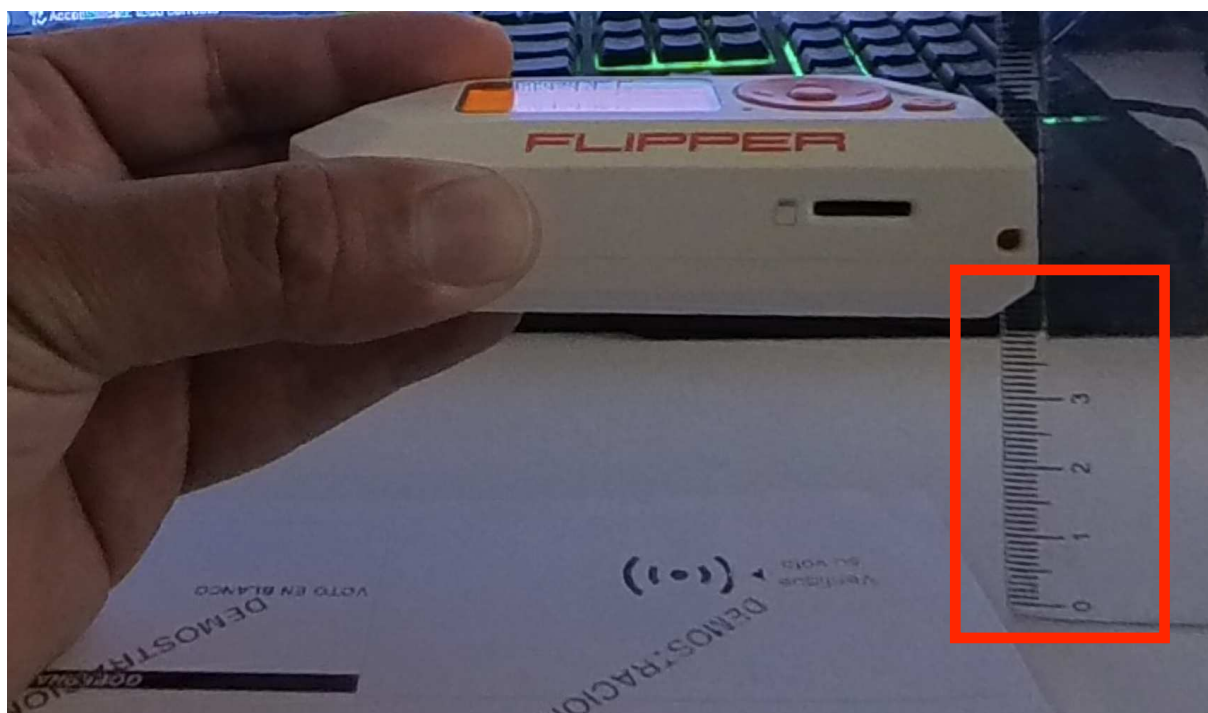


Figura 28: Vista Lateral



Figura 29: Vista Arriba

4. Remediación

Se recomienda agregar la línea `autoescape=True` como se muestra a continuación:

```
1 def init_jinja():
2     jinja_cache = FileSystemBytecodeCache()
3     jinja_env = Environment(
4         autoescape=True, loader=FileSystemLoader([PATH_TEMPLATES_VARS]),
5         bytecode_cache=jinja_cache,
6         autoescape=True,
7     )
8     return jinja_env
```

5. Conclusiones

- Durante el análisis realizado, se han podido identificar que las máquinas de votación realizan un conjunto de validaciones en el proceso de arranque que garantizan que solo se pueda iniciar la máquina con un medio de arranque autorizado. Esto asegura que cualquier intento de iniciar la máquina con un medio no autorizado, como una unidad de DVD, CD, USB o un disco duro externo, sea bloqueado. Además, se ha llevado a cabo varias pruebas en el DVD que contiene el sistema de votación, las cuales han permitido comprobar que este realiza validaciones en el proceso de arranque para garantizar que solo se permita iniciar en las máquinas de votación utilizadas para el proceso. El proceso de modificación de la imagen del DVD para hacer que su ejecución pueda realizarse en un computador de propósito general es de elevada complejidad y requeriría la inclusión de equipamiento que emule la funcionalidad de la máquina de votación.
- La máquina de votación utiliza una versión reducida de Ubuntu 20.04, en la cual se realizaron pruebas para identificar configuraciones o paquetes vulnerables. Los resultados demostraron que el sistema operativo se encuentra debidamente asegurado, ya que no se identificaron potenciales brechas de seguridad. No obstante, es importante mencionar que, debido a las restricciones de acceso a la shell impuestas por el aseguramiento del sistema operativo, no fue posible obtener detalles adicionales sobre el bastionado del sistema. Cabe destacar que las restricciones de acceso a la línea de comando, es una medida de seguridad implementada en el sistema operativo, la cual no se pudo omitir durante las pruebas realizadas.
- Durante las pruebas realizadas se comprobó que para leer la información de las boletas, se requiere que el lector esté a una distancia de 4 cm. Además, se utilizó un dispositivo de propósito específico para llevar a cabo auditorías que involucren tecnologías como RFID. Cabe destacar que no se realizaron pruebas con antenas de gran tamaño, amplificadores de señal u otro equipo similar, ya que se considera que la probabilidad de que alguien

instale este tipo de equipos en los lugares de votación sin ser detectado por el personal de la entidad electoral o la fuerza pública es muy baja. Por otro lado, se constató que, incluso si se lee el contenido de las boletas a distancia, el contenido de estas se encuentra cifrado mediante el algoritmo AES. En consecuencia, aún en el caso improbable de que se pudiera acceder a la información de las boletas mediante equipos no autorizados, el contenido seguiría estando protegido por este cifrado.

- Durante las pruebas realizadas, se intentó modificar el contenido de las boletas sin éxito. Esto se debe a tres factores clave: en primer lugar, el contenido de las boletas se almacena de manera cifrada utilizando el algoritmo AES. En segundo lugar, la llave de cifrado es única para cada mesa y el Vector de Inicialización (IV) es único para cada boleta. En tercer lugar, una vez que se escribe en las boletas, estas se ponen en modo de solo lectura, estos tres factores juntos generan una gran dificultad para llevar a cabo la alteración de los resultados. Es importante destacar que para lograr una modificación masiva que afecte el resultado de la elección, la dificultad se eleva aún más, porque habría que omitir los tres factores clave mencionados previamente, en cada una de las mesas. En consecuencia, se considera que el sistema cuenta con niveles de seguridad adecuados para garantizar la integridad de los resultados electorales.
- En las pruebas realizadas se ha podido comprobar que las máquinas de votación utilizadas no dependen de las mesas de votación, lo que significa que estas no almacenan información relacionada con la elección que las vincule a una ubicación específica. Esto permite que cualquier máquina de votación pueda ser inicializada para reemplazar a otra que esté defectuosa o dañada, lo que aumenta significativamente la disponibilidad del sistema, ya que no se limita a un solo reemplazo. Además, se ha identificado que las máquinas de votación cuentan con dos baterías y un conector eléctrico, lo que asegura un respaldo eléctrico que contribuye a la alta disponibilidad del sistema de votación. Esta característica garantiza que el sistema esté siempre funcionando, incluso en caso de una interrupción inesperada del suministro eléctrico. Por lo tanto, la combinación de la posibilidad de múltiples reemplazos de máquinas de votación y el respaldo eléctrico asegurado por las baterías y el conector eléctrico, hacen que el sistema de votación sea altamente disponible y pueda funcionar de manera continua durante toda la jornada electoral.
- Durante el análisis de vulnerabilidades del código de la aplicación, se utilizaron más de 200 reglas que permiten identificar omisiones a las buenas prácticas de desarrollo seguro, con el objetivo de prevenir posibles vulnerabilidades en la aplicación. Los resultados demostraron que solo se identificó una vulnerabilidad, la cual no representa un riesgo significativo para el sistema debido a la naturaleza de este y las interfaces de acceso limitadas para la operación de la máquina de votación por parte del votante. El análisis de vulnerabilidades realizado incluyó una revisión exhaustiva de los paquetes de software y librerías que forman parte del

sistema operativo, específicamente se examinaron 610 paquetes y en las versiones instaladas no se encontraron vulnerabilidades reportadas hasta el momento de la realización del ejercicio.

- Se realizaron pruebas de intrusión sobre el software y el hardware de la máquina de votación, para el caso del hardware las pruebas se concentraron en hacer que la máquina interactúe con hardware externo no autorizado, obtener control de la máquina de votación a través de puertos de red, o un método de interacción distinto a los provistos por el mismo sistema, como por ejemplo una línea de comandos, terminal físico o similares. No fue posible obtener un acceso distinto al provisto por la interface de votación. Para las pruebas del software, se entregó al equipo consultor acceso al código fuente de toda la aplicación, se pudo comprobar que este no guarda datos sensibles o información que permita obtener algún tipo de acceso no autorizado a la máquina de votación, además de que se pudo analizar los procedimientos de cifrado que por el proceso de votación y las consideraciones de la implementación de este, mantiene una elevada postura de seguridad.
- Se llevó a cabo una evaluación exhaustiva del código de la aplicación utilizando tanto métodos automatizados como manuales, y no se encontraron vulnerabilidades relacionadas con malas prácticas de desarrollo, uso de funciones inseguras o similares.
- Las pruebas de caja gris fueron realizadas en la máquina de votación electrónica, tanto en el software como en el hardware, con el fin de identificar posibles vulnerabilidades y debilidades del sistema. Se llevaron a cabo pruebas de intrusión, análisis de vulnerabilidades, evaluación de controles y niveles de aseguramiento del sistema operativo y análisis del código de la aplicación en modalidad automatizada y manual. A partir de estos análisis se pudo comprobar que el sistema presenta un alto nivel de seguridad y que se ha seguido buenas prácticas de desarrollo seguro. Se identificó una sola vulnerabilidad en la aplicación, la cual no representa un riesgo significativo para la integridad del sistema.

Después de las pruebas realizadas se puede concluir que el sistema de votación electrónica usado en la fase de sufragio, por el Tribunal Superior de Justicia Electoral de la República de Paraguay, cuenta con una elevada postura de seguridad, se recomienda agregar al alcance de un próximo ejercicio la fase de generación de credenciales, considerando que estos documentos permiten obtener la llave de cifrado de los datos que se almacenan en las boletas, así como también la inicialización de una máquina de votación.

Elaborado por:

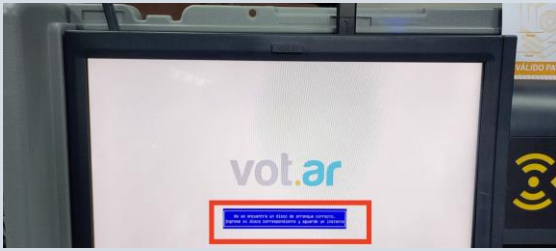
Ing. Jorge Moya

Consultor Ciberseguridad

CAPEL

FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD

Nombre o Tipo de Prueba Realizada:
Prueba de arranque seguro

Objetivo de la Prueba	Descripción de la Prueba:
Evaluar los controles para arranque seguro de las máquinas de votación.	La prueba inicia probando el inicio de un equipo de votación con un dispositivo usb no autorizado distinto al liveDVD usado por la máquina para el arranque.
	
	La siguiente prueba fue realizada con un DVD de arranque del sistema operativo debian. El resultado fue, un mensaje de advertencia de que la firma del disco es incorrecta.
	
	Otra prueba fue alterar el contenido del liveDVD que usa la máquina de votación y validar si arranca.

**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**

FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD

[illegible]**Firma y sello**

Cargo

Nombre Empresa

Lugar y fecha

FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD

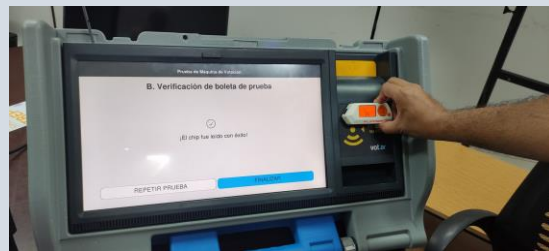
Nombre o Tipo de Prueba Realizada:
Prueba de garantía de integridad

Objetivo de la Prueba

Evaluar la garantía de integridad (no alteración) de la información de votos registrados electrónicamente durante todo el proceso electoral

Descripción de la Prueba:

La prueba inicia leyendo las boletas con un dispositivo de lectura RFID, y posteriormente replicando esta lectura a las máquinas de votación.



De la misma manera que se replicó los datos de las boletas, se modificó el contenido de la data del tag de la boleta por contenido aleatorio, no se obtuvo ninguna respuesta por parte de las máquinas al momento de acercar al lector el equipo de replicación.

Se pudo identificar en el código las funciones donde se puede comprobar el cifrado del contenido de la boleta.



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD

	<pre>def encryptar_votales_key, serial_number, datos: """Funcion de alto nivel para encriptar un voto. Argumentos: serial_number -- un stream de 16 bytes con la clave de encriptación. serial_number -- un stream de 8 bytes con el serial_number del tag. datos -- el stream de bytes que queremos encriptar. ret = datos # si no queremos encriptar el voto devolvemos los datos que nos mandaron if not datos: return datos # el vector clave que tiene 12 bytes así que le agregamos 4 bytes como # padding key_vector = serial_number + b'\x00\x00\x00\x00' gcm_tag, data_encryptada = encrypt(serial_number, key_vector, datos) # creamos un container de construct para armar el voto con el tiempo # correcto container = Container(gcm_tag=gcm_tag, ver_datos=len(data_encryptada), data=data_encryptada) ret = struct_voto.build(container) return ret</pre>
Resultados de la prueba: Mediante esta prueba se comprobó que la data que se almacena en las boletas se registra de manera cifrada, la llave de cifrado se extrae de las credenciales y es única para cada mesa. La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.	

Firma y sello

Cargo

Nombre Empresa



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**

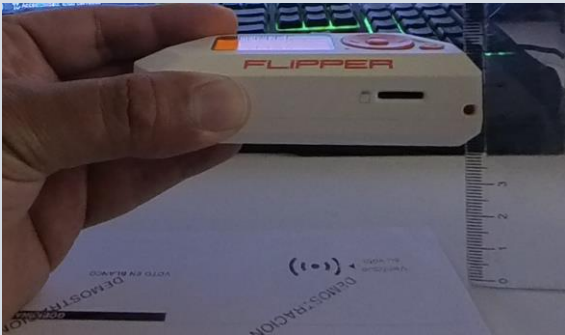


FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD

Lugar y fecha

FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD

Nombre o Tipo de Prueba Realizada:
Prueba de lectura a distancia

Objetivo de la Prueba	Descripción de la Prueba:
Evaluar el registro electrónico utilizado no admita lectura a distancia.	Para la prueba se utilizó un dispositivo específico de análisis y auditoría de tecnologías RFID. El equipo utilizado, si pudo leer las boletas a una muy corta distancia.  Se hicieron varias lecturas y se pudo identificar que a una distancia aproximada de 4 cm. Es posible leer la boleta.  Sin embargo ampliando el rango a una distancia superior a 4 cm, la lectura no es posible.

FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD

	En esta fotografía se puede ver que aún cuando la boleta está bajo el dispositivo de lectura, este no puede leer el contenido de la boleta, la distancia aproximada es de 8 cm. 
--	---

Resultados de la prueba:

Mediante esta prueba se comprobó que no es posible realizar a través de dispositivos portátiles una lectura a distancia de las boletas. Cabe destacar que no se realizaron pruebas con antenas de gran tamaño, amplificadores de señal u otro equipo similar, ya que se considera que la probabilidad de que alguien instale este tipo de equipos en los lugares de votación sin ser detectado por el personal de la entidad electoral o la fuerza pública es muy baja.

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.

Firma y sello

Cargo

Nombre Empresa

Lugar y fecha

FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD

Nombre o Tipo de Prueba Realizada:
Prueba de operación aislada

Objetivo de la Prueba	Descripción de la Prueba:
Evaluar una operación aislada de cualquier tipo de conectividad con el exterior durante el proceso de votación.	La prueba inicia con una identificación visual de puertos de conexión físicos que permitan transmisión de datos.   En los dos equipos se identificó puertos USB y un puerto de red. En el caso del equipo P4, se pudo comprobar que el puerto USB se encuentra energizado, se realizó una prueba para determinar si había la posibilidad de cerrar la aplicación y acceder a la línea de comandos usando fuerza bruta de combinación de teclas. No se obtuvo el acceso no autorizado.

FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD



En el equipo P6 se pudo comprobar que el puerto USB está deshabilitado de manera física, el puerto no está energizado y el dispositivo de prueba no detecta conexión como se puede ver a continuación.



En ambos casos se realizó la ejecución de un ataque de fuerza bruta con un dispositivo badUSB, sin obtener ejecución de los payloads en ninguna de las máquinas evaluadas.

También se identificó el puerto de red en las dos máquinas evaluadas, para identificar posibles conexiones a través de este puerto se utilizó un sniffer de red conectado a la máquina de votación.



FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD

	 Se pudo evidenciar que en las máquinas P4 y P6 los puertos de red no se activan al conectar el cable de red. Se probó conectando un sniffer y conectando directamente a un puerto del switch. No existe otro tipo de puerto en la máquina de votación que permita algún tipo de conexión o transferencia de datos.
Resultados de la prueba: Mediante esta prueba se comprobó que los puertos de conexión no están habilitados para acceso externo y proporciona una operación aislada. La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.	

Firma y sello

Cargo

Nombre Empresa

Lugar y fecha

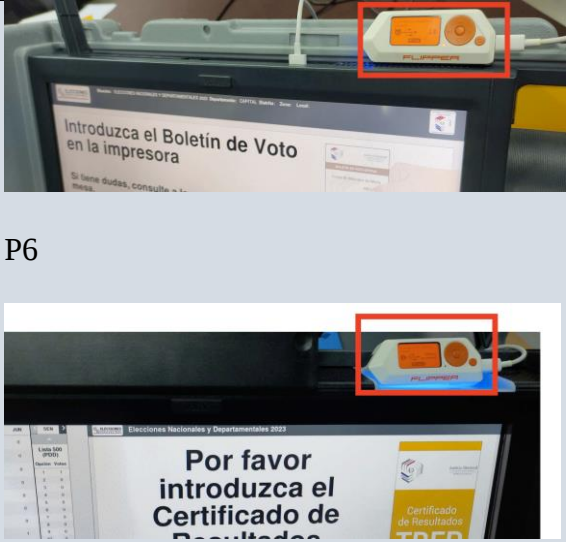
FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD

Nombre o Tipo de Prueba Realizada:

Prueba de voto secreto sin almacenar información del voto y de los electores

Objetivo de la Prueba	Descripción de la Prueba:
Evaluar la garantía de voto secreto, sin almacenar información relacionada con el voto de cada elector	La prueba inicia con un análisis visual de las placas principales de los dos equipos, no se identificaron dispositivos de almacenamiento persistente.   Además, se pudo comprobar que al conectar dispositivos de almacenamiento USB estos no son energizados en el caso de la máquina P6 y en el caso de la P4, si se energiza pero no hay interacción con el sistema operativo. P4

FICHA DE PRUEBA SOBRE LA REVISIÓN DE LA SEGURIDAD

	 P6
Resultados de la prueba: Mediante esta prueba se comprobó que no existen dispositivos de almacenamiento persistente en la máquina de votación. La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.	

Firma y sello

Cargo

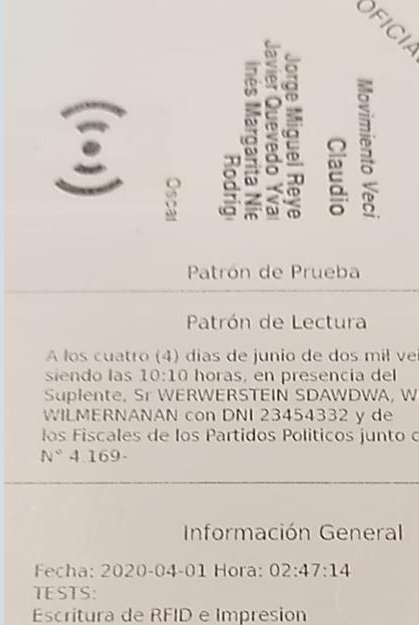
Nombre Empresa

Lugar y fecha

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

Nombre o Tipo de Prueba Realizada:

Probar la existencia de fechas en el hardware y verificar si la fecha es escrita en las boletas de votación.

Objetivo de la Prueba Acceder por medio de la utilidad de mantenimiento y/o pruebas para la consulta de la fecha actual. Verificación en las boletas impresas que están no hagan referencia a una marca de tiempo de algún tipo. La lectura de chip de la boleta para presentación en pantalla.	Descripción de la Prueba: Se revisa primero la boleta que se imprime desde la utilidad de mantenimiento de la terminal para verificar si existe fecha y hora. 
--	--

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

por el mismo principio de no “almacenar información”.

En el siguiente escenario se verifican que las boletas no tengan ningún tipo de referencia en tiempo, esto verificándolo tanto en la boleta física como en pantalla.

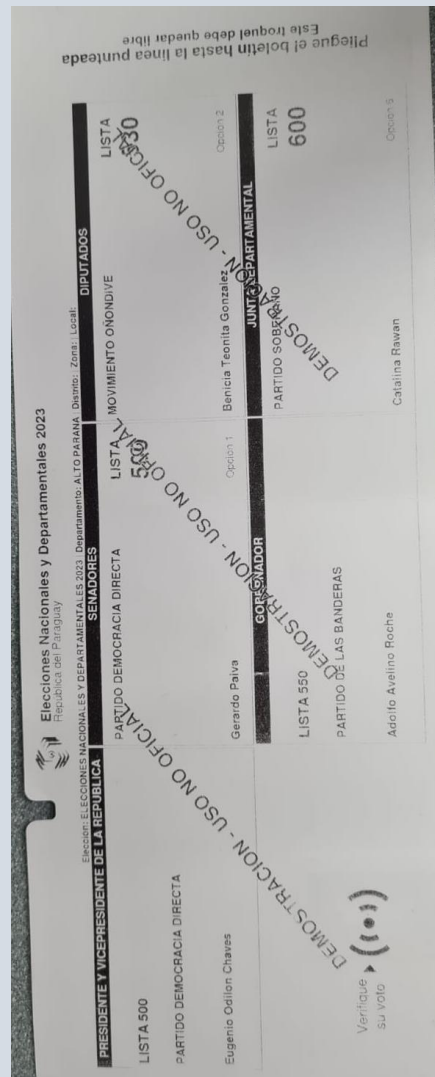


Fig 2. Boleta de votación, sin evidencia de fecha impresa.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

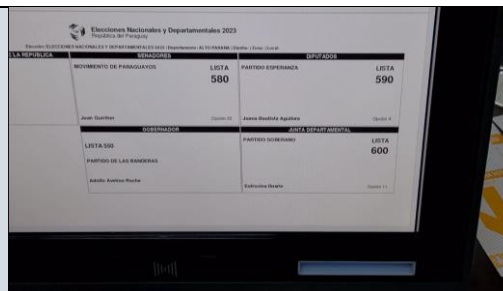


Fig 3. Boleta de votación, sin evidencia de fecha en pantalla.

Resultados de la prueba:

En la utilidad de mantenimiento solo se presenta la fecha y hora de fabricación, no se tiene una fecha actualizada, la fecha siempre se reinicia a la fecha de fabricación de la placa de computo cuando se enciende el equipo.

Se revisaron la impresión de las boletas de votación y estas no tienen fecha de creación en ninguno de los casos, de igual forma la lectura del chip no presenta tampoco una fecha de creación en pantalla.

Firma y sello

Cargo

Nombre Empresa

Lugar y fecha

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

Nombre o Tipo de Prueba Realizada:

Probar el uso de equipos celulares para la lectura a distancia en la zona del equipo de votación.

Objetivo de la Prueba

Usar un dispositivo común como un celular para capturar información de los chips pasivos a una distancia.

Descripción de la Prueba:

Para estas pruebas se realizó por medio de dos celulares marca Samsung modelos S20 FE y S8, la aplicación NFC Taginfo, y se usaron unas cajas plásticas de distancias de 1cm y 3cm respectivamente. Se ubicaron los dispositivos móviles de una forma paralela al chip RFID y se observó en varios intentos si se podría leer el chip, la distancia máxima usada fue 4 cm (usando el recipiente de 3cm y el de 1cm apilado).

En el caso de la boleta de votación y usando el Samsung S8:



Fig 1. Boleta de votación usada.



FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

Fig.2. Distancia de 1 cm.



Fig 3. Lectura exitosa al primer intento.



Fig 4. Distancia de 3 cm.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE



Fig 5. Detección no exitosa a 3 cm.

En el caso de la boleta TREP y usando el Samsung S8:

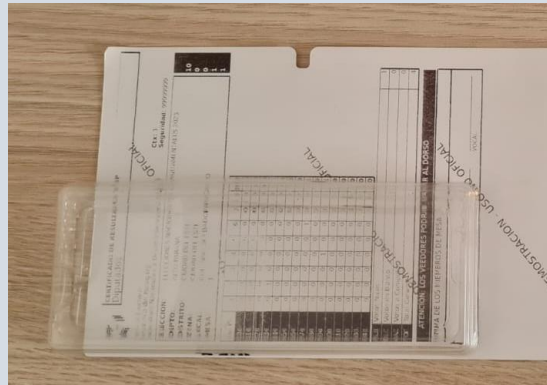


Fig 6. Boleta TREP.

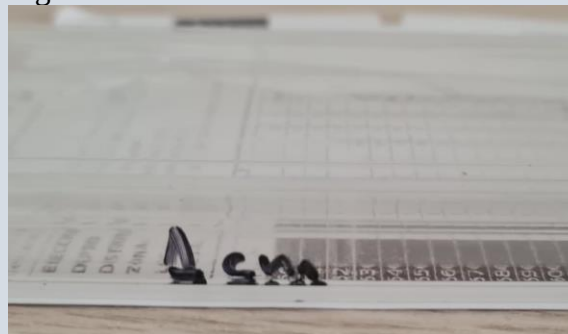


Fig 7. Boleta TREP a 1 cm.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE



Fig 8. Lectura Exitosa al primer intento.

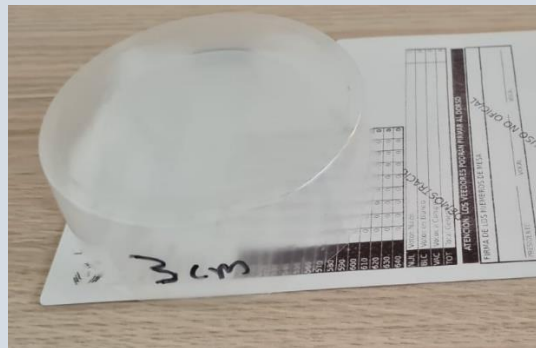


Fig 9. Distancia de 3cm.



Fig 10. Lectura inestable a 3cm.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

Se realizan las mismas pruebas, pero en este caso con un Samsung S20 FE:

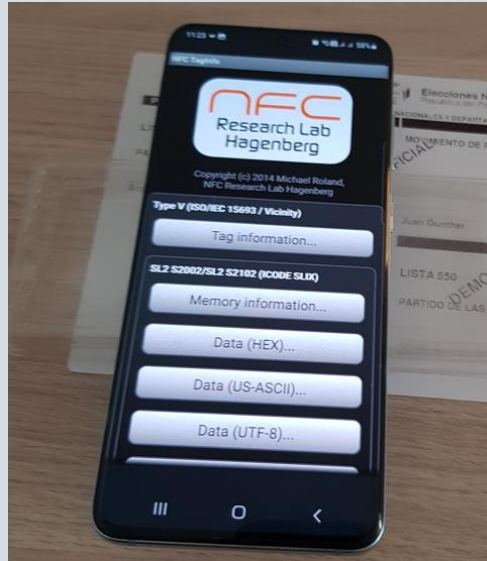


Fig 11. Lectura exitosa al primer intento boleta de votación a 1 cm.

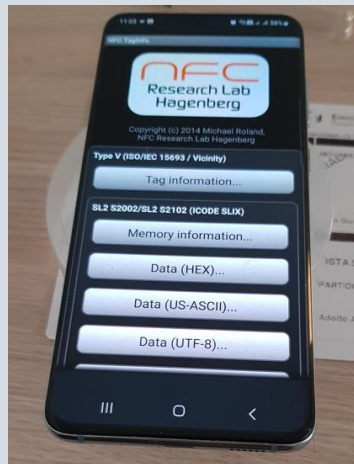


Fig 12. Lectura exitosa al primer intento boleta de votación a 3 cm.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

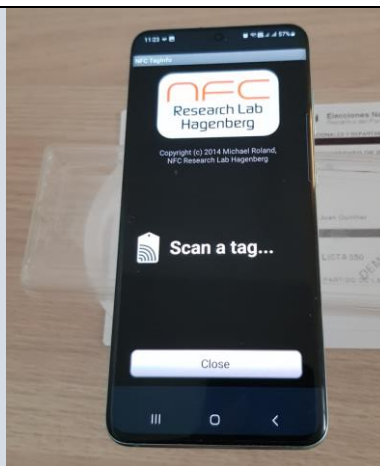


Fig 13. Lectura no exitosa boleta de votación a 4 cm.

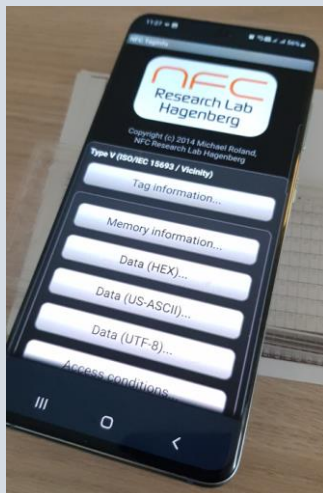


Fig 14. Lectura exitosa al primer intento boleta TREP a 1 cm.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE



Fig 15. Lectura exitosa al primer intento boleta TREP a 3 cm.



Fig 16. Lectura inestable a 4cm.

Resultados de la prueba:

Se concluye que desde un equipo como un lector nfc de un celular la única forma de capturar datos es una distancia de menos de 4 cm y en un escenario estable sin movimiento, con esto se garantiza que las boletas no serán leídas a distancia.

Según el estándar y teniendo tecnología especializada se puede obtener datos a 1mts de distancia, y si aún existiera una antena conectada a un dispositivo de mucha potencia, obtener los datos de la boleta no serían interpretados por que esta información está cifrada para garantizar el secreto del voto.



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

Firma y sello

Cargo

Nombre Empresa

Lugar y fecha



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

Nombre o Tipo de Prueba Realizada:
Pruebas de modificación de los boletas o boletines.

Objetivo de la Prueba

Constatar que las boletas de votación o TREP no se pueden modificar.

Descripción de la Prueba:

Crear en el terminal de votación una boleta y un boletín, posteriormente usar una aplicación nfc desde el celular para enviar los comandos necesarios para la modificación de la información.

Para estas pruebas se realizó por medio de un celular Samsung S20 FE, y dos aplicaciones que son NFC tools(free) y NFC Taginfo, por medio de NFC Tool, nos permite enviar comandos personalizados al chip y NFC Taginfo, nos permite revisar la información al detalle del chip RFID, su estado, y el contenido de sus bloques.

Se usa como referencia los comandos descritos en la siguiente tabla:

Table 16. Command codes

Command code standard	Function	Command code custom	Function
01h	Inventory	2Ch	Get Multiple Block Security Status
02h	Stay Quiet	B1h	Write-sector Password
20h	Read Single Block	B2h	Lock-sector Password
21h	Write Single Block	B3h	Present-sector Password
23h	Read Multiple Block	C0h	Fast Read Single Block
25h	Select	C1h	Fast Inventory Initiated
26h	Reset to Ready	C2h	Fast Initiate
27h	Write AFI	C3h	Fast Read Multiple Block
28h	Lock AFI	D1h	Inventory Initiated
29h	Write DSFID	D2h	Initiate
2Ah	Lock DSFID		
2Bh	Get System Info		

Tabla 1 obtenida de:

https://www.st.com/resource/en/application_note/an3163-configuring-your-iso-15693-reader-to-support-the-m24lrxr-and-m24lrxer-devices-stmicroelectronics.pdf

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

Se crea una boleta en la terminal de votación, y un boletín trep, en el caso de la boleta de votación utiliza un chip rfid de 28 bloques de marca NXP y para el trep es de 80 bloques marca ST.

Posteriormente, se usa el NFC Taginfo para entregar la siguiente información con respecto la boleta de votación.



Fig 1. Información del CHIP RFID Boleta de votación.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

NFC TagInfo
Data (HEX)
Block 0
1c01002a
Block 1
937c37c6
Block 2
5e9221d4
Block 3
dc7c24bb
Block 4
eb079dde
Block 5
66eebb3b
Block 6
19a11e9e
Block 7
81bae089
Block 8
4e2efc4e
Block 9
5d73cd9a
Block 10
94352d44
Block 11
d883ab56
Block 12
dc3e0000

Fig 2. Información escrita en el Chip RFID de boleta de votación.

NFC TagInfo
Access conditions
Block 0
read-only
Block 1
read-only
Block 2
read-only
Block 3
read-only
Block 4
read-only
Block 5
read-only
Block 6
read-only
Block 7
read-only
Block 8
read-only
Block 9
read-only
Block 10
read-only
Block 11
read-only
Block 12
read-only
Block 13

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

Fig 3. Estado de los bloques del Chip RFID de la boleta de votación.

A Continuación, se realizan las pruebas por medio de NFC Tools, se usan comandos de escritura y lectura, para verificar que los datos no se modifiquen.

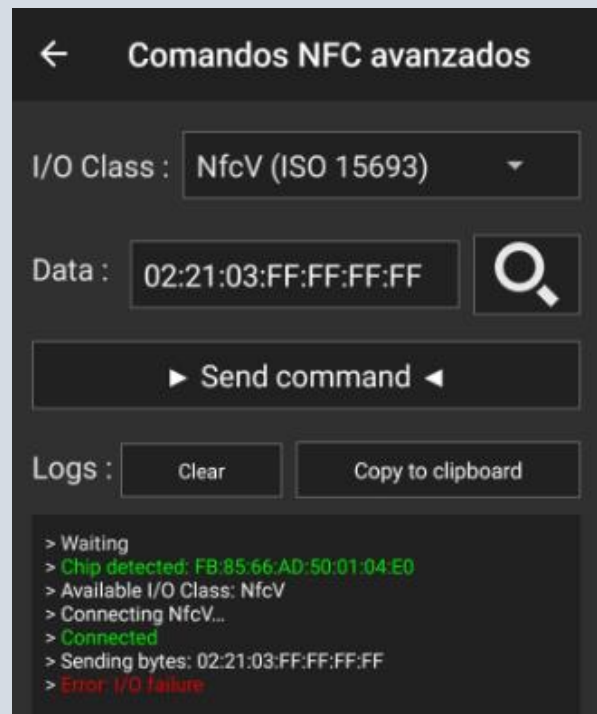


Fig 4. Prueba de escritura del bloque 3 en el CHIP RFID de la boleta de votación no exitosa.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

The screenshot displays the 'Comandos NFC avanzados' (Advanced NFC Commands) interface. It features a dropdown menu for 'I/O Class' set to 'NfcV (ISO 15693)', a 'Data' input field containing '02:20:03', and a 'Send command' button. Below the button are 'Clear' and 'Copy to clipboard' options for the logs. The log output shows a successful sequence: '> Waiting', '> Chip detected: FB:85:66:AD:50:01:04:E0', '> Available I/O Class: NfcV', '> Connecting NfcV...', '> Connected', '> Sending bytes: 02:20:03', and '> Result: 00:DC:7C:24:BB'.

Fig 5. Prueba de lectura del bloque 3 en el CHIP RFID de la boleta de votación, resultado exitoso, el mismo del bloque 3 en la Fig 2.

Con respecto a la boleta TREP se realiza el mismo ejercicio anterior.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

	NFC TagInfo Tag information UID e002080391785c5a RF technology Type V (ISO/IEC 15693 / Vicinity) Manufacturer STMicroelectronics SA (France) Application family identifier (AFI) all families and sub-families AFI (numeric) 00 DSF Id 00 Response flags 00 IC reference 08 Target technology classes (Android) android.nfc.tech.NfcV, android.nfc.tech.NdefFormatable	
	NFC TagInfo Memory information Memory size 320 Byte Block size 4 Byte Number of blocks 80	

Fig 6. Información del CHIP RFID Boleta TREP.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

NFC TagInfo
Data (HEX)
Block 0
1c040024
Block 1
9182a611
Block 2
00000000
Block 3
6daf1221
Block 4
03789c33
Block 5
545466bf
Block 6
c000030e
Block 7
0c488005
Block 8
443032a0
Block 9
83870c00
Block 10
4ba20273
Block 11
00000000
Block 12
00000000

Fig 7. Información escrita en el Chip RFID de boleta TREP.

NFC TagInfo
Access conditions
Block 0
read-only
Block 1
read-only
Block 2
read-only
Block 3
read-only
Block 4
read-only
Block 5
read-only
Block 6
read-only
Block 7
read-only
Block 8
read-only
Block 9
read-only
Block 10
read-only
Block 11
read-only
Block 12
read-only

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

Fig 8. Estado de los bloques del Chip RFID de la boleta.

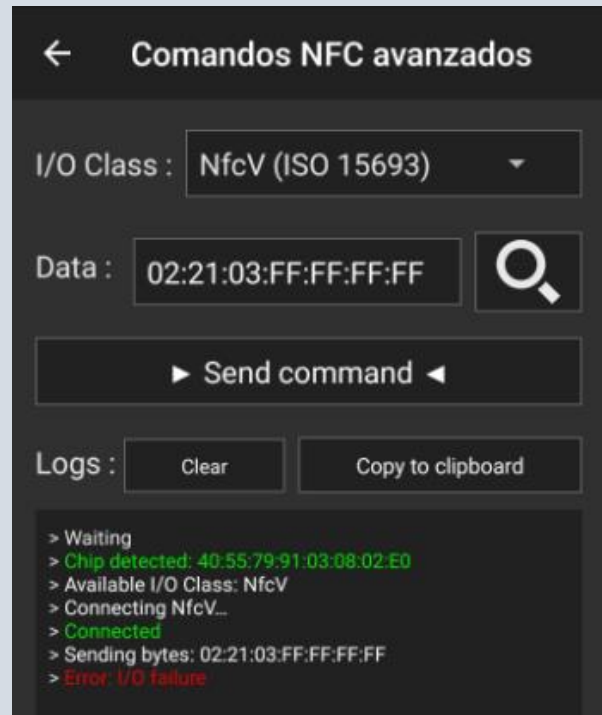


Fig 9. Prueba de escritura del bloque 3 en el CHIP RFID de la boleta TREP.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

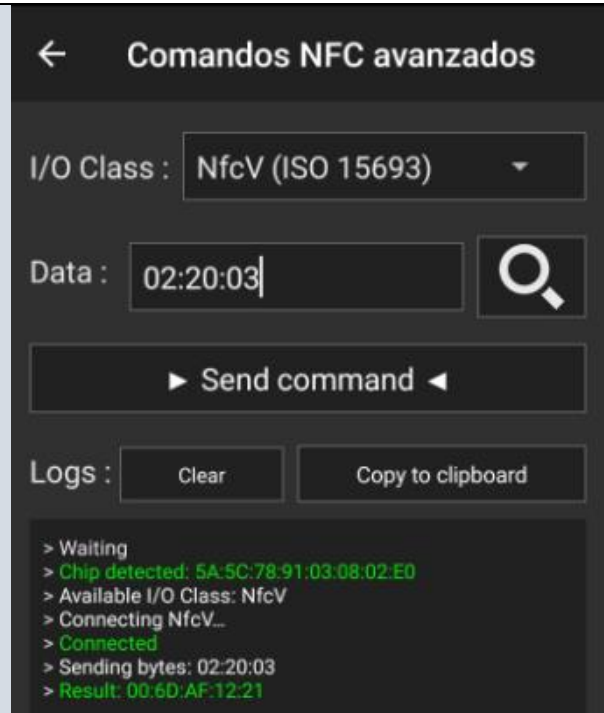


Fig 10. Prueba de lectura del bloque 3 en el CHIP RFID de la boleta TREP, resultado exitoso, el mismo del bloque 3 en la Fig 7.

Se puede comprobar desde el NFC Tool que para los dos tipos de chips que se usan estos una vez escritos en la terminal de votación quedan en estado bloqueado.

Con el comando que se envía al chip el 02:2C y el rango de bloques 00:28, se evidencia que en el caso de la boleta de votación el resultado después de la respuesta 00 para todos los bloques es 01, que significa que están en esta lock, y esto impide la escritura de los datos del chip.



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



FICHA DE PRUEBA SOBRE LA REVISIÓN DEL HARDWARE

Firma y sello

Cargo

Nombre Empresa

Lugar y fecha

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Objetivo General: Revisión detallada del diseño de software, documentación técnica, documentación de usuario, casos de uso, casos de prueba, QA, sistema operativo, parametrización, control de versiones, control de cambios, custodia de código, pruebas y simulacros.

Objetivos Específicos:

- Evaluar los procedimientos de diseño, desarrollo y versionado son adecuados.
- Evaluar que los aplicativos desarrollados se encuentren individualizados e identificados en un catálogo que permite validar su integridad.
- Evaluar los esquemas y estándares de seguridad utilizados.
- Evaluar que las capacidades de parametrización se adecúan a los requerimientos.
- Evaluar que se realice una adecuada gestión y control de cambios.
- Evaluar los procesos de control de calidad y pruebas.
- Evaluar que los casos de uso estén completos, detallados y acordes a las necesidades del proceso.
- Evaluar que los casos de prueba sean exhaustivos y estén acordes a los casos de uso.
- Evaluar el análisis de los sistemas desde una perspectiva de desarrollo de software, de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.
- Evaluar la integridad y la consistencia de los datos, de la información transmitida desde las máquinas de votación a las boletas de votación.

Nombre o Tipo de Prueba Realizada:

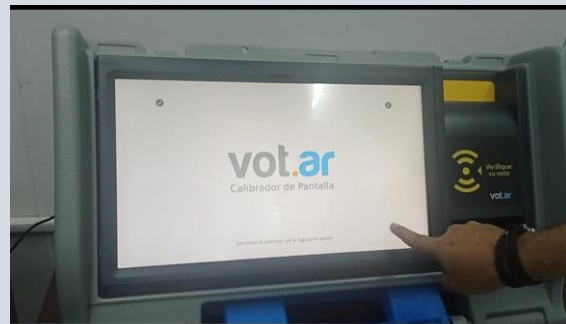
Prueba de arranque y del módulo de calibración de la máquina de votación electrónica

Objetivo de la Prueba	Descripción de la Prueba:
Constatar el arranque y la funcionalidad de las opciones de calibración con las que cuenta la máquina de votación Electrónica	La prueba inició con la comprobación del encendido del equipo, carga del sistema operativo y el software de votación que están contenidos en el DVD de arranque. Durante este primer proceso se comprobó que el equipo queda a la espera del inicio del sistema a través del DVD de arranque sin el cual la maquina no inicia ninguna aplicación.

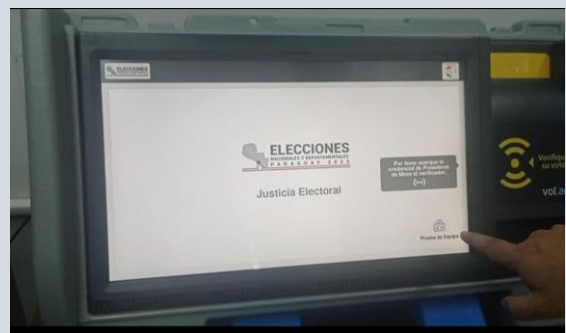
FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE



Una vez cargado el Sistema Operativo y el Software de Votación, se probó la función de calibración de la pantalla.



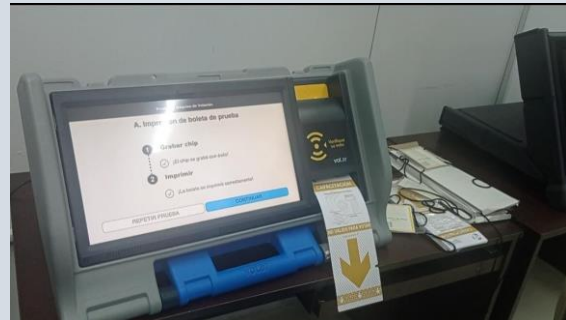
Luego de esto se probaron las opciones de calibración y prueba de los componentes del equipo a través del módulo de **“Pruebas de Equipo”**.



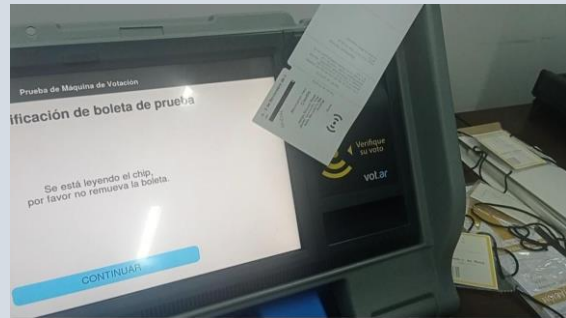
Dentro del módulo de Pruebas del Equipo se realizaron las siguientes comprobaciones:

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Escritura del Chip RFID
Impresión de la papeleta de votación



Lectura del Chip RFID



Las pruebas fueron satisfactorias y sin ningún contratiempo.

Resultados de la prueba:

Se comprobó el funcionamiento correcto de la impresión de la boleta electoral, así como la lectura y escritura del Chip RFID.

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Firma y sello

Cargo

Nombre Empresa

Lugar y fecha

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Objetivo General: Revisión detallada del diseño de software, documentación técnica, documentación de usuario, casos de uso, casos de prueba, QA, sistema operativo, parametrización, control de versiones, control de cambios, custodia de código, pruebas y simulacros.

Objetivos Específicos:

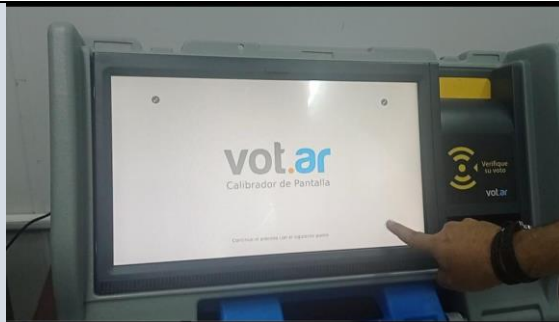
- Evaluar los procedimientos de diseño, desarrollo y versionado son adecuados.
- Evaluar que los aplicativos desarrollados se encuentren individualizados e identificados en un catálogo que permite validar su integridad.
- Evaluar los esquemas y estándares de seguridad utilizados.
- Evaluar que las capacidades de parametrización se adecúan a los requerimientos.
- Evaluar que se realice una adecuada gestión y control de cambios.
- Evaluar los procesos de control de calidad y pruebas.
- Evaluar que los casos de uso estén completos, detallados y acordes a las necesidades del proceso.
- Evaluar que los casos de prueba sean exhaustivos y estén acordes a los casos de uso.
- Evaluar el análisis de los sistemas desde una perspectiva de desarrollo de software, de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.
- Evaluar la integridad y la consistencia de los datos, de la información transmitida desde las máquinas de votación a las boletas de votación.

Nombre o Tipo de Prueba Realizada:

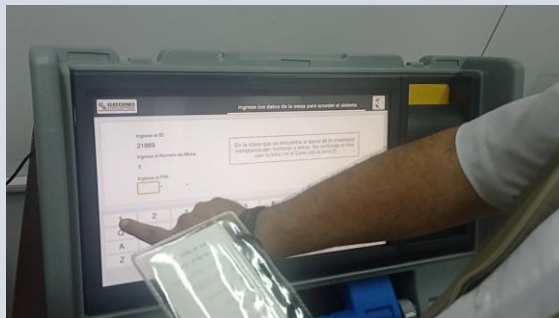
Prueba del módulo de cierre de mesa y escrutinio

Objetivo de la Prueba	Descripción de la Prueba:
Constatar el correcto funcionamiento de las opciones del módulo de cierre de mesa y escrutinio.	La prueba inicia con el encendido del equipo, la carga del sistema operativo y el software de votación contenidos en un DVD. Una vez cargado el Sistema Operativo y el Software de Votación, se probó nuevamente la función de calibración de la pantalla.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

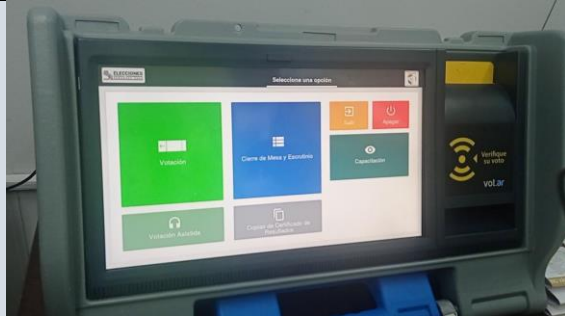


Luego se comprobó que es necesario habilitar nuevamente el sistema con la credencial de miembro de mesa proporcionada acercando el Chip para su lectura e ingresando los datos impresos en la credencial para vincular la máquina con la mesa electoral respectiva.

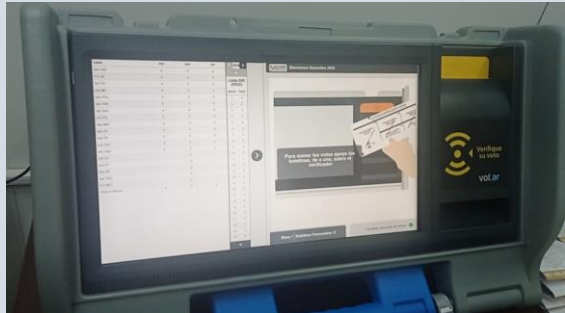


Luego de confirmar la información de la mesa, se habilita la pantalla con el acceso a los diferentes módulos del sistema y procedemos a seleccionar el módulo de “Cierre de Mesa y Escrutinio”.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE



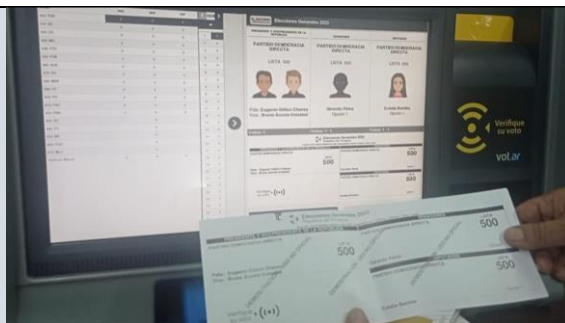
Una vez se seleccionó esta opción, el sistema presenta la interfaz en la cual se realizará la contabilización de los votos que emitimos para esta mesa electoral.



En esta interfaz se realizó la prueba de conteo acercando cada voto emitido al lector de RFID y constatando que este voto va sumándose al candidato seleccionado en cada una de las dignidades o categorías.

Se destaca el hecho que en cada voto contabilizado es presentado también en pantalla para su comprobación.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

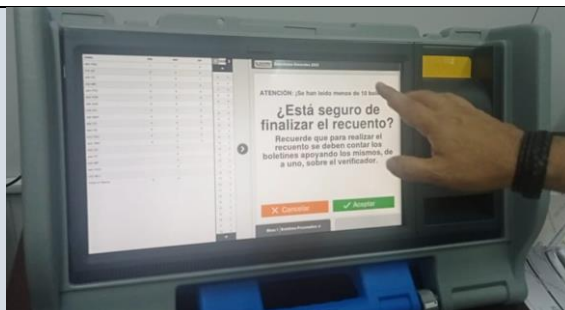


Se comprobó también que al pasar la misma boleta más de una vez, el sistema lo rechaza y presenta una alerta en pantalla. Además, se comprobó que este voto no sea contabilizado nuevamente.

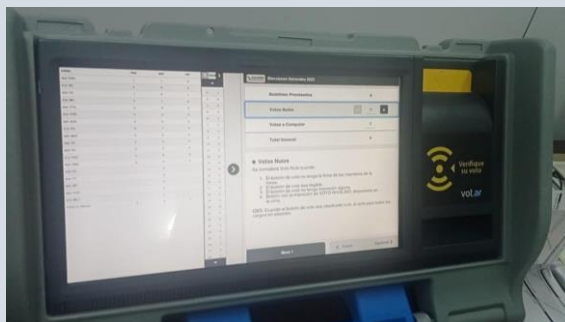


Finalmente, para terminar el conteo de votos, seleccionamos la opción “Terminar Recuento”, en este caso al tener un número menor de 10 votos, el sistema presenta una alerta antes de proceder al cierre del escrutinio. Esta es una medida de precaución para que la autoridad de mesa no cierre el proceso de escrutinio sin primero haber contabilizado todas las boletas pendientes de conteo.

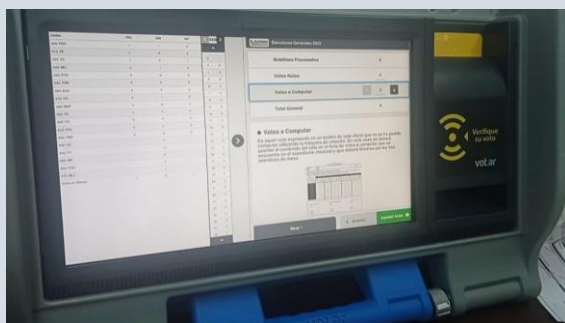
FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE



Luego el sistema presenta una pantalla en la que se nos permite registrar de manera manual, los votos nulos y votos a computar, para información de los miembros de mesa en cada opción se nos indica las causas por las cuales un voto es nulo o cuando se suma un voto a computar.

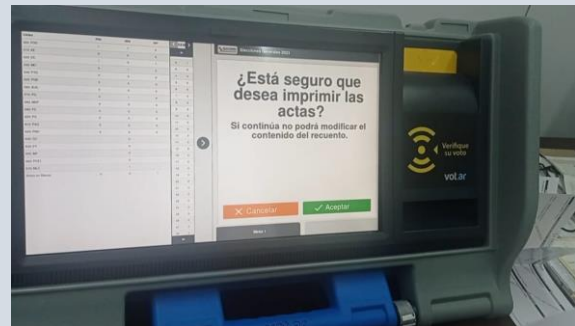


Una vez realizado este registro, se activa la opción para la impresión de actas y certificados.

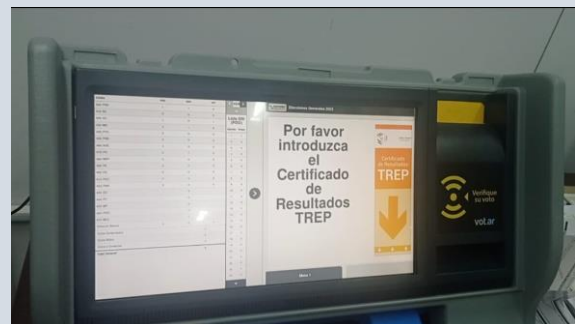


FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Al seleccionar la opción de impresión, el sistema presenta una alerta indicando que se terminará el recuento de votos y que ya no se podrá realizar ninguna modificación al conteo realizado.



El primer certificado que el sistema imprime es el “Certificado de Resultados TREP”.



Se comprobó la impresión de un certificado por cada una de las dignidades o categorías a elegir.

Se verificó que este tipo de certificado cuenta con un Chip RFID y además se imprime un código QR que contiene los resultados de la mesa.

Se prioriza este certificado debido a que este es enviado para su transmisión en el sistema



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

	TREP, que es un sistema propio del Tribunal Supremo de Justicia Electoral. Seguidamente el sistema procede con la impresión de las actas de escrutinio, las cuales se entregarán a los veedores de las agrupaciones políticas presentes en el escrutinio. Estas actas no poseen un Chip RFID, pero si se imprime un código QR para una lectura rápida de los resultados del acta. Así mismo se comprobó que se imprime un acta por cada dignidad o categoría a elegir.
Resultados de la prueba: Se comprobó el funcionamiento correcto de cada una de las funcionalidades del módulo de “Cierre de Mesa y Escrutinio”. Debido al alcance de la auditoría, esta prueba concluyó con la impresión de los certificados y actas de escrutinio sin validar la transmisión de los resultados que se realizan a través de los mismos con el sistema TREP. La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.	

Firma y sello

Cargo

Nombre Empresa



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Lugar y fecha



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Objetivo General: Revisión detallada del diseño de software, documentación técnica, documentación de usuario, casos de uso, casos de prueba, QA, sistema operativo, parametrización, control de versiones, control de cambios, custodia de código, pruebas y simulacros.

Objetivos Específicos:

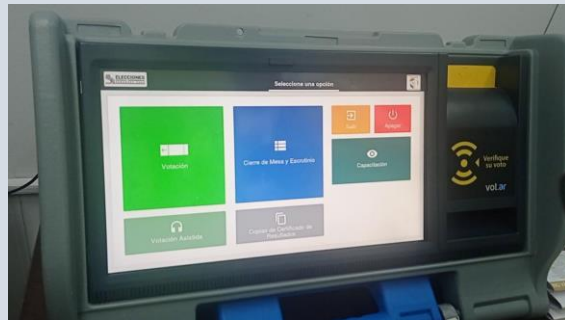
- Evaluar los procedimientos de diseño, desarrollo y versionado son adecuados.
- Evaluar que los aplicativos desarrollados se encuentren individualizados e identificados en un catálogo que permite validar su integridad.
- Evaluar los esquemas y estándares de seguridad utilizados.
- Evaluar que las capacidades de parametrización se adecúan a los requerimientos.
- Evaluar que se realice una adecuada gestión y control de cambios.
- Evaluar los procesos de control de calidad y pruebas.
- Evaluar que los casos de uso estén completos, detallados y acordes a las necesidades del proceso.
- Evaluar que los casos de prueba sean exhaustivos y estén acordes a los casos de uso.
- Evaluar el análisis de los sistemas desde una perspectiva de desarrollo de software, de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.
- Evaluar la integridad y la consistencia de los datos, de la información transmitida desde las máquinas de votación a las boletas de votación.

Nombre o Tipo de Prueba Realizada:

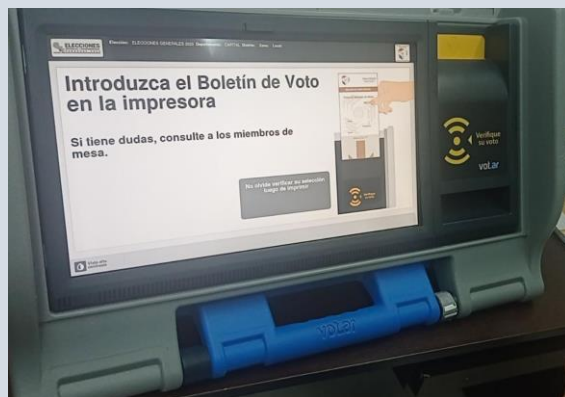
Prueba del módulo de votación

Objetivo de la Prueba	Descripción de la Prueba:
Constatar el correcto funcionamiento del módulo de votación.	La prueba inicia con la máquina de votación encendida, el sistema operativo y el software de votación contenidos en el DVD ejecutándose en el equipo y el sistema habilitado para su uso, vinculando la máquina con la mesa electoral a la que pertenece mediante la credencial respectiva. En este punto el sistema presenta una pantalla los diferentes módulos a los que se puede tener acceso.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE



Seleccionando el módulo de “Votación”, el sistema queda listo para recibir la votación de los electores.



Para esta prueba se nos proporcionó un paquete de boletas de votación utilizadas en capacitación, las que están sin imprimir y con el Chip RFID en blanco.

Se realizó una primera prueba insertando una boleta con un voto impreso en ella y grabado en el Chip RFID y se constató que el sistema expulsa la boleta y presenta el voto impreso en la pantalla.

A continuación, se colocó una boleta de votación en blanco en la bandeja de la impresora.

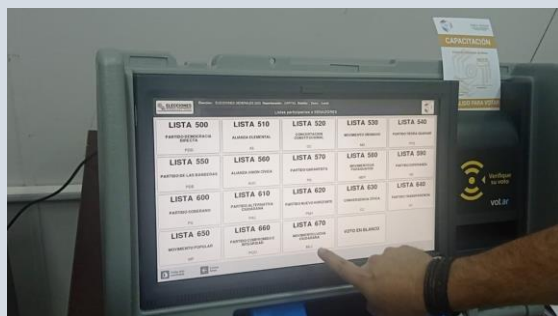
FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE



Inmediatamente el sistema presenta en pantalla a los candidatos debidamente identificados para la elección de presidente y vicepresidente de la República.



Se realizó la selección de unos de los candidatos al azar; luego de esto, el sistema presenta los partidos o agrupaciones políticas participantes en la elección de senador.



FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

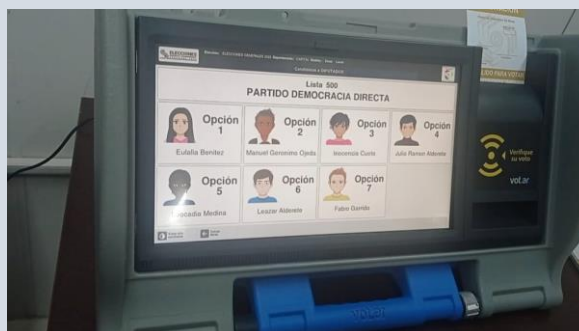
Una vez seleccionada la agrupación política, el sistema presenta los candidatos de dicha agrupación para su selección.



Una vez realizada la selección del candidato a senador, el sistema presenta los partidos o agrupaciones políticas participantes en la elección de diputado.

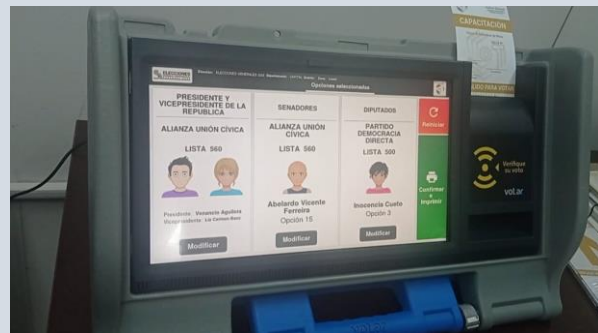


Seleccionada la agrupación política, el sistema presenta los candidatos de dicha agrupación para la selección del diputado.



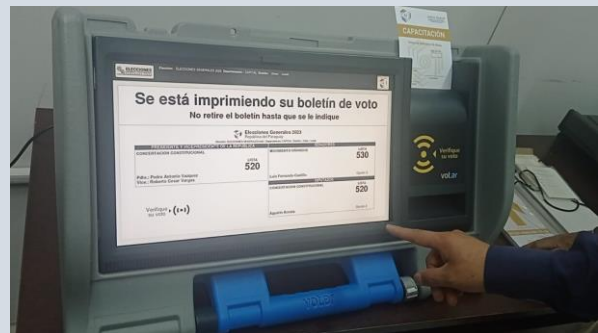
FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Finalizada la selección de candidatos el sistema presenta una pantalla con la selección realizada para su confirmación.



Se comprobó que también es posible realizar modificaciones a la selección de candidatos las veces que el usuario lo crea conveniente hasta confirmar su elección.

Una vez confirmada la selección realizada, el sistema inició con la grabación de la información del voto realizado en el Chip RFID y la inmediata impresión de la papeleta.



Finalmente se pudo comprobar la lectura del Chip RFID al acercar la boleta al lector RFID lo que produce que se presente en pantalla la selección de candidatos que se grabó en el Chip y se pueda comprobar que es la misma información que esta impresa en la boleta.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE



Resultados de la prueba:

Mediante esta prueba se comprobó el funcionamiento del módulo de votación y se determinó que se puede realizar un voto únicamente con una boleta que contenga un Chip RFID en blanco. Una vez realizado el voto se comprobó que la impresión concuerda con lo grabado en el Chip.

También se pudo comprobar que el elector puede modificar su voto las veces que crea conveniente hasta quedar conforme con la selección

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.

Firma y sello

Cargo

Nombre Empresa



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Lugar y fecha

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Objetivo General: Revisión detallada del diseño de software, documentación técnica, documentación de usuario, casos de uso, casos de prueba, QA, sistema operativo, parametrización, control de versiones, control de cambios, custodia de código, pruebas y simulacros.

Objetivos Específicos:

- Evaluar los procedimientos de diseño, desarrollo y versionado son adecuados.
- Evaluar que los aplicativos desarrollados se encuentren individualizados e identificados en un catálogo que permite validar su integridad.
- Evaluar los esquemas y estándares de seguridad utilizados.
- Evaluar que las capacidades de parametrización se adecúan a los requerimientos.
- Evaluar que se realice una adecuada gestión y control de cambios.
- Evaluar los procesos de control de calidad y pruebas.
- Evaluar que los casos de uso estén completos, detallados y acordes a las necesidades del proceso.
- Evaluar que los casos de prueba sean exhaustivos y estén acordes a los casos de uso.
- Evaluar el análisis de los sistemas desde una perspectiva de desarrollo de software, de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.
- Evaluar la integridad y la consistencia de los datos, de la información transmitida desde las máquinas de votación a las boletas de votación.

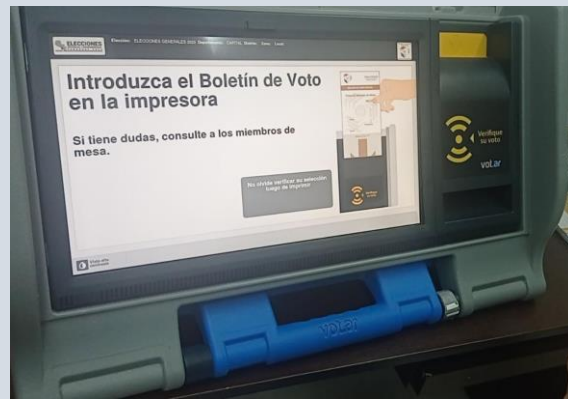
Nombre o Tipo de Prueba Realizada:

Prueba del módulo de votación asistida

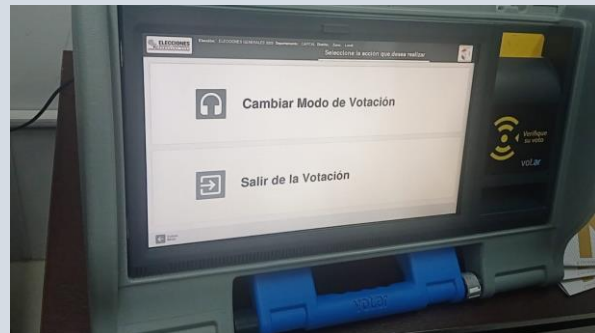
Objetivo de la Prueba	Descripción de la Prueba:
Constatar el correcto funcionamiento del módulo de votación asistida, el cual ayuda a las personas no videntes a realizar el proceso de votación.	La prueba inicia con la máquina de votación encendida, el sistema operativo y el software de votación contenidos en el DVD ejecutándose en el equipo y el sistema habilitado para su uso, vinculando la máquina con la mesa electoral a la que pertenece mediante la credencial respectiva y se ha seleccionado el módulo de votación y el sistema se encuentra listo a recibir los votos de los electores.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Además, se contó con una plantilla acrílica que ayuda a la persona no vidente en la selección de las opciones de votación.



Para activar el módulo de “Votación Asistida”, es necesario acercar nuevamente la credencial de “Miembro de Mesa” al lector de RFID, lo cual activa la pantalla para la selección del modo de votación asistida.

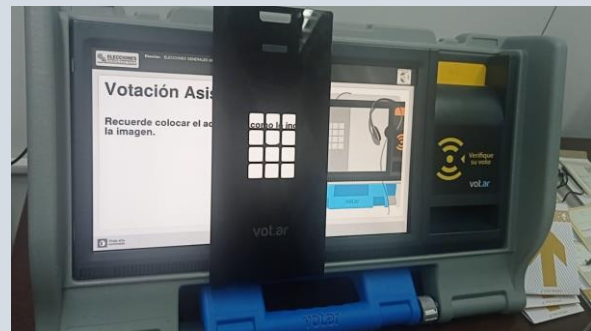


Al seleccionar la opción “Cambiar Módulo de Votación”, se activa el módulo de votación asistida.

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE



En este punto es necesario colocar el acrílico en la posición indicada en el gráfico de la pantalla y luego introducir la boleta de votación en la ranura respectiva.



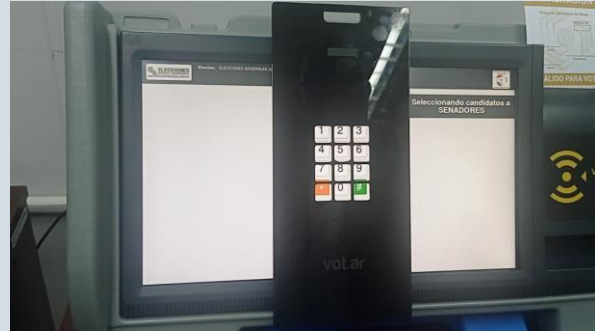
Una vez colocada la boleta en la posición correcta, se presentan en pantalla un panel de números que coinciden con la plantilla acrílica y el sistema inicia la lectura de las opciones de votación la cual se escucha a través de unos audífonos proporcionados por la mesa.

En este caso cada candidatura es vinculada a un código numérico y se procedió a la selección de los candidatos de acuerdo al código dictado por el sistema.

Para efectos de esta prueba, no se utilizaron los audífonos para que los auditores podamos escuchar cada una de las opciones dictadas por

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

el sistema a través de los altavoces de la máquina.



Finalizada la selección de candidatos el sistema al igual que en la votación normal, también repasa las candidaturas seleccionadas y solicita al elector confirmarlas digitando la tecla numeral (#) como confirmación.

Una vez confirmada la selección de candidatos se procede con la impresión de la boleta de votación con las opciones seleccionadas.



Se verificó que el elector en este modo también puede confirmar la selección guardada en el Chip e impresa en la boleta. Para esto solamente tiene que introducir la boleta nuevamente en la ranura de la impresora y el sistema procederá con la lectura de lo que se guardó en el Chip RFID.



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Resultados de la prueba:

Mediante esta prueba se comprobó el funcionamiento del módulo de votación asistida y se determinó que es factible para un elector no vidente poder realizar su proceso de votación a través de esta opción con la seguridad y confidencialidad que exige una votación electoral.

También se pudo comprobar que el elector de igual forma que en la votación normal, puede modificar su voto las veces que crea conveniente hasta quedar conforme con la selección

La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.

Firma y sello

Cargo

Nombre Empresa

Lugar y fecha

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Objetivo General: Revisión detallada del diseño de software, documentación técnica, documentación de usuario, casos de uso, casos de prueba, QA, sistema operativo, parametrización, control de versiones, control de cambios, custodia de código, pruebas y simulacros.

Objetivos Específicos:

- Evaluar los procedimientos de diseño, desarrollo y versionado son adecuados.
- Evaluar que los aplicativos desarrollados se encuentren individualizados e identificados en un catálogo que permite validar su integridad.
- Evaluar los esquemas y estándares de seguridad utilizados.
- Evaluar que las capacidades de parametrización se adecúan a los requerimientos.
- Evaluar que se realice una adecuada gestión y control de cambios.
- Evaluar los procesos de control de calidad y pruebas.
- Evaluar que los casos de uso estén completos, detallados y acordes a las necesidades del proceso.
- Evaluar que los casos de prueba sean exhaustivos y estén acordes a los casos de uso.
- Evaluar el análisis de los sistemas desde una perspectiva de desarrollo de software, de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.
- Evaluar la integridad y la consistencia de los datos, de la información transmitida desde las máquinas de votación a las boletas de votación.

Nombre o Tipo de Prueba Realizada:

Prueba de habilitación del sistema y credenciales

Objetivo de la Prueba	Descripción de la Prueba:
Constatar la habilitación correcta del sistema mediante credenciales de acceso.	La prueba inicia con la máquina de votación electrónica ya encendida y el sistema operativo y el software de votación contenidos en el DVD ya ejecutándose en el equipo. En este punto la máquina se encuentra a la espera de recibir la información de las credenciales de acceso.

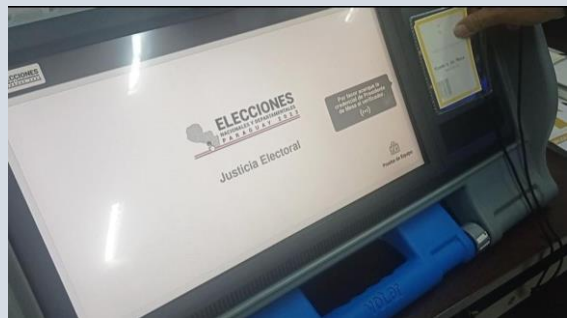
FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE



Para esta prueba se nos proporcionó una credencial electrónica de miembro de mesa.

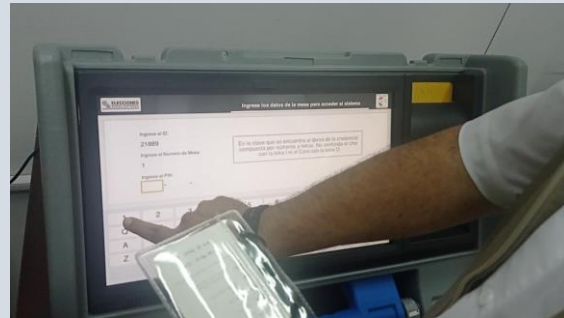


Para la iniciar la habilitación del equipo, se acercó la credencial proporcionada al lector de RFID de la máquina, con lo cual se habilita la pantalla para el ingreso de la identificación de la mesa electoral que se va a habilitar.

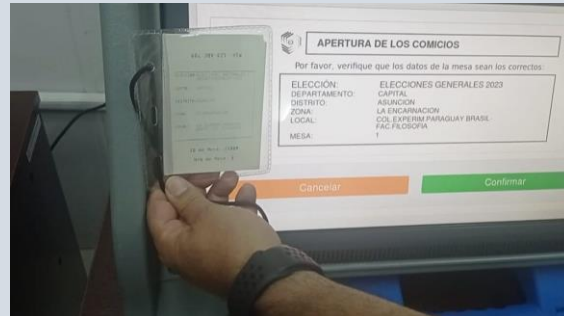


FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Se debe registrar el id de la credencial, el número de mesa electoral y un PIN. Estos datos están impresos en la credencial.



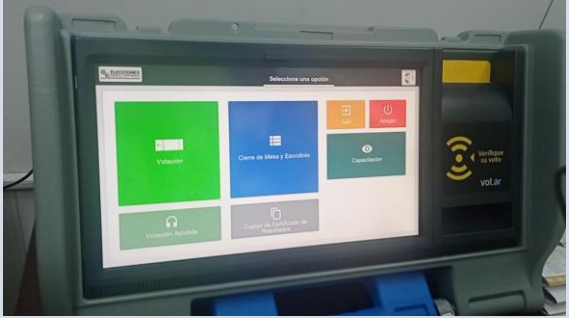
Una vez proporcionada esta información, el sistema realiza la carga de la información de la mesa electoral correspondiente y la presenta en pantalla para comprobar que los datos fueron los correctos.



Luego de confirmar la información de la mesa, se habilita la pantalla con el acceso a los siguientes módulos:

- Votación
- Votación asistida
- Cierre de mesa y escrutinio
- Copia de certificado de resultados
- Capacitación

FICHA DE PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

	Además, se presentan las opciones de “Salir” y “Apagar”.  Finalmente, el sistema queda habilitado, a la espera de la selección que realice el usuario
Resultados de la prueba: Mediante esta prueba se comprobó que únicamente con la credencial y la información impresa en la misma, se puede habilitar el sistema y acceder a sus diferentes módulos. La prueba realizada fue satisfactoria y se ejecutó sin contratiempos.	

Firma y sello

Cargo

Nombre Empresa

Lugar y fecha



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



CUESTIONARIO SOBRE LA REVISIÓN DEL SOFTWARE

Objetivo General: Revisión detallada del diseño de software, documentación técnica, documentación de usuario, casos de uso, casos de prueba, QA, sistema operativo, parametrización, control de versiones, control de cambios, custodia de código, pruebas y simulacros.

Objetivos Específicos:

- Evaluar los procedimientos de diseño, desarrollo y versionado son adecuados.
- Evaluar que los aplicativos desarrollados se encuentren individualizados e identificados en un catálogo que permite validar su integridad.
- Evaluar los esquemas y estándares de seguridad utilizados.
- Evaluar que las capacidades de parametrización se adecúan a los requerimientos.
- Evaluar que se realice una adecuada gestión y control de cambios.
- Evaluar los procesos de control de calidad y pruebas.
- Evaluar que los casos de uso estén completos, detallados y acordes a las necesidades del proceso.
- Evaluar que los casos de prueba sean exhaustivos y estén acordes a los casos de uso.
- Evaluar el análisis de los sistemas desde una perspectiva de desarrollo de software, de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.
- Evaluar la integridad y la consistencia de los datos, de la información transmitida desde las máquinas de votación a las boletas de votación.

No.	Concepto	SI	NO	Cantidades/Detalles/ Observaciones / Fuentes de Información
I. SOFTWARE				
1	Utilizan alguna herramienta para el control de versiones del software?	Si		Cubre el objetivo 1 Gitlab
2	Cuál es el nombre y versión de la base de datos utilizada para el manejo de la información?		No	Cubre el objetivo 10 Utilizan archivo json.
3	Se utiliza algún mecanismo de para ocultar el codigo fuente sensible de la aplicación?		No	Cubre el objetivo 1 Para facilitar su auditaribilidad, no hay información sensible
4	Existe documentos formales de levantamiento de requerimientos	Si		Cubre el objetivo 1



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



CUESTIONARIO SOBRE LA REVISIÓN DEL SOFTWARE

				Formulario de datos de entrada (En la docuemnatcion) El documento se llama parametrización, personalización y automatizacion
5	Cuál es el nombre y la versión del Sistema Operativo utilizado en las maquinas de votación electrónica?	SI		Cubre el objetivo 3 Linux personalizada versión 20.04 LTS, kernel 5.4
6	Existen librerías de terceros o referencias externas utilizadas en el desarrollo de la aplicación?	SI		Cubre el objetivo 2 Jinja, Jandar
7	Se requiere de algún tipo de licenciamiento para la utilización del software o de alguna de sus librerías?	SI		Cubre el objetivo 2 LICENCIAS DE SOFTWARE
8	Se realizó procesos de testeos y de control de calidad del software por una empresa externa?		NO	Cubre el objetivo 6
10	El software tiene opciones para el manejo de personas con discapacidad?	Si		Cubre el objetivo 2 Modulo de no videntes y pantalla para miopes.
11	El software maneja un control de usuarios y roles por usuario?	Si		Cubre el objetivo 1 Soporte técnico y miembros de mesa, se define en el sistema de credenciales.
12	Metodología que se utiliza para el desarrollo de software?	Si		Cubre el objetivo 1 SCRUM BAN
13	El código fuente se encuentra debidamente documentado?	SI		Cubre el objetivo 1 USAN SPHINX
14	Manejan algún estándar para la documentación del código fuente?	SI		Cubre el objetivo 1 SPHINX PEP8
15	Qué metodología se utiliza para el proceso de levantamiento de requerimientos?	SI		Cubre el objetivo 1 epicas
16	Manejan un catálogo de software donde los productos estén debidamente identificados?	Si		Cubre el objetivo 2 Documento que se llama catalogo del software
17	Cuales son los esquemas y estándares de seguridad utilizados en la aplicación?			Cubre el objetivo 3

CUESTIONARIO SOBRE LA REVISIÓN DEL SOFTWARE

				Desarrollamos en base al esquema ASBS de owasp
18	El software desarrollado es parametrizable?	SI		Cubre el objetivo 4 El software se entrega parametrizado.
19	Tienen un procedimiento de gestión de cambios dentro de su proceso de desarrollo?	SI		Cubre el objetivo 5 Mediante Ticket llevan el control
20	Cuál es el proceso que se lleva para el control de calidad y pruebas del software desarrollado			Cubre el objetivo 6 Manual de testing, se ejecuta un protocolo de pruebas cuando sale un nuevo ISO del DVD, son pruebas de hardware y software. Tienen un área de calidad para desarrollar esta actividad.
21	Que control se utiliza para garantizar la integridad y consistencia de los datos que se almacena en el chip ?			Cubre el objetivo 10 Se graba en el chip, se lee en el chip y se compara, y esta información esta encriptada.
22	Se puede abrir una consola Linux para la ejecución de comandos del SO?		NO	Cubre el objetivo 3 No hay terminales en el casper de producción
23	Se utiliza la misma version de software para los distintos modelos de maquinas de votación electrónica existentes?	Si		Cubre el objetivo 2 y 5 Es el mismo para todos los modelos.
24	Como se alimentan los datos en el sistema de votación?			Cubre el objetivo 10 A través de un intercambio seguro de SFTP, se define una persona del Tribunal que es la que sube los



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



CUESTIONARIO SOBRE LA REVISIÓN DEL SOFTWARE

				datos en formato csv y los transforman en json. También se utiliza este mismo procedimiento para las imágenes.
25	Describa el procedimiento de generacion de credenciales o ids de acceso			Cubre el objetivo 3 Las credenciales se generan con un software del proveedor MSA , y se imprima y vienen troqueladas y genera el chip.
26	El sistema de archivos del sistema operativo está cifrado?		NO	Cubre el objetivo 3 Por tema de rendimiento y por transparencia.
27	Se mantienen ambientes de desarrollo, pruebas, capacitación, soporte y producción del software desarrollado?	SI		Desarrollo, pruebas, y el producción.

Firma y sello

Cargo

Nombre Empresa

Lugar y fecha



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



CUESTIONARIO SOBRE LA REVISIÓN DE PROCESOS

Objetivo General: Revisión de los procesos de capacitación, soporte técnico, carga de datos, validación de pantallas, aceptación y sellado de versiones, distribución de software, procesos en mesa antes durante y después de las elecciones, verificación de autenticidad del software y revisión de manuales técnicos del sistema, de procedimientos, de capacitación para miembros de mesa, soporte técnico y electorado en general.

Objetivos Específicos:

- Evaluar el alcance y amplitud del manual del sistema.
- Evaluar la documentación de características funcionales y no funcionales del sistema.
- Evaluar los procedimientos para la carga de los datos de la elección.
- Evaluar los procedimientos para la verificación y validación de las pantallas.
- Evaluar los procedimientos para la verificación de la autenticidad del software a utilizar.
- Evaluar los procedimientos para la distribución y personalización del software a utilizar en cada mesa de votación.
- Evaluar los procedimientos de despliegue y repliegue de las máquinas de votación.
- Evaluar los procedimientos de almacenamiento, distribución y custodia de las máquinas.
- Evaluar los Procedimientos de soporte técnico.
- Evaluar el alcance y amplitud de los manuales de capacitación al electorado.
- Evaluar los procedimientos y herramientas de capacitación al electorado.
- Evaluar el alcance y amplitud de los manuales de capacitación de las autoridades de mesa.
- Evaluar los procedimientos y herramientas de capacitación a las autoridades de mesa.
- Evaluar el alcance y amplitud de los manuales de capacitación al personal técnico de soporte en campo y remoto.
- Evaluar los procedimientos y herramientas de capacitación del personal técnico de soporte en campo y remoto.
- Evaluar los procedimientos y herramientas de capacitación de los operadores técnicos de los sistemas de transmisión, recuento y publicación de resultados

No.	Concepto	SI	NO	Cantidades/Detalles/ Observaciones / Fuentes de Información
	I. PROCESOS			
1	¿Existe un manual (para los dos (2) modelos) para usar la máquina de votación?	Si		Se tienen los documentos Manual de



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



CUESTIONARIO SOBRE LA REVISIÓN DE PROCESOS

				P4_2023 y Manual de P6_2023 en los cuales están descritas las partes, funcionalidades y soluciones a las incidencias con respecto al uso de los dos modelos de máquinas utilizados durante el proceso electoral.
2	¿Están actualizado los manuales del sistema de votación electrónica?	Si		La documentación referente al proceso electoral con el sistema de votación electrónica ha sido actualizada y existen manuales de procesos y manuales de usuario que explican a detalle este sistema
3	¿Existe documentación del proceso de votación en el que se incluya el uso de la máquina de votación electrónica?	Si		Existen los documentos Manual de soporte técnico, Manual de Procedimientos para capacitación, preparación, distribución y recolección de las máquinas de votación, materiales, documentos y útiles electorales, Manual De Funciones de Miembros de Mesa Receptora de Votos Y Agentes Electorales, entre otros.
4	¿Existe la documentación en la que se detalla el proceso para el registro de información de los datos de la elección (distributivo electoral, candidaturas, imágenes, etc) ?	Si		El documento "Procesos tecnológicos DTIC 2023" describe el procedimiento a seguir para el intercambio de datos electorales



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



CUESTIONARIO SOBRE LA REVISIÓN DE PROCESOS

				necesarios para los ajustes del software de votación y capacitación.
5	¿Existe documentación del proceso de control de calidad de las interfaces que presenta el software de votación?	Si		En el documento "Procesos tecnológicos DTIC 2023" Esta el Procedimiento para la auditoria de pantallas el cual es aplicado como una actividad dentro del cronograma electoral.
6	¿Existe un proceso de verificación de la autenticidad del software a utilizar y su cadena de custodia?	Si		Existe el procedimiento para la generación del hash para el sellado del software de votación y la generación de medios – discos Master, el cual es aplicado como una actividad dentro del cronograma electoral.
7	¿Existe un proceso detallado de la creación y distribución de las credenciales utilizadas por el sistema de votación?	Si		En el documento "Procesos tecnológicos DTIC 2023" Esta el Procedimiento de Generación de Medios ópticos Oficiales, el cual describe la creación de las credenciales utilizadas por el sistema de votación. En el Documento "Manual de Procedimientos para capacitación, preparación, distribución y recolección de las máquinas de votación, materiales, documentos y útiles electorales" se registra el procedimiento



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



CUESTIONARIO SOBRE LA REVISIÓN DE PROCESOS

				para la distribución de las credenciales oficiales.
8	¿Existe un procedimiento para el despliegue y repliegue de las máquinas de votación durante el proceso de capacitación a la ciudadanía?	Si		El documento “Manual de Procedimientos para capacitación, preparación, distribución y recolección de las máquinas de votación, materiales, documentos y útiles electorales”, describe a detalle el proceso de despliegue y repliegue de todo el material electoral, incluidas las máquinas de votación tanto en el proceso electoral como en el de capacitación.
9	¿Existe un procedimiento documentado del armado del kit técnico electoral (máquina de votación, boletas, credenciales y software de votación) , su despliegue y repliegue?	Si		En el documento “Manual de Procedimientos para capacitación, preparación, distribución y recolección de las máquinas de votación, materiales, documentos y útiles electorales”, se describe el procedimiento para el armado del Kit técnico y su distribución.
10	¿Existe la documentación necesaria para la capacitación del personal de soporte técnico?	Si		El documento “Manual de Soporte Técnico” describe a detalle las funciones que debe cumplir el personal técnico, además de los manuales de las máquinas p4 y p6 en los que se explica el manejo



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



CUESTIONARIO SOBRE LA REVISIÓN DE PROCESOS

				a detalle de las máquinas de votación.
11	¿Se implementaron herramientas adicionales para la capacitación del proceso electoral al personal técnico?	Si		Para la capacitación del personal técnico se crearon Foros virtuales y videos de capacitación , además de que se creó material para procesos de capacitación online
12	¿Se implementaron herramientas adicionales para la capacitación del ciudadano en el proceso electoral?	Si		Para la capacitación a la ciudadanía se desarrollaron Simuladores WEB para el uso de las máquinas de votación
13	¿Existe documentación para la capacitación de los miembros de las mesas electorales?	Si		El documento “Manual de Funciones Miembros de Mesa Receptora de Votos y Agentes Electorales” describe las funciones que debe cumplir a detalle los miembros de las mesas electorales.
14	¿Se implementaron herramientas adicionales para la capacitación en los procesos electorales a los miembros de mesa?	Si		Se crearon videos de capacitación en el que se indica las funciones que deben cumplir los miembros de mesa y su interacción con la maquina de votación.
15	¿Existe documentación del proceso de cierre de mesa y escrutinio con la máquina de votación?	Si		El documento “Manual de Funciones Miembros de Mesa Receptora de Votos y Agentes Electorales” describe el proceso de cierre de mesa el proceso de escrutinio con la maquina de votación. Información adicional también se encuentra en



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



CUESTIONARIO SOBRE LA REVISIÓN DE PROCESOS

				el documento "Manual de Soporte Técnico"
16	¿Existe un procedimiento documentado para la transmisión de los resultados electorales de mesa?	Si		En el documento "Manual CTX -TREP" se describe a detalle el proceso de transmisión de los resultados electorales de mesa.

Firma y sello

Cargo

Nombre Empresa

Lugar y fecha



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



CUESTIONARIO SOBRE LA REVISIÓN DEL HARDWARE

Objetivo General: Revisión detallada de la arquitectura de las máquinas de votación, análisis documental de su diseño, componentes y funcionamiento. Revisión física y pruebas de cada modelo, incluye verificación de diseño, aislamiento de la máquina, tipos de almacenamiento, tecnología RFID, registro y seguridad, entre otros.

Objetivos Específicos:

- Evaluar el diseño y construcción para las condiciones particulares de exigencia del proceso electoral.
- Evaluar una operación aislada de cualquier tipo de conectividad con el exterior durante el proceso de votación.
- Evaluar la garantía de voto secreto, sin almacenar información relacionada con el voto de cada elector.
- Evaluar la garantía de integridad (no alteración) de la información de votos registrados electrónicamente durante todo el proceso electoral.
- Evaluar las Condiciones para la continuidad de la operación durante toda la jornada electoral.
- Evaluar el registro electrónico utilizado no admita lectura a distancia.

No.	Concepto	SI	NO	Cantidades/Detalles/ Observaciones / Fuentes de Información
	I. HARDWARE			
1	¿Se almacena la información en la máquina de votación? (2 modelos)		NO	No tienen dispositivo de almacenamiento permanente
2	¿La máquina de votación cuenta con un medio interno de almacenamiento de información?		NO	Todo el sistema operativo y aplicativo se cargan al momento desde un DVD
3	¿La máquina de votación cuenta con un sistema operativo?		No	El sistema operativo se carga desde un DVD
4	¿La máquina de votación cuenta con doble fuente de poder de energía para garantizar una alta disponibilidad?		NO	Tiene una (1) fuente de alimentación
5	¿Hay algún tipo de seguro físico para evitar el acceso al botón de encendido y el acceso a la unidad de dvd?		NO	No tiene un seguro físico.

CUESTIONARIO SOBRE LA REVISIÓN DEL HARDWARE

6	¿La estructura física del equipo tiene protección ante vandalismo o sabotaje?		NO	La maquina de votación cuenta con protección contra caídas.
7	¿Cuánta con algún método para evitar la interceptación de las tarjetas RFID para que no exista escritura, modificación o borrado de las boletas a distancia?	SI		Protección pasiva es la jaula que la rodea alrededor a las antenas, Un jammer incorporado que emite una señal en la misma frecuencia de funcionamiento del RFID interno con una potencia superior 100 veces mayor.
8	En los puertos USB y ethernet que se tienen en los equipos y no serán usados en el proceso electoral de Paraguay, ¿están bloqueados de alguna forma?	Si		En la máquina P6 el bloqueo seda en 2 formas: 1: cortados físicamente a través de llaves electrónicas y 2: El sistema operativo no monta las librerías, no carga los drivers, tiene una whitelist
9	¿Dispone de estándares eléctricos en aspectos como, conectores, ahorro de energía, etc? ¿Cuáles?	Si		La fuente esta certificada.
10	¿Se dispone de accesibilidad para personas con discapacidad visual reducida o nula?	Si		Visual: reducción visual de alto contraste, visión nula el módulo de votación asistida.
11	¿Se dispone de respaldo de energía? ¿De cuál forma está diseñado y cuanto es la duración estimada?	SI		Doble respaldo, o redundante, 12 horas de autonomía de la máquina de votación. habiendo realizado 400 votos
12	¿Por medio de hardware existe algún chip que controle el cifrado o que genere el cifrado para el manejo de llaves u otros datos sensibles que se carguen del software?	SI		Tiene 2 tipos: 1: TPM 2.1 y 2: el SE050 en sistemas embebidos. pero no se utilizan, porque las llaves de cifrado son creadas previamente en un entorno controlado.



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



CUESTIONARIO SOBRE LA REVISIÓN DEL HARDWARE

13	¿Existe alguna utilidad en el firmware del uefi que haga las pruebas necesarias del hardware?		NO	Tienen a nivel del aplicativo.
14	¿Existen controles para evitar fallas en la selección de candidatos en la pantalla touch? ¿Cuáles?	SI		Siempre en el encendido del equipo se realiza la calibración de la pantalla, posterior a eso se tiene una característica de control "antiblinking" que evita que el votante se equivoque cuando toque un punto varias veces seguidas.
15	¿El proceso de actualización de firmware tiene controles de seguridad ante fallas?	SI		El diseño del hardware permite mantener una copia anterior y cargas parciales del firmware si falla, permitiendo que, aunque falle la actualización del firmware el equipo pueda seguir operando y recuperarse ante la falla.

Firma y sello

Cargo

Nombre Empresa

Lugar y fecha

PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

Objetivo General: Revisión detallada del diseño de software, documentación técnica, documentación de usuario, casos de uso, casos de prueba, QA, sistema operativo, parametrización, control de versiones, control de cambios, custodia de código, pruebas y simulacros.

Objetivos Específicos:

- Evaluar los procedimientos de diseño, desarrollo y versionado son adecuados.
- Evaluar que los aplicativos desarrollados se encuentren individualizados e identificados en un catálogo que permite validar su integridad.
- Evaluar los esquemas y estándares de seguridad utilizados.
- Evaluar que las capacidades de parametrización se adecúan a los requerimientos.
- Evaluar que se realice una adecuada gestión y control de cambios.
- Evaluar los procesos de control de calidad y pruebas.
- Evaluar que los casos de uso estén completos, detallados y acordes a las necesidades del proceso.
- Evaluar que los casos de prueba sean exhaustivos y estén acordes a los casos de uso.
- Evaluar el análisis de los sistemas desde una perspectiva de desarrollo de software, de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.
- Evaluar la integridad y la consistencia de los datos, de la información transmitida desde las máquinas de votación a las boletas de votación.

Nombre o Tipo de Prueba Realizada:

Prueba de consistencia de datos almacenados en la boleta

Objetivo de la Prueba	Descripción de la Prueba:
• Constatar el contenido del chip marca ST en los bloques del 63 a 79. • Validar que una vez utilizada una boleta con firma digital del fabricante los bloques del 63 al 79 se reinician en ceros.	La prueba inicia con analizar el contenido del datasheet del fabricante del chip ST FRID EEPROM (ST25TVcccX) en el cual se indica que los bloques del 63 al 79 son utilizados por la empresa ST para almacenar una firma digital que permita para quienes adquieran el chip poder validar su autenticidad. Esta firma es específica para cada chip porque utiliza el ID del chip para formar esa firma digital.

PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

	Para esto se requiere acceder a un documento del fabricante (para el cual se requiere firmar un NDA), en el cual se indican las instrucciones que permiten acceder al contenido de los bloques del 63 al 79. Por medio de un script de Python se implementan esas instrucciones y se puede validar en contenido, tanto en hexadecimal como en código ASCII de lo que está almacenado en forma inicial en el chip. Estos datos pueden compararse con el contenido del chip por medio de alguna aplicación, en nuestra prueba utilizando NFC Reader en sistema operativo Android. También se realizó la prueba con una boleta que contaba con firma digital del fabricante en los bloques del 63 al 79. En esta prueba se utilizó la boleta para realizar una votación y validar que una vez que se confirmaron las elecciones del elector, se pudo constatar en el código de la aplicación que además cada bloque es inicializado en cero antes de grabar el voto. El contenido del voto se guarda encriptado en el chip en los bloques del 1 al 13 y que los bloques del 63 al 79 se reinician en cero. Se verifica que el elector en este modo también puede confirmar la selección guardada en el Chip e impresa en la boleta, introduciendo la boleta nuevamente en la ranura de la impresora y el sistema procederá con la lectura de lo que se guardó en el chip RFID.
Resultados de la prueba: Mediante esta prueba se comprobó el contenido de los bloques 63 al 79 de los chips del fabricante ST son los mismos según una aplicación de un tercero comparados con los del script generado con las especificaciones del fabricante.	



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**

PRUEBA SOBRE LA REVISIÓN DEL SOFTWARE

También se pudo comprobar una vez que se ha emitido el voto, todos los bloques se reinician en cero y además se marcan como escritos para que no puedan ser modificados.

Las pruebas realizadas fueron satisfactorias y se ejecutaron sin contratiempos.

Firma y sello

Cargo

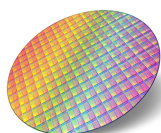
Nombre Empresa

Lugar y fecha

NFC Type 5 / RFID tag IC with up to 2.5 Kbits of EEPROM, product identification and protection



UDFPN5
1.7 x 1.4 mm



Wafer



Product status link

[ST25TV02KC](#)

[ST25TV512C](#)

Features

Includes ST state-of-the-art patented technology

Contactless interface

- Compliant with ISO/IEC 15693
- NFC Forum Type 5 tag certified by the NFC Forum
- Supports all ISO/IEC 15693 modulations, coding, subcarrier modes, and data rates up to 26 Kbit/s
- Single block reads and writes, multiple block reads
- Internal tuning capacitance: 23 pF or 99.7 pF

Memory

- Up to 2560 bits (320 bytes) of EEPROM
- Accessible by blocks of four bytes
- Write time from RF: typical 5 ms per block
- Data retention: 60 years at 55°C
- Minimum endurance: 100k write cycles
- 3-digit unique tap code
- Augmented NDEF (contextual automatic NDEF message)

Data protection

- User memory configurable in one or two areas:
 - in single area mode, access protectable by one 64-bit password
 - in flexible dual area mode, access protectable by two 32-bit passwords
- System configuration: access protected by a 32-bit password
- Permanent write lock of specific user area blocks
- Temporary write lock at user area level
- Permanent write lock of specific system configuration blocks

Product identification and protection

- Password features: cover coding, recovery, failed attempt counter
- Tamper detection capability with memorization of open/resealed events
- TruST25 digital signature

Privacy

- Configurable kill mode for permanent deactivation of the tag
- Untraceable mode with configurable responsiveness

Temperature range

- From -40 to 85 °C

Package

- 5-pin package, ECOPACK2 (RoHS compliant)
- Bumped and sawn wafer

1 Description

The **ST25TV02KC** and **ST25TV512C** devices are NFC/RFID tag ICs with an Augmented NDEF feature, a tamper detection interface, and specific modes to protect customer privacy.

The Augmented NDEF feature is a contextual automatic NDEF message service, allowing the tag to respond dynamic content without an explicit update of the EEPROM by the end-user.

The tamper detection interface is available on ST25TV02KC-T devices only. This interface is not available on ST25TV02KC-A and ST25TV512C devices.

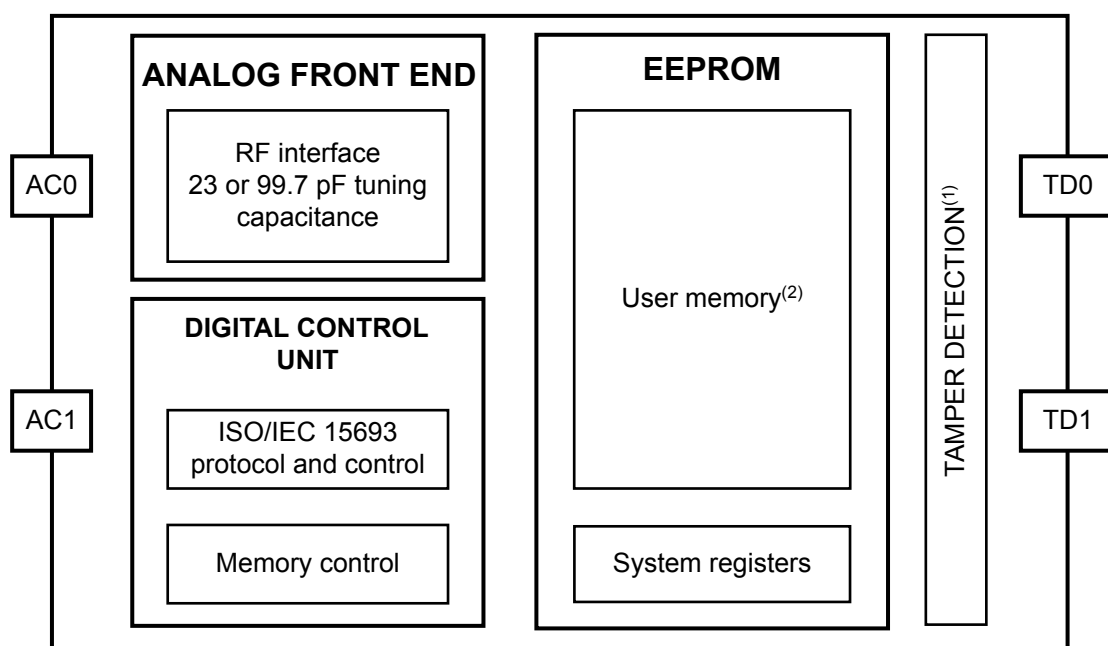
The ST25TV02KC and ST25TV512C devices hold a digital signature generated by TruST25 (a set of software and procedures) to prove the origin of the chip in cloning detection, embeds a configurable EEPROM with 60-year data retention, and can be operated from a 13.56 MHz long range RFID reader or an NFC phone.

The contactless interface is compliant with the ISO/IEC 15693 standard and NFC Forum Type 5 tag specification.

1.1 Block diagram

The ST25TV02KC and ST25TV512C (hereinafter, it is referred to as ST25TVxxxC) devices are depicted in the following block diagram:

Figure 1. ST25TVxxxC block diagram



1. The tamper detection interface is available on ST25TV02KC-T devices only.
2. Respectively 512 and 2560 bits on ST25TV512C and ST25TV02KC devices.

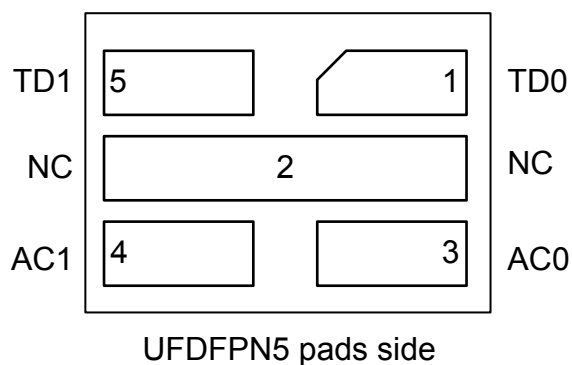
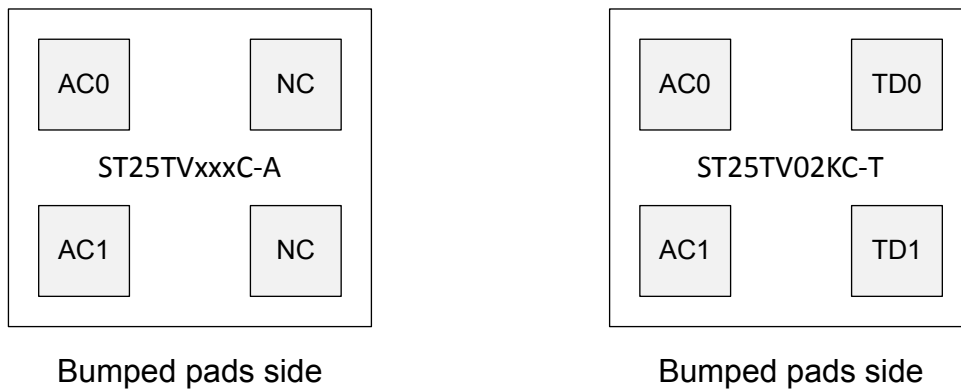
1.2 Package connections

ST25TV02KC and **ST25TV512C** are provided in two delivery forms:

- UDFPN5 package (ST25TV02KC-T devices only)
- Sawn and bumped wafer (ST25TV512C, ST25TV02KC-A and ST25TV02KC-T devices)

Table 1. Signal names

Signal name	Function	Direction
AC0	Antenna coils	In-out
AC1	Antenna coils	In-out
TD0	Tamper detection loop	In
TD1	Tamper detection loop	Out

Figure 2. UFDFPN5 package connections

Figure 3. Die connections for sawn and bumped wafer


2 Signal descriptions

2.1 Antenna coil (AC0, AC1)

These inputs are used to connect the ST25TVxxxC device to an external coil exclusively. It is advised not to connect any other DC or AC path to AC0 or AC1.

When correctly tuned, the coil is used to power and access the device using the ISO/IEC 15693 and ISO 18000-3 mode 1 protocols.

2.2 Tamper detection (TD0, TD1)

These inputs are used to connect a wire loop to the ST25TVxxxC device to detect an open or a short between the TD0 and TD1 pins.

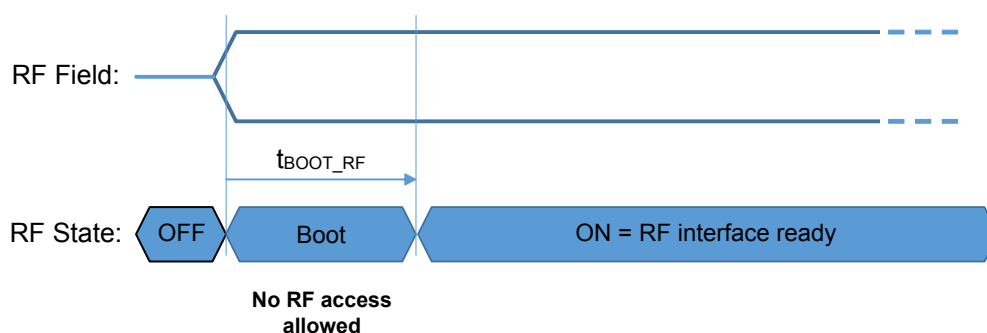
3 Power management

The ST25TVxxxC device is powered through its contactless interface.

3.1 Device set

To ensure a proper boot of the RF circuitry, the RF field must be turned ON without any modulation for a minimum period of time t_{BOOT_RF} (see Table 172. RF characteristics). During t_{BOOT_RF} , the ST25TVxxxC ignores all received RF commands (see Figure 4).

Figure 4. RF power-up sequence



3.2 Device reset

To ensure a proper reset of the RF circuitry, the RF field must be turned off (100% modulation) for a minimum t_{RF_OFF} amount of time (see Table 172. RF characteristics).

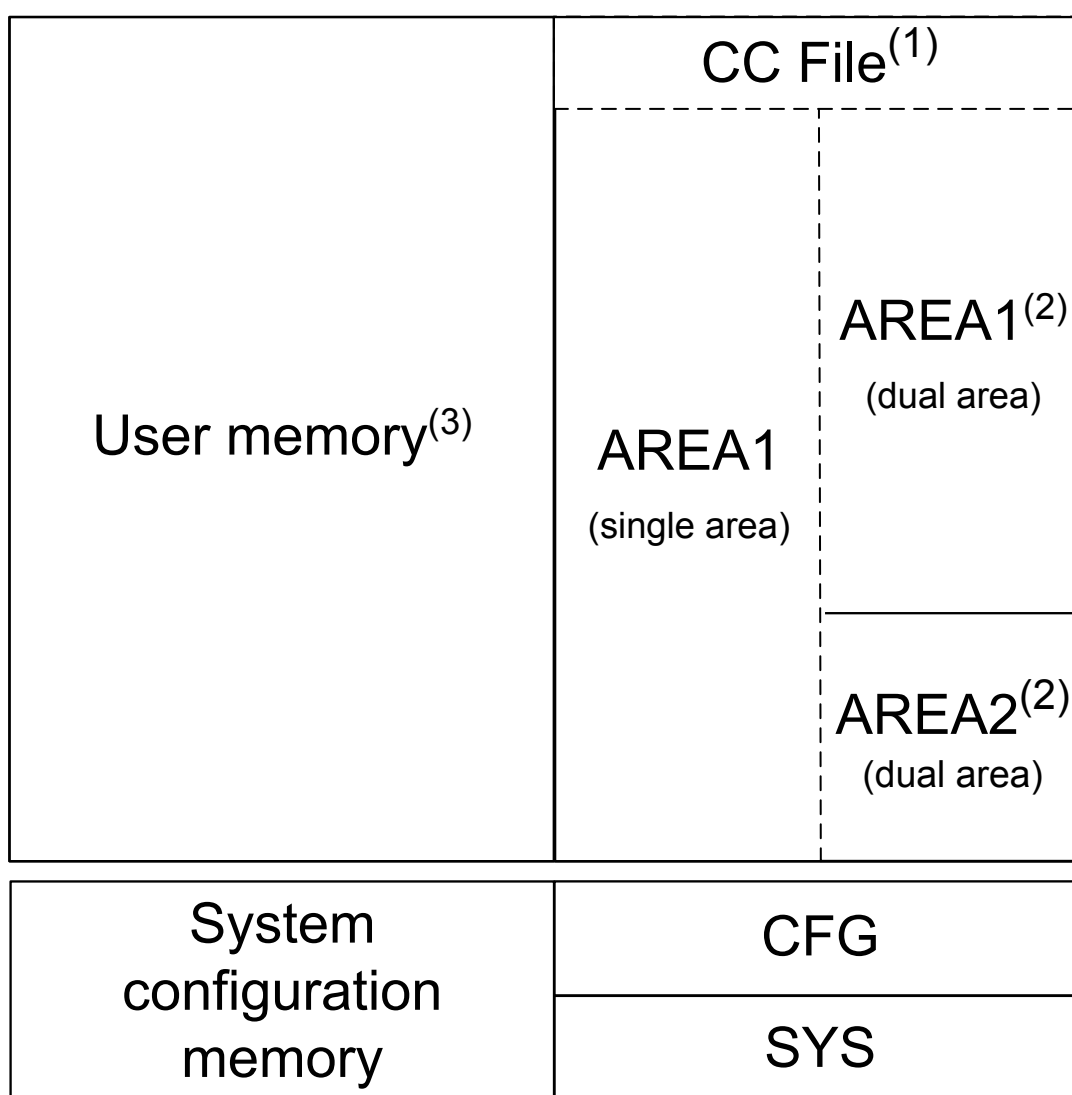
4 Memory management

4.1 Memory organization

The ST25TVxxxC memory is organized as follows:

- User memory: it can be configured in one or two different areas, as described in [Section 4.2 User memory](#). Those areas can be used for user data and NFC Forum Type 5 Capability Container (CC) if required.
- System configuration memory: it is composed of different registers, including the device configuration, the ISO15693 AFI and DSFID registers. It also contains the UID and different protection registers. Refer to [Section 4.3 System configuration memory](#) for more details

Figure 5. Memory organization



1. NFC Forum T5T CC file is coded on block 00h which is part of AREA1.
2. In dual area mode, the AREA1/AREA2 boundary can be configured with a block granularity.
3. Respectively 16 and 80 blocks of 32 bits for ST25TV512C and ST25TV02KC devices.

4.2 User memory

User memory is addressed as blocks (= pages) of 4 bytes, starting at address 0 and ending at address END_MEM. Value of END_MEM is 0Fh and 4Fh for ST25TV512C and ST25TV02KC devices respectively. The ST25TVxxxC user memory can be configured in single area (AREA1) or in dual area mode (AREA1 and AREA2) depending on the value of the END_A1 register at the start of a RF session (see [Table 2. User memory in single area mode](#), [Table 3. User memory in dual area mode](#) and [Table 13. END_A1 content](#)).

When the value of END_A1 is equal to END_MEM, the ST25TVxxxC user memory is configured in single area mode defined as follows:

- AREA1 starts at address 00h. It is composed of (END_MEM+1) blocks. It can be read- or readwrite-protected by a dedicated 64-bit password. AREA1 is dedicated to user data.

When the value of END_A1 is lower than END_MEM, the ST25TVxxxC user memory is configured in dual area mode defined as follows :

- AREA1 starts at address 00h. It is composed of (END_A1+1) blocks. It can be read- or readwrite-protected by a dedicated 32-bit password. AREA1 is dedicated to user data.
- AREA2 starts at address (END_A1+1). It is composed of (END_MEM-END_A1) blocks. It can be read- or readwrite-protected by a dedicated 32-bit password. AREA2 is dedicated to user data.

Block 00h belongs to AREA1, but can always be read regardless of the read-protection mode of AREA1. This block is dedicated to the CC file content defined by the NFC Forum Type 5 application. An application that does not need to comply with NFC Forum Type 5 specifications can use block 00h for any purpose.

Table 2. User memory in single area mode

RF command	Block address	Byte address				Comment
		LSByte	-	-	MSByte	
ReadSingleBlock ReadMultipleBlocks WriteSingleBlock	00h ⁽¹⁾	0000h	0001h	0002h	0003h	AREA1 ⁽²⁾
	01h	0004h	0005h	0006h	0007h	
	02h	0008h	0009h	000Ah	000Bh	
	...	...	...	...	...	
	END_MEM	END_MEM*4+0	END_MEM*4+1	END_MEM*4+2	END_MEM*4+3	

1. Block 00h is always readable

2. For single area mode, set the value of END_A1 register to END_MEM

Table 3. User memory in dual area mode

RF command	Block address	Byte address				Comment
		LSByte	-	-	MSByte	
ReadSingleBlock ReadMultipleBlocks WriteSingleBlock	00h ⁽¹⁾	0000h	0001h	0002h	0003h	AREA1 ⁽²⁾
	01h	0004h	0005h	0006h	0007h	
	02h	0008h	0009h	000Ah	000Bh	
	...	...	...	...	...	
	END_A1	END_A1*4+0	END_A1*4+1	END_A1*4+2	END_A1*4+3	
	END_A1+1	END_A1*4+4	END_A1*4+5	END_A1*4+6	END_A1*4+7	AREA2 ⁽²⁾
	...	...	...	...	...	
	END_MEM	END_MEM*4+0	END_MEM*4+1	END_MEM*4+2	END_MEM*4+3	

1. Block 00h is always readable

2. For dual area mode, set value of END_A1 register between 00h and (END_MEM-1)

4.3 System configuration memory

In addition to user memory, ST25TVxxxC includes a set of registers located in the system configuration memory. Registers are read during the boot sequence and define basic ST25TVxxxC behaviour.

4.3.1 System configuration registers

Table 4. List of configuration registers lists the configuration registers of the ST25TVxxxC device. They are accessed with the ReadConfiguration and WriteConfiguration commands and two arguments FID and PID, respectively acting as a feature identifier and a parameter identifier.

The write access to the configuration registers is protected by the CONFIG security session which is opened by a successful presentation of the PWD_CFG password (see Section 5.1.2 Password management).

Configuration registers are grouped by FID value. The write access to a group of registers may be permanently locked.

Depending on the configuration register, its read access is either always granted or protected with the same mechanisms as its write access.

Depending on the configuration register, when its content is updated during a RF session, the effect of the new value is activated either immediately or at the start of the next RF session.

Table 4. List of configuration registers

Name	FID	PID	Bytes	Read ⁽¹⁾	Write ⁽²⁾	Activation time ⁽³⁾	Section
RW_PROTECTION_A1	00h	00h	1	Y	W	B	Section 5.1.1
END_A1	00h	01h	1	Y	W'	B	Section 5.1.1
RW_PROTECTION_A2	01h	00h	1	Y	W	B	Section 5.1.1
UTC_EN	02h	00h	1	Y	W	B	Section 5.2.1
UTC	02h	01h	3	Y	N	-	Section 5.2.1
TD_EVENT_UPDATE_EN ⁽⁴⁾	03h	00h	1	Y	W	B	Section 5.3.1
TD_SEAL_MSG ⁽⁴⁾	03h	01h	2	R	W	I	Section 5.3.1
TD_UNSEAL_MSG ⁽⁴⁾	03h	02h	2	R	W	I	Section 5.3.1
TD_RESEAL_MSG ⁽⁴⁾	03h	03h	2	R	W	I	Section 5.3.1
TD_SHORT_MSG ⁽⁴⁾	03h	04h	1	R	W	I	Section 5.3.1
TD_OPEN_MSG ⁽⁴⁾	03h	05h	1	R	W	I	Section 5.3.1
TD_STATUS ⁽⁴⁾	03h	06h	3	Y	N	-	Section 5.3.1
ANDEF_EN	04h	00h	1	Y	W	B	Section 5.4.1
ANDEF_CFG	04h	01h	2	Y	W	B	Section 5.4.1
ANDEF_SEP	04h	02h	1	R	W	I	Section 5.4.1
ANDEF_CUSTOM_LSB	04h	03h	4	R	W	I	Section 5.4.1
ANDEF_CUSTOM_MSB	04h	04h	4	R	W	I	Section 5.4.1
PRIVACY	05h	00h	1	Y	W	B	Section 5.5.1
AFI_PROT	08h	00h	1	Y	W	B	Section 5.7.1
REV	FEh	00h	1	Y	N	-	Section 5.9
UID	FEh	01h	8	Y	N	-	Section 5.9
LCK_CONFIG	FFh	00h	2	Y	W''	I	Section 5.1.1

1. Y: read access not protected, R: read access granted if LCK_CONFIG[FID]=0b and CONFIG security session open

2. N: write access not available, W: write access granted if LCK_CONFIG[FID]=0b and CONFIG security session open, W': write access granted if LCK_CONFIG[1:0]=00b and CONFIG security session open, W'': write access granted if CONFIG security session open

3. B: update is effective on next RF boot sequence, I: update is effective immediately

4. Registers with FID=03h are available only on ST25TV02KC-T devices (see section 10)

4.3.2 System registers

Table 5 lists the system registers of the ST25TVxxxC device. They are accessed with other RF commands than ReadConfiguration and WriteConfiguration.

When the write access to a system register is available, it may be protected by a password and/or a lock mechanism.

When the read access to a system register is available, it is always granted through the relevant RF command.

When the content of a system register is updated, the effect of the new value is activated immediately.

Table 5. List of system registers

Name	Bytes	Read ⁽¹⁾	Write ⁽²⁾	Activation time	Section
LCK_BLOCK	10	R	W	I	Section 5.1.1
LCK_DSFDID	1	N	W	I	Section 5.9
LCK_AFI	1	N	W	I	Section 5.9
DSFDID	1	Y	W	I	Section 5.9
AFI	1	Y	W	I	Section 5.9
IC_REF	1	Y	N	-	Section 5.9
UID	8	Y	N	-	Section 5.9
ANDEF_UID	16	Y	N	-	Section 5.4.1
KILL_CMD	1	N	W	I	Section 5.5.1
UNTR_CMD	1	N	W	I	Section 5.5.1
RND_NUMBER	2	Y	N ⁽³⁾	-	Section 5.1.1
PWD_CFG	4	N	W	I	Section 5.1.1
PWD_A1	4	N	W	I	Section 5.1.1
PWD_A2	4	N	W	I	Section 5.1.1
PWD_UNTR	4	N	W	I	Section 5.1.1

1. Y: read access granted without condition, R: read access granted with condition

2. N: write access not available, W: write access granted with condition

3. The content of the RND_NUMBER register is updated internally on a successful GetRandomNumber request

5 Specific features

ST25TVxxxC offers the following features:

- [Section 5.1 Data protection](#)
- [Section 5.2 Unique tap code](#)
- [Section 5.3 Tamper detection](#)
- [Section 5.4 Augmented NDEF](#)
- [Section 5.5 Consumer privacy protection](#)
- [Section 5.6 TruST25 digital signature](#)
- [Section 5.7 AFI protection](#)
- [Section 5.8 Inventory Initiated](#)

The features from [Section 5.1](#) to [Section 5.7](#) can be programmed by accessing registers of the ST25TVxxxC using the ReadConfiguration and WriteConfiguration commands. Update of configuration registers is only possible when the access right has been granted by presenting the configuration password (PWD_CFG), and if the configuration of the feature was not previously locked (see register LCK_CONFIG).

Depending on the configuration register, the effect of a valid write access may be applied immediately or during the boot sequence of the next RF session.

An additional set of registers allows to identify and customize the product (see [Section 5.9 Device identification registers](#)).

5.1 Data protection

ST25TVxxxC provides a special data protection mechanism based on passwords that unlock security sessions.

Read and/or write access to the user memory can be protected. Write access to the configuration registers is always protected. Read access to some configuration registers is protected.

Other lock mechanisms are supported (LockBlock, lock by feature), as described in this section.

5.1.1 Data protection registers

Table 6. LCK_CONFIG access

RF Command	Access type
ReadConfiguration @(FID=FFh, PID=00h)	R : always possible
WriteConfiguration @(FID=FFh, PID=00h)	W : if the CONFIG security session is open
	W effective time : immediate

Table 7. LCK_CONFIG content

Bit	Name	Function	Factory value
b0	LCK_A1	0: configuration registers with FID=00h are not locked 1: configuration registers with FID=00h are locked	0b
b1	LCK_A2	0: configuration registers with FID=01h are not locked 1: configuration registers with FID=01h are locked	0b
b2	LCK_UTC	0: configuration registers with FID=02h are not locked 1: configuration registers with FID=02h are locked	0b
b3	LCK_TD	0: configuration registers with FID=03h are not locked 1: configuration registers with FID=03h are locked	0b
b4	LCK_ANDEF	0: configuration registers with FID=04h are not locked 1: configuration registers with FID=04h are locked	0b
b5	LCK_PRIV	0: configuration registers with FID=05h are not locked 1: configuration registers with FID=05h are locked	0b
b7-b6	RFU	-	00b
b8	LCK_AFIP	0: configuration registers with FID=08h are not locked 1: configuration registers with FID=08h are locked	0b
b15-b9	RFU	-	0000000b

Note: Refer to [Table 4. List of configuration registers for the LCK_CONFIG register](#).

If value 1b is issued for a field already set to 1b, the WriteConfiguration command has no effect and error 11h shall be responded.

Otherwise, if value 0b is issued for a field set to 1b, the corresponding feature remains locked and no errorcode is responded to the WriteConfiguration command.

Table 8. LCK_BLOCK access

RF Command	Access type
ReadSingleBlock	R : if Option_flag=1 and write access to parent area is allowed ⁽¹⁾
ReadMultipleBlocks	R : if Option_flag=1 and write access to parent area is allowed ⁽¹⁾
GetMultipleBlockSecurityStatus	R : if write access to parent area is allowed ⁽¹⁾
LockBlock	W : if not already locked and write access to parent area is allowed
-	W effective time : immediate

1. When the write access to an area is not allowed (write access forbidden, or protected with closed security session), then the value of LCK_BLOCK is masked by 1 in a BSS field (see sections [Section 6.4.3 ReadSingleBlock](#), [Section 6.4.6 ReadMultipleBlocks](#) and [Section 6.4.14 GetMultipleBlockSecurityStatus](#))

Table 9. LCK_BLOCK content

Bit	Name	Function	Factory Value
b79-b0	LCK_BLOCK	For each bit b_N : 0: write access of block N not locked 1: write access of block N permanently	0

Note: Refer to [Table 5. List of system registers for the LCK_BLOCK register](#).

Table 10. RW_PROTECTION_A1 access

RF Command	Type
ReadConfiguration @(FID=00h, PID=00h)	R : always possible
WriteConfiguration @(FID=00h, PID=00h)	W : if the CONFIG security session is open and LCK_A1=0b
	W effective time : on next RF boot sequence

Table 11. RW_PROTECTION_A1 content

Bit	Name	Function	Factory Value
b1-b0	RW_PROTECTION_A1	AREA1 access rights (except block 00h): 00: read always allowed / write always allowed 01: read always allowed / write allowed if AREA1 security session is open 10: read allowed if AREA1 security session is open / write allowed if AREA1 security session is open 11: read allowed if AREA1 security session is open / write forbidden Block 00h access rights: read always allowed 00: write always allowed 01: write allowed if AREA1 security session is open 10: write allowed if AREA1 security session is open 11: write forbidden	00b
b7-b2	RFU	-	000000b

Note: Refer to Table 4. List of configuration registers for the RW_PROTECTION_A1 register.

Table 12. END_A1 access

RF command	Access type
ReadConfiguration @(FID=00h, PID=01h)	R : always possible
WriteConfiguration @(FID=00h, PID=01h)	W : if the CONFIG security session is open and LCK_A1=LCK_A2=0b
	W effective time : on next RF boot sequence

Table 13. END_A1 content

Bit	Name	Function	Factory Value
b7-b0	END_A1	Number of the last block belonging to AREA1. When lower than END_MEM, user memory is split in two areas : - AREA1 (blocks 00h to END_A1) - AREA2 (blocks END_A1 + 1 to END_MEM). Otherwise user memory contains a single area : AREA1 (blocks 00h to END_MEM)	END_MEM ⁽¹⁾

1. END_MEM value is 0Fh / 4Fh for ST25TV512C / ST25TV02KC devices respectively.

Note: Refer to Table 4. List of configuration registers for the END_A1 register.

Table 14. RW_PROTECTION_A2 access

RF command	Access type
ReadConfiguration @(FID=01h, PID=00h)	R : always possible
WriteConfiguration @(FID=01h, PID=00h)	W : if the CONFIG security session is open and LCK_A2=0b
	W effective time : on next RF boot sequence

Table 15. RW_PROTECTION_A2 content

Bit	Name	Function	Factory Value
b1-b0	RW_PROTECTION_A2	AREA2 access rights: 00: read always allowed / write always allowed 01: read always allowed / write allowed if AREA2 security session is open 10: read allowed if AREA2 security session is open / write allowed if AREA2 security session is open 11: read allowed if AREA2 security session is open / write not allowed	00b
b7-b2	RFU	-	000000b

Note: Refer to [Table 4. List of configuration registers for the RW_PROTECTION_A2 register](#).

Table 16. PWD_CFG access

RF command	Access type
-	R: no read access
WritePassword @PID=00h	W: if the CONFIG security session is open
	W effective time: immediate

Table 17. PWD_CFG content

Bit	Name	Function	Factory Value
b31-b0	PWD_CFG	Password for access to configuration registers and Kill command	00000000h

Note: Refer to [Table 5. List of system registers for the PWD_CFG register](#).

Table 18. PWD_A1 access

RF command	Access type
-	R : no read access
WritePassword @PID=01h	W : if AREA1 security session is open
	W effective time : immediate

Table 19. PWD_A1 content

Bit	Name	Function	Factory Value
b31-b0	PWD_A1_LSB	Password for access to AREA1	00000000h
b63-b32	PWD_A1_MSB ⁽¹⁾	In single area mode, bits 0 to 63 are used. In dual area mode only bits 0 to 31 are used	00000000h

1. PWD_A1_MSB is an alias of register PWD_A2:

- when switching from dual to single area mode, the value of PWD_A1_MSB is the latest known value of PWD_A2
- when switching from single to dual area mode, the value of PWD_A2 is the latest known value of PWD_A1_MSB

Note: Refer to [Table 5. List of system registers for the PWD_A1 register.](#)

Table 20. PWD_A2 access

RF command	Access type
-	R : no read access
WritePassword @PID=02h	W : if AREA2 security session is open
	W effective time : immediate

Table 21. PWD_A2 content

Bit	Name	Function	Factory Value
b31-b0	PWD_A2 ⁽¹⁾	Password for access to AREA2	00000000h

1. PWD_A1_MSB is an alias of register PWD_A2:

- when switching from dual to single area mode, the value of PWD_A1_MSB is the latest known value of PWD_A2
- when switching from single to dual area mode, the value of PWD_A2 is the latest known value of PWD_A1_MSB

Note: Refer to [Table 5. List of system registers for the PWD_A2 register.](#)

Table 22. PWD_UNTR access

RF command	Access type
-	R : no read access
WritePassword @PID=03h	W : if UNTR security session is open
	W effective time : immediate

Table 23. PWD_UNTR content

Bit	Name	Function	Factory Value
b31-b0	PWD_UNTR	Password used with ToggleUntraceable command	00000000h

Note: Refer to [Table 5. List of system registers for the PWD_UNTR register.](#)

Table 24. RND_NUMBER access

RF command	Access type
GetRandomNumber	R : always possible
-	W : no write access ⁽¹⁾

1. the content of the RND_NUMBER register is updated internally on a successful GetRandomNumber command.

Table 25. RND_NUMBER content

Bit	Name	Function	Factory value
b15-b0	RND_NUMBER	16-bit random number	N/A

Note: Refer to Table 5. List of system registers for the RND_NUMBER register.

5.1.2 Password management

ST25TVxxxC provides protection of user and system configuration memories. Access to groups of data are controlled by security sessions based on passwords. On successful (respectively failed) presentation of a password, a security session is open (respectively closed) and grants (respectively denies) access to the protected group of data.

Table 26. Security session type

Security session	Open by presenting	Rights granted when session is open
CONFIG	PWD_CFG	Access to configuration registers Update of PWD_CFG
AREA1	PWD_A1	Access to blocks from AREA1 in user memory Update of PWD_A1
AREA2	PWD_A2	Access to blocks from AREA2 in user memory Update of PWD_A2
UNTR	PWD_UNTR	Update of PWD_UNTR

Each of the PWD_CFG and PWD_UNTR passwords is 32-bit long.

In dual area mode (END_A1 < END_MEM), each of the PWD_A1 and PWD_A2 passwords is 32-bit long.

In single area mode (END_A1 = END_MEM), the PWD_A1 password is 64-bit long, and AREA2 security session is not applicable: password commands fail with password identifier 02h when single area mode is used.

Note: In addition to the security session mechanism described in this section, the PWD_CFG and PWD_UNTR passwords are respectively used with the Kill and ToggleUntraceable commands.

Table 27. List of password registers

Password	Password_id	Password_data size
PWD_CFG	00h	4 bytes
PWD_A1	01h	4 bytes if END_A1 < END_MEM
		8 bytes if END_A1 = END_MEM
PWD_A2	02h	4 bytes if END_A1 < END_MEM
		Invalid request if END_A1 = END_MEM
PWD_UNTR	03h	4 bytes

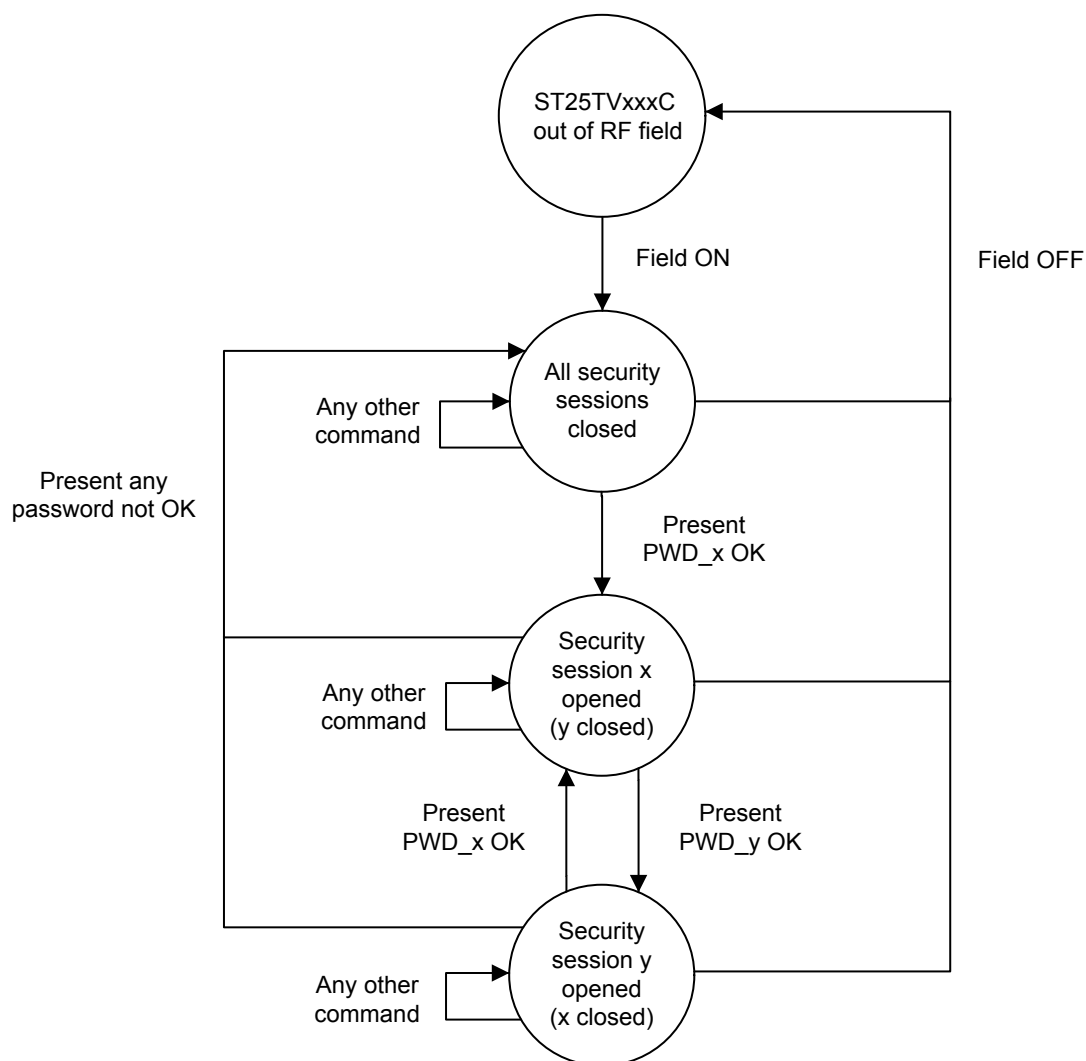
The ST25TVxxxC passwords management is based on three commands:

- WritePassword (see [Section 6.4.18 WritePassword](#))
- PresentPassword (see [Section 6.4.19 PresentPassword](#))
- GetRandomNumber (see [Section 6.4.24 GetRandomNumber](#))

For any of the 4x passwords available, three actions are possible:

- **Open Security Session:**
 - Use GetRandomNumber command if needed
 - Use PresentPassword command with corresponding password identifier and valid encrypted password value (see [Section 5.1.4 User memory protection](#))
- **Update Password:**
 - While the security session for the corresponding password is open, use WritePassword command with same password identifier and the new encrypted password value (see [Section 5.1.4 User memory protection](#)).
- **Close Security Session:**
 - To close the security session corresponding to a password identifier, user can choose one of the following options:
 - Remove tag from RF field
 - Use PresentPassword command with same password identifier and an invalid password value
 - Open a security session corresponding to a different password identifier. Opening a new security session automatically closes the previously opened one (even if the open operation fails)

Figure 6 describes the mechanism to open/close the security sessions.

Figure 6. Security sessions management


Password recovery

The ST25TVxxxC devices provide a password recovery feature, which allows the user to reprogram a corrupted password after a RF field failure during a WritePassword command.

Refer to “AN5577 - Password management for ST25TV512C and ST25TV02KC devices”, for more details on how to use it. Contact your STMicroelectronics sales office to get this document.

Password attempt limit

The ST25TVxxxC devices offer the capability to protect a password against brute-force attacks, thanks to a limiter mechanism on failed password attempts.

Refer to “AN5577 - Password management for ST25TV512C and ST25TV02KC devices”, for more details on how to use it. Contact your STMicroelectronics sales office to get this document.

5.1.3 Password encryption

An encryption mechanism - known as cover coding - is used to transmit coded password values in the Password_data field of the following command frames:

- PresentPassword request (see Section 6.4.19 PresentPassword),
- WritePassword request (see Section 6.4.18 WritePassword)
- Kill request (see Section 6.4.20 Kill)
- ToggleUntraceable request (see Section 6.4.23 ToggleUntraceable)

The mechanism requires that a call to the GetRandomNumber command has been issued since the latest boot of the ST25TVxxxC device, otherwise these password commands fail.

Additionally, if the latest call to a PresentPassword / Kill / ToggleUntraceable command failed because of an invalid value of the Password_data field, it is required that a call to the GetRandomNumber command is issued before attempting a new call to either of these three commands, otherwise their execution will fail regardless of the new value of the Password_data field.

Note: If the latest execution of a PresentPassword / ToggleUntraceable command was successful, it is not necessary to issue a new call to the GetRandomNumber command before issuing a new PresentPassword / Kill / ToggleUntraceable request.

Assuming these constraints are fulfilled, let the RND_NUMBER_4B and RND_NUMBER_8B values be computed from the concatenation of the RND_NUMBER register value returned by the latest call to the GetRandomNumber request.

Table 28. RND_NUMBER_4B

b31-b16	b15-b0
RND_NUMBER	RND_NUMBER

Table 29. RND_NUMBER_8B

b63-b48	b47-b32	b31-b16	b15-b0
RND_NUMBER	RND_NUMBER	RND_NUMBER	RND_NUMBER

Let PASSWORD_4B (resp. PASSWORD_8B) be the unencrypted value of a 32-bit (resp. 64-bit) password to be transmitted over a PresentPassword / WritePassword / Kill / ToggleUntraceable request.

The Password_data field in a request frame shall be computed as follows :

- for a 32-bit password :
 - $\text{Password_data} = \text{XOR}(\text{RND_NUMBER_4B}, \text{PASSWORD_4B})$
- for a 64-bit password :
 - $\text{Password_data} = \text{XOR}(\text{RND_NUMBER_8B}, \text{PASSWORD_8B})$

Table 30. Example of 64-bit Password_data value computation

Data name	b63-b56	b55-b48	b47-b40	b39-b32	b31-b24	b23-b16	b15-b8	b7-b0
RND_NUMBER	-	-	-	-	-	-	1Dh	E6h
RND_NUMBER_8B	1Dh	E6h	1Dh	E6h	1Dh	E6h	1Dh	E6h
PASSWORD_8B	FAh	D7h	5Eh	15h	CAh	A5h	D0h	D4h
Password_data	E7h	31h	43h	F3h	D7h	43h	CDh	32h

Note: A field coded on several bytes – such as Password_data – is transmitted in LSB to MSB byte order in ISO15693 request and response frames

When processing a PresentPassword / Kill / ToggleUntraceable request, the ST25TVxxxC device decrypts the Password_data field to obtain the unencrypted value PASSWORD_4B (or PASSWORD_8B), which is used for comparison with the password register identified by the Password_id field.

When processing a WritePassword request, the ST25TVxxxC device decrypts the Password_data field to obtain the unencrypted value PASSWORD_4B (or PASSWORD_8B) , which is used for update of the password register identified by the Password_id field.

5.1.4 User memory protection

A read and/or write access protection can be globally applied to the blocks of an area. Such protection can be individually configured for AREA1 and AREA2, thanks to the RW_PROTECTION_A1 and RW_PROTECTION_A2 registers (see [Table 11. RW_PROTECTION_A1 content](#) and [Table 15. RW_PROTECTION_A2 content](#)).

On factory delivery, access to AREA1 and AREA2 are not protected. When updating RW_PROTECTION_Ax registers, the new protection mode is effective during the boot sequence of the next RF session.

In addition to the area protection mechanism, the write access to each block composing AREA1 and AREA2 can be individually locked thanks to the LockBlock command.

Block 00h is an exception to the area protection mechanism:

- when block 00h is not locked, the protection of its write access is determined by the value of RW_PROTECTION_A1 register, like other blocks of AREA1
- read access to block 00h is always allowed, regardless of the value of RW_PROTECTION_A1 register

The RW_PROTECTION_A1 register is locked when register LCK_A1 is set to 1b.

The RW_PROTECTION_A2 register is locked when register LCK_A2 is set to 1b.

The END_A1 register is locked when either of LCK_A1 and LCK_A2 registers is set to 1b.

Retrieve the security status of a user memory block

User can read a block security status (BSS) by issuing following commands:

- GetMultipleBlockSecurityStatus
- ReadSingleBlock with Option_flag set to 1
- ReadMultipleBlocks with Option_flag set to 1

For each block, ST25TVxxxC will respond with a BSS byte containing a Lock_bit flag (b0 in [Table 31](#)) as specified in ISO 15693 standard.

Table 31. Block security status

b7	b6	b5	b4	b3	b2	b1	b0
0: RFU							0: Write access to current block granted 1: Write access to current block denied

This Lock_bit flag is set to one if write access to the corresponding block is not allowed. This happens when either of the following conditions is met:

- the write access to the block was permanently locked (corresponding bit of LCK_BLOCK register set to 1b) by a successful LockBlock command
- write access to parent area is protected (RW_PROTECTION_Ax = 01b or 10b at start of the RF session) and security session is closed
- write access to parent area is forbidden (RW_PROTECTION_Ax = 11b at start of the RF session)

5.1.5 System configuration memory protection

Configurations registers listed [Table 4. List of configuration registers](#) are accessed using the ReadConfiguration and WriteConfiguration commands.

Configuration registers are grouped by feature. A group is identified by parameter FID, a register from this group is identified by parameter PID.

Write access to configuration registers is protected or forbidden.

Note: Write access to read-only configuration registers is forbidden

Protected write access to a configuration register is granted when the CONFIG security session is open, and its parent group is not permanently locked.

Read access to configuration registers is protected or always allowed. Protected read access to a configuration register is granted when the CONFIG security session is open, and its parent group is not permanently locked.

On factory delivery, configuration groups are not locked (all bits of LCK_CONFIG register are set to 0b). A configuration group identified by FID (00h, 01h, 02h, 03h, 04h, 05h or 08h) can be permanently locked by setting bit FID of LCK_CONFIG register to 1b:

- if the read access to a configuration register from this group was protected, the register can no longer be read even if CONFIG security session is open
- if the write access to a configuration register from this group was protected, the register can no longer be written even if CONFIG security session is open
- write access to LCK_CONFIG register (FID=FFh, PID=00h) is granted when the CONFIG security session is open
- user cannot unlock a configuration group by setting bit FID of LCK_CONFIG back to 0b, even after opening CONFIG security session (Lock is permanent)
- user may lock several configuration groups with a single WriteConfiguration command by setting the respective bits of LCK_CONFIG to 1b in the request

System registers listed in [Table 5. List of system registers](#) include passwords, device identification registers, lock status and command status.

Read access to system registers is available except for passwords, AFI and DSFID lock status, Kill and ToggleUntraceable command status.

Device identification registers are detailed in section 5.10:

- Write access to AFI and DSFID registers can be respectively locked by LockAFI and LockDSFID commands. Lock is permanent: once locked, write access to AFI and DSFID registers is forbidden.
- Other device identification registers (IC_REF, UID) are read only registers.

5.2 Unique tap code

5.2.1 Unique tap code registers

Table 32. UTC_EN access

RF command	Access type
ReadConfiguration @(FID=02h, PID=00h)	R : always possible
WriteConfiguration @(FID=02h, PID=00h)	W : if the CONFIG security session is open and LCK_UTC=0b
	W effective time : on next RF boot sequence

Table 33. UTC_EN content

Bit	Name	Function	Factory value
b0	UTC_EN	0: Unique tap code is disabled 1: Unique tap code is enabled	0b
b7-b1	RFU	-	0000000b

Note: Refer to [Table 4. List of configuration registers for the UTC_EN register](#).

Table 34. UTC access

RF command	Access type
ReadConfiguration @(FID=02h, PID=01h)	R : always possible
-	W : no write access ⁽¹⁾

1. the content of the UTC register is updated internally during the RF boot sequence when UTC_EN is set to 1b

Table 35. UTC content

Bit	Name	Function	Factory value
b23-b0	UTC	Unique tap code value	Not applicable

Note: Refer to [Table 4. List of configuration registers for the UTC register](#).

5.2.2 Unique tap code description

When the UTC_EN register is set to 1b, the content of the UTC register is updated with an ASCII value. This value is generated once every time the device is powered. It is unique to each user tap of the tag, and predictable.

The UTC_EN register is locked when register LCK_UTC is set to 1b.

A typical usage of UTC is to embed it in the URI record of an NDEF message. In this case, when a user taps the tag with a smartphone, its web browser natively opens a URL including the unique tap code, which can be processed as an element of tag authentication by the web server.

More details on this feature are provided in "AN5578 - Unique tap code for ST25TV512C and ST25TV02KC devices". Contact your STMicroelectronics sales office to get this document.

Note: When the unique tap code is enabled, the duration of the RF boot sequence t_{Boot_RF} (see [Section 8.2 RF electrical parameters](#)) is:

- compliant with the 5ms guard-time value defined in the NFC Forum [DIGITAL] specification
- not compliant with the 1ms guard-time value defined in the ISO15693 specification

5.3 Tamper detection

The tamper detection feature is available on ST25TV02KC-T devices only (see section 10). On ST25TVxxC-A devices, ReadConfiguration and WriteConfiguration commands requested with FID=03h fail with error code 10h.

5.3.1 Tamper detection registers

Table 36. TD_EVENT_UPDATE_EN access

RF command	Access type
ReadConfiguration @(FID=03h, PID=00h)	R : always possible
WriteConfiguration @(FID=03h, PID=00h)	W : if the CONFIG security session is open and LCK_TD=0b
	W effective time : on next RF boot sequence

Table 37. TD_EVENT_UPDATE_EN content

Bit	Name	Function	Factory value
b0	TD_EVENT_UPDATE_EN	0: memorization of tamper events disabled 1: memorization of tamper events enabled	0b
b7- b1	RFU	-	0000000b

Note: Refer to [Table 4. List of configuration registers for the TD_EVENT_UPDATE_EN register.](#)

Table 38. TD_SEAL_MSG access

RF command	Access type
ReadConfiguration @(FID=03h, PID=01h)	R : if the CONFIG security session is open and LCK_TD=0b
WriteConfiguration @(FID=03h, PID=01h)	W : if the CONFIG security session is open and LCK_TD=0b W effective time : immediate

Table 39. TD_SEAL_MSG content

Bit	Name	Function	Factory value
b15-b0	TD_SEAL_MSG	Value of TD_EVENT displayed before first occurrence of a TD_UNSEAL event	3030h

Note: Refer to [Table 4. List of configuration registers for the TD_SEAL_MSG register.](#)

Table 40. TD_UNSEAL_MSG access

RF command	Access type
ReadConfiguration @(FID=03h, PID=02h)	R : if the CONFIG security session is open and LCK_TD=0b
WriteConfiguration @(FID=03h, PID=02h)	W : if the CONFIG security session is open and LCK_TD=0b W effective time : immediate

Table 41. TD_UNSEAL_MSG content

Bit	Name	Function	Factory value
b15-b0	TD_UNSEAL_MSG	Value of TD_EVENT displayed after first occurrence of a TD_UNSEAL event	5555h

Note: *Note:* Refer to [Table 4. List of configuration registers for the TD_UNSEAL_MSG register.](#)

Table 42. TD_RESEAL_MSG access

RF command	Access type
ReadConfiguration @(FID=03h, PID=03h)	R : if the CONFIG security session is open and LCK_TD=0b
WriteConfiguration @(FID=03h, PID=03h)	W : if the CONFIG security session is open and LCK_TD=0b W effective time : immediate

Table 43. TD_RESEAL_MSG content

Bit	Name	Function	Factory value
b15-b0	TD_RESEAL_MSG	Value of TD_EVENT displayed after occurrence of a TD_RESEAL event	5252h

Note: Refer to [Table 4. List of configuration registers for the TD_RESEAL_MSG register](#).

Table 44. TD_SHORT_MSG access

RF command	Access type
ReadConfiguration @(FID=03h, PID=04h)	R : if the CONFIG security session is open and LCK_TD=0b
WriteConfiguration @(FID=03h, PID=04h)	W : if the CONFIG security session is open and LCK_TD=0b
	W effective time : immediate

Table 45. TD_SHORT_MSG content

Bit	Name	Function	Factory value
b7- b0	TD_SHORT_MSG	Message displayed when the tamper loop was in closed status during the latest boot sequence	63h

Note: Refer to [Table 4. List of configuration registers for the TD_SHORT_MSG register](#).

Table 46. TD_OPEN_MSG access

RF command	Access type
ReadConfiguration @(FID=03h, PID=05h)	R : if the CONFIG security session is open and LCK_TD=0b
WriteConfiguration @(FID=03h, PID=05h)	W : if the CONFIG security session is open and LCK_TD=0b
	W effective time : immediate

Table 47. TD_OPEN_MSG content

Bit	Name	Function	Factory value
b7- b0	TD_OPEN_MSG	Message displayed when the tamper loop was in open status during the latest boot sequence	6Fh

Note: Refer to [Table 4. List of configuration registers for the TD_OPEN_MSG register](#).

Table 48. TD_STATUS access

RF command	Access type
ReadConfiguration @(FID=03h, PID=06h)	R : always possible
-	W : no write access

Table 49. TD_STATUS content

Bit	Name	Function	Factory value
b15-b0	TD_EVENT	TD_SEAL_MSG, TD_UNSEAL_MSG or TD_RESEAL_MSG according to result of tamper event detection	Not applicable
b23-b16	TD_LOOP	TD_SHORT_MSG or TD_OPEN_MSG according to the status of the tamper loop during the latest boot sequence	Not applicable

Note: Refer to [Table 5. List of system registers for the TD_STATUS register](#).

5.3.2 Tamper detection description

The tamper detection feature allows to check the shortage status between the TD0 and TD1 pins of the ST25TV02KC-T, and monitor tamper events.

See [Section 8.2 RF electrical parameters](#) for recommended impedance values R_{open} and R_{closed} in cases of open and closed tamper loop.

The shortage status TD_LOOP and event status TD_EVENT are read in the response to a ReadConfiguration request with FID=03h and PID=06h.

This is the customer responsibility to check the values of TD_LOOP and TD_EVENT and behave accordingly.

TD_LOOP

The shortage status TD_LOOP is captured by ST25TV02KC-T each time that the device is powered- up. Value of TD_LOOP is equal to value of:

- TD_SHORT_MSG when TD0 and TD1 were connected at capture time
- TD_OPEN_MSG when TD0 and TD1 were not connected at capture time

This information will be lost during power off (no permanent storage of TD_LOOP).

TD_EVENT

The TD_EVENT status is used to monitor the first occurrences of TD_UNSEAL and TD_RESEAL events defined as follows:

- TD_UNSEAL: TD_EVENT_UPDATE_EN register was set to 1b, and TD0 and TD1 were not connected at capture time
- TD_RESEAL: TD_EVENT_UPDATE_EN register was set to 1b, TD_UNSEAL already occurred, and TD0 and TD1 were connected at capture time

On factory delivery, TD_EVENT_UPDATE_EN is set to 0b and TD_EVENT is set to the value of TD_SEAL_MSG.

When the first TD_UNSEAL event occurs, TD_EVENT is updated to the value of TD_UNSEAL_MSG.

When the first TD_RESEAL event occurs, TD_EVENT is updated to the value of TD_RESEAL_MSG.

The update of the TD_EVENT register occurs during the RF boot sequence, and its value is stored in the EEPROM of the ST25TV02KC-T device.

When the LCK_TD register is set to 1b, the TD_EVENT_UPDATE_EN, TD_SEAL_MSG, TD_UNSEAL_MSG, TD_RESEAL_MSG, TD_SHORT_MSG and TD_OPEN_MSG registers are locked.

Note: When TD_EVENT is updated, the duration of the RF boot sequence t_{Boot_RF} (see [Section 8.2 RF electrical parameters](#)) is:

- compliant with the 5ms guard-time value defined in the NFC Forum [DIGITAL] specification
- not compliant with the 1ms guard-time value defined in the ISO15693 specification

Note: When TD_EVENT_UPDATE_EN and UTC_EN registers are set to 0b, no programming of the EEPROM occurs during the RF boot sequence, and its duration is compliant with the 1ms guard-time value defined in the ISO15693 specification.

Note: Tamper detection events occurring outside of the capture window (for instance while the IC is in POWER-OFF state, or during the RF session following the boot sequence) are **not** detected by the ST25TV02KC-T.

5.4 Augmented NDEF

5.4.1 Augmented NDEF registers

Table 50. ANDEF_EN access

RF command	Access type
ReadConfiguration @(FID=04h, PID=00h)	R : always possible
WriteConfiguration @(FID=04h, PID=00h)	W : if the CONFIG security session is open and LCK_ANDEF=0b W effective time : on next RF boot sequence

Table 51. ANDEF_EN content

Bit	Name	Function	Factory value
b0	ANDEF_EN	0: ANDEF feature is disabled, 1: ANDEF feature is enabled	0b
b7- b1	RFU	-	0000000b

Note: Refer to [Table 4. List of configuration registers for the ANDEF_EN register](#).

Table 52. ANDEF_CFG access

RF command	Access type
ReadConfiguration @(FID=04h, PID=01h)	R : always possible
WriteConfiguration @(FID=04h, PID=01h)	W : if the CONFIG security session is open and LCK_ANDEF=0b W effective time : on next RF boot sequence

Table 53. ANDEF_CFG content

Bit	Name	Function	Factory value
b0	ANDEF_UID_EN	0: UID field disabled in ANDEF feature 1: UID field enabled in ANDEF feature	0b
b1	ANDEF_CUS_EN	0: Custom field disabled in ANDEF feature 1: Custom field enabled in ANDEF feature	0b
b2	ANDEF_UTC_EN	0: Unique tap code field disabled in ANDEF feature 1: Unique tap code field enabled in ANDEF feature	0b
b3	RFU	-	0b
b4	ANDEF_TD_EN ⁽¹⁾	0: Tamper detection field disabled in ANDEF feature 1: Tamper detection field enabled in ANDEF feature	0b
b5	ANDEF_SEP_EN	0: ANDEF field separator disabled 1: ANDEF field separator enabled	1b
b7- b6	ANDEF_BYTE	Byte offset in block ANDEF_BLOCK where the ANDEF feature starts operating	00b
b15-b8	ANDEF_BLOCK	Block address where the ANDEF feature starts operating	00h

¹. relevant on ST25TV02KC-T devices only, forced to 0b on ST25TVxxxC-A devices

Note: Refer to [Table 4. List of configuration registers for the ANDEF_CFG register](#).

Table 54. ANDEF_SEP access

RF command	Access type
ReadConfiguration @(FID=04h, PID=02h)	R : if the CONFIG security session is open and LCK_ANDEF=0b
WriteConfiguration @(FID=04h, PID=02h)	W : if the CONFIG security session is open and LCK_ANDEF=0b W effective time : immediate

Table 55. ANDEF_SEP content

Bit	Name	Function	Factory value
b7- b0	ANDEF_SEP	Character used as ANDEF field separator when ANDEF_SEP_EN=1b	78h

Note: Refer to [Table 4. List of configuration registers for the ANDEF_SEP register](#).

Table 56. ANDEF_CUSTOM_LSB access

RF command	Access type
ReadConfiguration @(FID=04h, PID=03h)	R : if the CONFIG security session is open and LCK_ANDEF=0b
WriteConfiguration @(FID=04h, PID=03h)	W : if the CONFIG security session is open and LCK_ANDEF=0b W effective time : immediate

Table 57. ANDEF_CUSTOM_LSB content

Bit	Name	Function	Factory value
b31-b0	ANDEF_CUSTOM_LSB	First 4 characters of the ANDEF custom field	2E2E2E2Eh

Note: Refer to [Table 4. List of configuration registers for the ANDEF_CUSTOM_LSB register](#).

Table 58. ANDEF_CUSTOM_MSB access

RF command	Access type
ReadConfiguration @(FID=04h, PID=04h)	R : if the CONFIG security session is open and LCK_ANDEF=0b
WriteConfiguration @(FID=04h, PID=04h)	W : if the CONFIG security session is open and LCK_ANDEF=0b W effective time : immediate

Table 59. ANDEF_CUSTOM_MSB content

Bit	Name	Function	Factory value
b31-b0	ANDEF_CUSTOM_MSB	Last 4 characters of the ANDEF custom field	2E2E2E2Eh

Note: Refer to [Table 4. List of configuration registers for the ANDEF_CUSTOM_MSB register](#).

Table 60. ANDEF_UID access

RF command	Access type
ReadSingleBlock ReadMultipleBlocks	R : if ANDEF_EN=1b and ANDEF_UID_EN=1b
-	W : no write access

Table 61. ANDEF_UID content

Bit	Name	Function	Factory value
b127-b0	ANDEF_UID	Value displayed in the UID field of the ANDEF feature	UID in ASCII format starting with "E0"

Note: Refer to [Table 5. List of system registers for the ANDEF_UID register](#).

5.4.2 Augmented NDEF description

The Augmented NDEF feature (ANDEF) is a contextual automatic NDEF message service, allowing the tag to respond dynamic content without an explicit update of the EEPROM by the end user.

The feature is enabled (resp. disabled) when the value of register ANDEF_EN is 1b (resp. 0b) during the latest RF boot sequence. When the feature is enabled, user memory data at byte addresses ranging from ANDEF_START to ANDEF_END is replaced by the content of a virtual memory ANDEF_MEM in the response to ReadSingleBlock and ReadMultipleBlocks requests.

Note: The BSS values responded to ReadSingleBlock and ReadMultipleBlocks requests are not modified when the ANDEF feature is enabled

Note: The ANDEF feature has no effect on the WriteSingleBlock command. When the feature is enabled, and a WriteSingleBlock command is issued on a block crossing the [ANDEF_START:ANDEF_END] range, the data from the command is directly written to user memory, without replacement by volatile memory content.

Table 62. Block data read when ANDEF feature is disabled on ST25TV02KC

Block address	Block data ⁽¹⁾				Comment
	Byte0	Byte1	Byte2	Byte3	
00h	UM000	UM001	UM002	UM003	First block of UM ⁽²⁾
...	...	...	...	...	No bytes read from ANDEF_MEM memory
4Fh ⁽³⁾	UM316	UM317	UM318	UM319	Last block of UM ⁽²⁾

1. Block data responded to ReadSingleBlock and ReadMultipleBlocks requests.

2. UM stands for user memory.

3. ST25TV02KC memory size is used in this example. Note that last block address is 0Fh on ST25TV512C devices.

Table 63. Block data read when ANDEF feature is enabled on ST25TV02KC

Block address	Block data ⁽¹⁾				Comment
	Byte0	Byte1	Byte2	Byte3	
00h	UM000	UM001	UM002	UM003	First block of UM ⁽²⁾
...	...	...	...	...	-
2Dh	UM180	UM181	UM182	UM183	Example with ANDEF_START=185 and ANDEF_END=190 (6 bytes of UM ⁽²⁾ replaced with AM ⁽³⁾)
2Eh	UM184	AM000	AM001	AM002	
2Fh	AM003	AM004	AM005	UM191	
30h	UM192	UM193	UM194	UM195	
...	...	...	...	...	-
4Fh ⁽⁴⁾	UM316	UM317	UM318	UM319	Last block of UM ⁽²⁾

1. Block data responded to ReadSingleBlock and ReadMultipleBlocks requests.

2. UM stands for user memory

3. AM stands for ANDEF_MEM memory

4. ST25TV02KC memory size is used in this example. Note that last block address is 0Fh on ST25TV512C devices.

Byte addresses ANDEF_START and ANDEF_END depend on the value of register ANDEF_CFG during the latest RF boot sequence:

- $\text{ANDEF_START} = \text{ANDEF_BLOCK} * 4 + \text{ANDEF_BYTE}$
- $\text{ANDEF_END} = \min(\text{END_MEM} * 4 + 3, \text{ANDEF_START} + \text{ANDEF_LEN} - 1)$

Where ANDEF_LEN is the number of bytes available from ANDEF_MEM memory:

- $$\text{ANDEF_LEN} = \text{ANDEF_UID_EN} * 16 + \text{ANDEF_CUS_EN} * 8 + \text{ANDEF_UTC_EN} * 3 + \text{ANDEF_TD_EN} * 3 + \text{ANDEF_SEP_EN} * (\text{ANDEF_UID_EN} + \text{ANDEF_CUS_EN} + \text{ANDEF_UTC_EN} + \text{ANDEF_TD_EN} - 1)$$

Content of ANDEF_MEM depends on the values of ANDEF_CFG, ANDEF_UID, ANDEF_CUSTOM_LSB, ANDEF_CUSTOM_MSB, UTC, TD_STATUS and ANDEF_SEP registers.

The content of ANDEF_MEM is the result of the concatenation of ANDEF fields. Each field corresponds to a configuration register. The order of appearance, content and condition of presence of each field is listed in the table below.

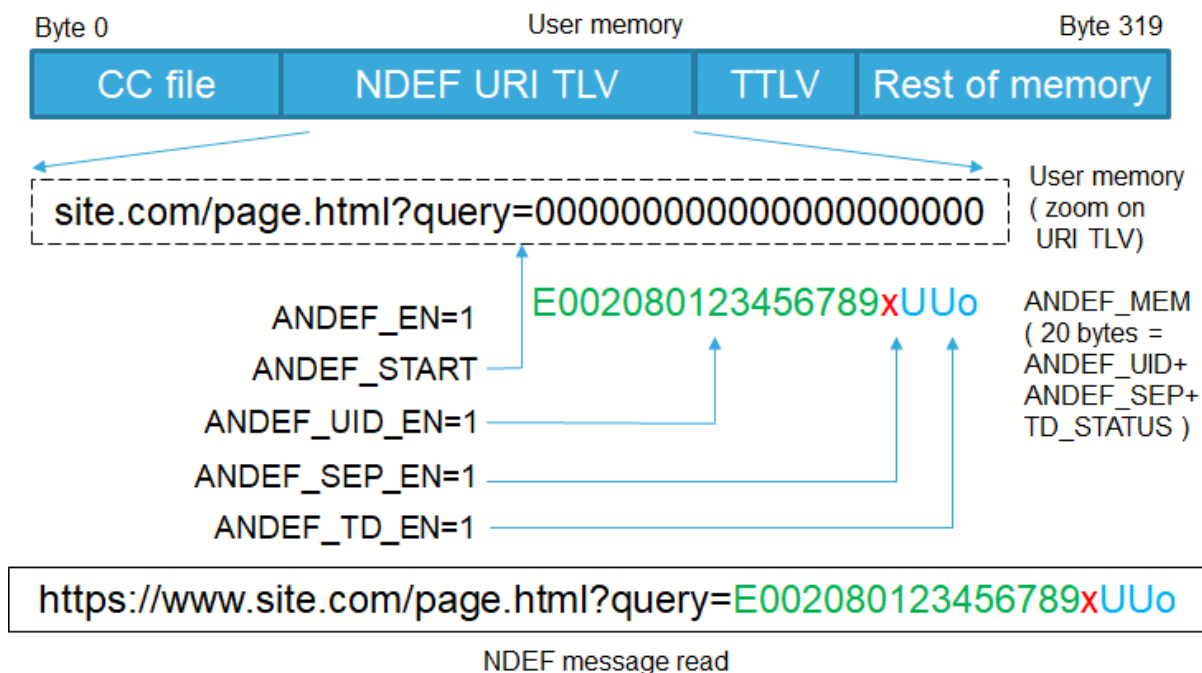
Table 64. ANDEF fields concatenated in ANDEF_MEM

Order	Content ⁽¹⁾	Bytes	Condition of presence
1	ANDEF_UID	16	ANDEF_UID_EN=1b
2	ANDEF_SEP	1	ANDEF_UID_EN=1b and ANDEF_CUS_EN=1b and ANDEF_SEP_EN=1b
3	ANDEF_CUSTOM_LSB	4	ANDEF_CUS_EN=1b
4	ANDEF_CUSTOM_MSB	4	ANDEF_CUS_EN=1b
5	ANDEF_SEP	1	(ANDEF_UID_EN=1b or ANDEF_CUS_EN=1b) and ANDEF_UTC_EN=1b and ANDEF_SEP_EN=1b
6	UTC	3	ANDEF_UTC_EN=1b
7	ANDEF_SEP	1	(ANDEF_UID_EN=1b or ANDEF_CUS_EN=1b or ANDEF_UTC_EN=1b) and ANDEF_TD_EN=1b ⁽²⁾ and ANDEF_SEP_EN=1b
8	TD_STATUS	3	ANDEF_TD_EN=1b ⁽²⁾

1. When a register value is coded on several bytes, it is copied in LSB to MSB byte order in the ANDEF_MEM memory.

2. TD_STATUS field available on ST25TV02KC-T devices only

As an example, [Figure 7](#) shows the usage of the ANDEF feature to display the value of the ANDEF_UID and TD_STATUS registers in a NDEF URI message : the content of the NDEF message may change after a tamper detection event without modification of the user memory content.

Figure 7. Example of augmented NDEF message on ST25TV02KC-T


On factory delivery, ANDEF_EN register is set to 0b and ANDEF_CFG register is set to 0020h.
 When the LCK_ANDEF register is set to 1b, ANDEF_EN, ANDEF_CFG, ANDEF_SEP, ANDEF_CUSTOM_LSB and ANDEF_CUSTOM_MSB registers are locked.

5.5 Consumer privacy protection

The Kill and Untraceable features offer consumer privacy capabilities required by the GDPR.

5.5.1 Privacy registers

Table 65. KILL_CMD access

RF command	Access type
-	R : no read access
Kill	W : if Kill command responds with Error_flag=0b
	W effective time : immediate

Table 66. KILL_CMD content

Bit	Name	Function	Factory value
b0	KILL_CMD	0: successful Kill command did not occur 1: successful Kill command did occur	0b

Note: Refer to Table 5. List of system registers for the KILL_CMD register.

Table 67. UNTR_CMD access

RF command	Access type
-	R : no read access
ToggleUntraceable	W : if ToggleUntraceable command responds with Error_flag=0b
	W effective time : immediate

Table 68. UNTR_CMD content

Bit	Name	Function	Factory value
b0	UNTR_CMD	0: last successful ToggleUntraceable command occurred with Address_flag=0b 1: last successful ToggleUntraceable command occurred with Address_flag=1b	0b

Note: Refer to [Table 5. List of system registers for the UNTR_CMD register](#).

Table 69. PRIVACY access

RF command	Access type
ReadConfiguration @(FID=05h, PID=00h)	R : always possible
WriteConfiguration @(FID=05h, PID=00h)	W : if the CONFIG security session is open and LCK_PRIV=0b
	W effective time : on next RF boot sequence

Table 70. PRIVACY content

Bit	Name	Function	Factory value
b1- b0	UNTR_DFT	00: device boots in UNTRACEABLE state when UNTR_CMD=1b 01: device always boots in UNTRACEABLE state 10: device boots in UNTRACEABLE state when UNTR_CMD=1b or tamper loop is closed 11: device boots in UNTRACEABLE state when UNTR_CMD=1b or tamper loop is open	00b
b2	DIS_INV	0: Inventory command responds in UNTRACEABLE state 1: Inventory command is mute in UNTRACEABLE state	0b
b3	DIS_KILL	0: Kill command is enabled 1: Kill command is disabled	0b
b7- b4	RFU	-	0000b

Note: Refer to [Table 4. List of configuration registers for the PRIVACY register](#).

5.5.2 Kill feature description

When the ST25TVxxxC is in KILLED state, all incoming RF requests are ignored.

The ST25TVxxxC enters the KILLED state on a successful Kill command (see [Section 6.4.20 Kill](#)), which sets the KILL_CMD register to 1b. Once the ST25TVxxxC has entered the KILLED state, it can only switch between the POWER-OFF and KILLED states (see [Section 6.2.8 ISO15693 states](#)).

The Kill command is enabled/disabled when the DIS_KILL register respectively has value 0/1b during the latest boot sequence. The update of the DIS_KILL register is effective on the next RF boot sequence.

While the Kill command is disabled, the Kill request is ignored and the ST25TVxxxC can not enter the KILLED state.

On factory delivery, the KILL_CMD and DIS_KILL registers are set to 0b.

When the LCK_PRIV register is set to 1b, the DIS_KILL register is locked.

5.5.3 Untraceable feature description

When the ST25TVxxxC is in UNTRACEABLE state, all incoming RF requests are ignored except:

- GetRandomNumber and ToggleUntraceable requests (see [Section 6.4.23 ToggleUntraceable](#) and [Section 6.4.24 GetRandomNumber](#))
- Inventory and ReadSingleBlock (block 00h only) requests if value of DIS_INV register was 0b during the latest RF boot sequence

The ST25TVxxxC enters the UNTRACEABLE state on a successful ToggleUntraceable command requested with Address_flag=1b, which sets the UNTR_CMD register to 1b.

The ST25TVxxxC leaves the UNTRACEABLE state on a successful ToggleUntraceable command requested with Address_flag=0b, which sets the UNTR_CMD register to 0b.

After a RF boot sequence, the ST25TVxxxC enters the UNTRACEABLE state if KILL_CMD register is set to 0b and either of the following conditions is met:

- value of UNTR_CMD register is 1b
- value of UNTR_DFT register is 01b
- value of UNTR_DFT register is 10b and tamper loop is closed (ST25TV02KC-T devices only)
- value of UNTR_DFT register is 11b and tamper loop is open (ST25TV02KC-T devices only)

See [Section 6.2.8 ISO15693 states](#) for further details.

Note: After a RF boot sequence with KILL_CMD=UNTR_CMD=0b and UNTR_DFT=10b :

- the ST25TV02KC-T enters the **UNTRACEABLE** state if the tamper loop is **closed**
- the ST25TV02KC-T enters the **READY** state if the tamper loop is **open**

Note: After a RF boot sequence with KILL_CMD=UNTR_CMD=0b and UNTR_DFT=11b:

- the ST25TV02KC-T enters the **UNTRACEABLE** state if the tamper loop is **open**
- the ST25TV02KC-T enters the **READY** state if the tamper loop is **closed**

Note: On ST25TVxxxC-A devices, 10b and 11b values of UNTR_DFT register are interpreted as value 00b.

Untraceability of the customer is claimed for the following reasons :

- in a NFC Forum application, block 00h contains the CC file which does not allow to identify a customer
- user blocks 01h to END_MEM - which contain customer data - can not be accessed in UNTRACEABLE state
- while in UNTRACEABLE state, the UID value used in request and response frames of Inventory and ReadSingleBlock commands is fixed (see [Section 7.1 Untraceable UID](#)) and does not allow to identify a customer

Furthermore, the user may configure the ST25TVxxxC to ignore Inventory and ReadSingleBlock requests in UNTRACEABLE state, by setting the DIS_INV register to 1b.

The update of the DIS_INV and UNTR_DFT registers is effective on the next RF boot sequence. On factory delivery, the DIS_INV and UNTR_DFT registers are set to 0.

When the LCK_PRIV register is set to 1b, the UNTR_DFT and DIS_INV registers are locked.

5.6 TruST25 digital signature

The ST25TVxxxC devices support the TruST25 digital signature feature, which allows the user to verify the authenticity of the device, thanks to a unique digital signature.

The TruST25 solution encompasses secure industrialization processes and tools deployed by STMicroelectronics to generate, store, and check the signature in the device.

For some configurations of this feature, the value of END_MEM may be reduced to 3Dh on ST25TV02KC devices.

Refer to "AN5580 - TruST25 digital signature for ST25TV512C and ST25TV02KC devices", for more details on how to use this feature. Contact your STMicroelectronics sales office to get this document.

5.7 AFI protection

5.7.1 AFI protection registers

Table 71. AFI_PROT access

RF command	Access type
ReadConfiguration @(FID=08h, PID=00h)	R : always possible
WriteConfiguration @(FID=08h, PID=00h)	W : if the CONFIG security session is open and LCK_AFIP=0b W effective time : on next RF boot sequence

Table 72. AFI_PROT content

Bit	Name	Function	Factory value
b0	AFI_PROT	0: WriteAFI and LockAFI commands do not depend from AREA1 security session 1: WriteAFI and LockAFI commands fail when AREA1 security session is closed	0b
b7- b1	RFU	-	0000000b

Note: Refer to [Table 4. List of configuration registers for the AFI_PROT register](#).

5.7.2 AFI protection description

This feature allows to protect the WriteAFI and LockAFI commands with the AREA1 security session, and is configured by register AFI_PROT.

On factory delivery, the AFI_PROT register is set to 0b. When AFI_PROT register is set to 0b:

- the WriteAFI command is successful if the LCK_AFI register is set to 0b, and fails otherwise
- the LockAFI command is successful if the LCK_AFI register is set to 0b, and fails otherwise

When AFI_PROT register is set to 1b:

- the WriteAFI command is successful if AREA1 security session is open and the LCK_AFI register is set to 0b, and fails otherwise
- the LockAFI command is successful if AREA1 security session is open and the LCK_AFI register is set to 0b, and fails otherwise

When the LCK_AFIP register is set to 1b, the AFI_PROT register is locked.

5.8 Inventory Initiated

ST25TVxxxC provides a special feature to improve the anticollision sequence on moving tags using the Initiate_flag volatile register. This register, controlled by the Initiate command (refer to [Section 6.4.21 Initiate](#)), allows ST25TVxxxC to respond to InventoryInitiated requests (refer to [Section 6.4.22 InventoryInitiated](#)).

For applications where multiple tags are crossing the RF field of a reader, it is possible to miss tags when the standard Inventory command is used. The reason is that the anticollision sequence performs a global tree search, calling the command at each node and leaf of the tree. In a worst case, a tag WC waits a long delay before it is inventoried as a leaf of the search. Such delay can be furthermore increased by tags entering the RF field of the reader during the search, and tag WC may have left the field before being inventoried.

This usecase can be improved by replacing the standard Inventory command with the custom InventoryInitiated command in the anticollision sequence. When multiple tags are crossing the RF field of the reader, the anticollision sequence is started by an Initiate command which initiates the set of tags within range. InventoryInitiated requests are ignored by tags entering the RF field after the Initiate command, they are only processed by the set of initiated tags, hence bounding the time necessary to complete the anticollision sequence. When an initiated tag is inventoried, it is sent to QUIET state to ignore further InventoryInitiated requests.

Once an anticollision sequence is completed, the reader starts a new sequence that will operate only on tags which have entered the RF field during the previous sequence, and so on.

5.9 Device identification registers

Registers described in this section are located in System configuration memory. Refer to section 4.3 for more details.

Table 73. LCK_DSFD access

RF command	Access type
-	R : no read access
LockDSFD	W : if LCK_DSFD=0b W effective time : immediate

Table 74. LCK_DSFD content

Bit	Name	Function	Factory value
b0	LCK_DSFD	0: successful LockDSFD command did not occur 1: successful LockDSFD command did occur	0b

Note: Refer to [Table 5. List of system registers for the LCK_DSFD register](#).

Table 75. LCK_AFI access

RF command	Access type
-	R : no read access
LockAFI	W : if LCK_AFI=0b and (AFI_PROT=0b or AREA1 security session is open) W effective time : immediate

Table 76. LCK_AFI content

Bit	Name	Function	Factory value
b0	LCK_AFI	0: successful LockAFI command did not occur 1: successful LockAFI command did occur	0b

Note: Refer to [Table 5. List of system registers for the LCK_AFI register](#).

Table 77. DSFD access

RF command	Access type
Inventory	R : always possible
GetSystemInfo	R : always possible
ExtendedGetSystemInfo	R : always possible
Initiate	R : always possible
InventoryInitiated	R : always possible
WriteDSFD	W : if LCK_DSFD=0b W effective time : immediate

Table 78. DSFID content

Bit	Name	Function	Factory value
b7-b0	DSFID	ISO/IEC 15693 Data Storage Format Identifier	00h

Note: Refer to [Table 5. List of system registers for the DSFID register](#).

Table 79. AFI access

RF command	Access type
GetSystemInfo	R : always possible
ExtendedGetSystemInfo	R : always possible
WriteAFI	W : if LCK_AFI=0b and (AFI_PROT=0b or AREA1 security session is open) W effective time : immediate

Table 80. AFI content

Bit	Name	Function	Factory value
b7-b0	AFI	ISO/IEC 15693 Application Family Identifier	00h

Note: Refer to [Table 5. List of system registers for the AFI register](#).

Table 81. IC_REF access

RF command	Access type
GetSystemInfo	R : always possible
ExtendedGetSystemInfo	R : always possible
-	W : no access

Table 82. IC_REF content

Bit	Name	Function	Factory value
b7-b0	IC_REF	ISO/IEC 15693 IC reference	08h

Note: Refer to [Table 5. List of system registers for the IC_REF register](#).

Table 83. REV access

RF command	Access type
ReadConfiguration @(FID=FEh, PID=00h)	R : always possible
-	W : no access

Table 84. REV content

Bit	Name	Function	Factory value
b7-b0	REV	IC revision number	12h for ST25TVxxxC-xxx3 25h for ST25TVxxxC-xxx9

Note: Refer to [Table 4. List of configuration registers for the REV register](#).

Table 85. UID access

RF command	Access type
Inventory	R : always possible
GetSystemInfo	R : always possible
ExtendedGetSystemInfo	R : always possible
Initiate	R : always possible
InventoryInitiated	R : always possible
ReadConfiguration @(FID=FEh, PID=01h)	R : always possible
-	W : no access

Table 86. UID content

Bit	Name	Function	Factory value
b7-b0	UID	ISO/IEC 15693 UID byte 0	IC manufacturer serial number
b15-b8		ISO/IEC 15693 UID byte 1	
b23-b16		ISO/IEC 15693 UID byte 2	
b31-b24		ISO/IEC 15693 UID byte 3	
b39-b32		ISO/IEC 15693 UID byte 4	
b47-b40		ISO/IEC 15693 UID byte 5	08h
b55-b48		ISO/IEC 15693 UID byte 6	02h
b63-b56		ISO/IEC 15693 UID byte 7	E0h

Note: Refer to [Table 5. List of system registers for the UID register](#).

6 RF Operation

The device follows ISO/IEC 15693 and NFC Forum Type 5 Tag specification for radio- frequency power and signal interface and for anticollision and transmission protocol.

The device communicates via the 13.56 MHz carrier electromagnetic wave on which incoming data are demodulated from the received signal amplitude modulation (ASK: amplitude shift keying). The received ASK wave is 10% or 100% modulated with a data rate of 1.6 Kbit/s using the 1/256 pulse coding mode or a data rate of 26 Kbit/s using the 1/4 pulse coding mode.

Outgoing data are generated by the ST25TVxxxC load variation using Manchester coding with one or two subcarrier frequencies at 423 kHz and 484 kHz. Data are transferred from the ST25TVxxxC at 6.6 Kbit/s in low data rate mode and 26 Kbit/s in high data rate mode.

6.1 RF communication

6.1.1 Access to a ISO/IEC 15693 device

The dialog between the reader and the ST25TVxxxC takes place as follows:

- activation of the ST25TVxxxC by the operating field of the reader
- transmission of a command by the reader (ST25TVxxxC detects carrier amplitude modulation)
- transmission of a response by the ST25TVxxxC using load modulation.

These operations use the power transfer and communication signal interface described below. This technique is called RTF (reader talk first).

Operating field

The ST25TVxxxC operates continuously between the minimum and maximum values of the electromagnetic field H defined in [Table 172. RF characteristics](#). The reader has to generate a field within these limits.

Power transfer

Power is transferred to the ST25TVxxxC by radio frequency at 13.56 MHz via coupling antennas in the ST25TVxxxC and the reader. The operating field of the reader is transformed on the ST25TVxxxC antenna to an AC voltage that is rectified, filtered and internally regulated. During communications, the amplitude modulation (ASK) on this received signal is demodulated by the ASK demodulator.

Frequency

The ISO 15693 standard defines the carrier frequency (f_C) of the operating field as 13.56 MHz $\pm$ 7 kHz.

Note: In this document, f_C symbol is used for the nominal value of f_{CC} ($f_C=13.56$ MHz).

6.2 RF protocol

6.2.1 Protocol description

The transmission protocol (or simply “the protocol”) defines the mechanism used to exchange instructions and data between the VCD (vicinity coupling device) and the VICC (vicinity integrated circuit card) in both directions. It is based on the concept of “VCD talks first”. The device acts as the VICC.

This means that a ST25TVxxxC does not start transmitting unless it has received and properly decoded an instruction sent by the VCD. The protocol is based on an exchange of commands, which consist in request/ response transactions between the VCD and the ST25TVxxxC:

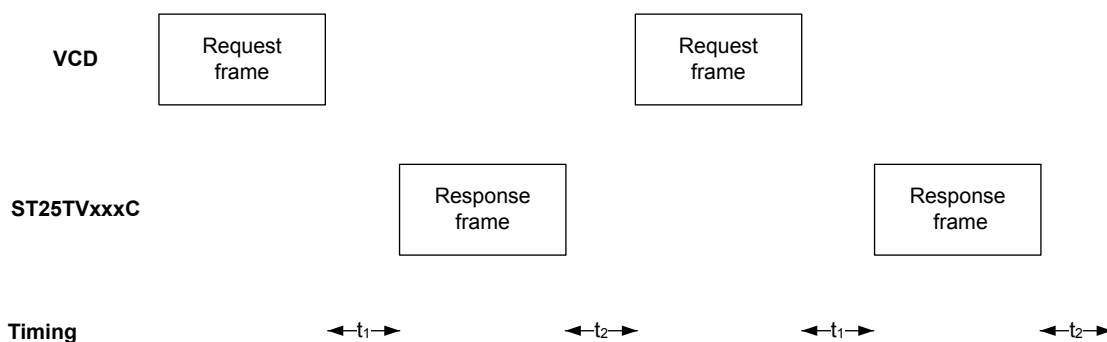
- a request is sent from the VCD to the ST25TVxxxC
- a response to this request is sent from the ST25TVxxxC to the VCD.

Each request and each response are contained in a frame. The frames are delimited by a Start of Frame (SOF) and End of Frame (EOF).

The protocol is bit-oriented. The number of bits transmitted in a frame is a multiple of eight (8), that is an integer number of bytes.

A single-byte field is transmitted least significant bit (LSBit) first. A multiple-byte field is transmitted least significant byte (LSByte) first and each byte is transmitted least significant bit (LSBit) first.

Figure 8. ISO15693 protocol timing



6.2.2

Request format

A request frame consists in :

- a SOF
- request flags
- a command code
- request parameters and data
- a CRC
- an EOF.

Table 87. General request format

SOF	Request_flags	Opcode	Parameters	Data	CRC_B	EOF
-	8 bits	8 bits	optional	optional	16 bits	-

6.2.3

Request flags

In a request frame, the Request_flags field specifies the actions to be performed by the ST25TVxxxC and whether corresponding fields are present or not.

The Request_flags field consists of eight bits indexed from 0 to 7.

Note:

Indexing of bits starts from 0 to comply with the convention used in this specification, however note that indexing of these bits starts at 1 in the ISO/IEC 15693 specification.

Bit 2 (Inventory_flag) of Request_flags defines the contents of the four MSBs (bits 4 to 7).

When Inventory_flag value is 0, bits 4 to 7 define the ST25TVxxxC selection criteria.

When Inventory_flag value is 1, bits 4 to 7 define the ST25TVxxxC Inventory parameters.

Table 88. Definition of Request_flags LSBs

Bit	Flag	Description
0	Subcarrier_flag ⁽¹⁾	0 : A single subcarrier is used by the VICC 1 : Two subcarriers are used by the VICC
1	Datarate_flag ⁽¹⁾	0 : Low data rate is used by the VICC 1 : High data rate used by the VICC
2	Inventory_flag	0 : Bits 4 to 7 are described by Table 89 1 : Bits 4 to 7 are described by Table 90
3	Protocol_extension_flag	0 : No protocol format extension 1 : Not supported (RFU)

1. Subcarrier_flag and Datarate_flag refer to the VICC-to-VCD communication.

Table 89. Definition of Request_flags MSBs when Inventory_flag value is 0

Bit	Flag	Description
4	Select_flag ⁽¹⁾	0 : The command is processed according to the value of Address_flag 1 : UID field not present. The command is processed only by the VICC in SELECTED state ⁽²⁾
5	Address_flag ⁽¹⁾	0 : UID field not present. command is processed by any VICC 1 : UID field present. command is processed only by the VICC whose UID matches the field value
6	Option_flag	0 : Option not activated 1 : Option activated
7	RFU_flag	0 : Unless otherwise specified 1 : Not supported (RFU)

1. Select_flag=1 and Address_flag=1 is an invalid case, a request with such setting is ignored by the ST25TVxxxC device.

2. The SELECTED state is defined in [Section 6.2.8 ISO15693 states](#).

Table 90. Definition of Request_flags MSBs when Inventory_flag value is 1

Bit	Flag	Description
4	AFI_flag	0 : AFI field is not present 1 : AFI field is present
5	Nb_slots_flag	0 : 16 slots mode 1 : 1 slot mode
6	Option_flag	0 : Option not activated 1 : Option activated
7	RFU_flag	0 : Unless otherwise specified 1 : Not supported (RFU)

6.2.4

Response format

A response frame consists in:

- a SOF
- response flags
- response data
- a CRC
- an EOF

Table 91. General response format

SOF	Response_flags	Response_data	CRC_B	EOF
-	8 bits	optional	16 bits	-

6.2.5 Response flags

In a response frame, the Response_flags field indicates how actions have been performed by the ST25TVxxxC and whether corresponding fields are present or not.

The Response_flags field consists of eight bits indexed from 0 to 7.

Note: Indexing of bits starts from 0 to comply with the convention used in this specification, however note that indexing of these bits starts at 1 in the ISO/IEC 15693 specification.

Table 92. Definition of Response_flags

Bit	Flag	Description
0	Error_flag	0 : No error 1 : Error detected. Error code present in the Data field
1	RFU	0 : Unless otherwise specified 1 : Not supported (RFU)
2		
3		
4		
5		
6		
7		

6.2.6 Response and error codes

If the Error_flag field is set to 1 by the ST25TVxxxC in the response, an Error code field is present and provides information about the error that occurred.

If an error occurs while processing a command, the ST25TxxxC remains silent instead of responding a frame with Error_flag set to 1 when :

- Inventory_flag is set to 1
- Inventory_flag, Select_flag and Address_flag are set to 0

Error codes not specified in Table 93 are reserved for future use.

Table 93. General response format when Error_flag equals 1

SOF	Response_flags	Error_code	CRC_B	EOF
-	01h	8 bits	16 bits	-

Table 94. Definition of response error codes

Error code	Description
01h	Invalid IC Mfg code value
02h	Invalid request format
03h	Invalid Request_flags value
0Fh	Error with no information given
10h	Requested data not available

Error code	Description
11h	Requested data is already locked and thus cannot be locked again
12h	Requested data is locked and its content cannot be changed
13h	Programming of requested data failed
14h	Lock of requested data failed
15h	Requested data is protected in read

6.2.7

Modes

The term “mode” refers to the mechanism used in a command to specify the set of VICC devices that must process a request with Inventory_flag set to 0. Three modes are defined depending on the values of Address_flag and Select_flag defined in [Section 6.2.3 Request flags](#).

Addressed mode

When Address_flag is set to 1 (Addressed mode), the request contains the UID (unique ID) of the addressed VICC.

Any ST25TVxxxC receiving a request with the Address_flag set to 1 compares the received UID to its own. If they match the device processes the request (if possible) and returns a response to the VCD as specified in the command description. Otherwise the device remains silent.

Select mode

When Select_flag is set to 1 (Select mode), the request frame does not contain a UID field. Only the VICC in SELECTED state that receives a request with Select_flag set to 1 processes it and returns a response to the VCD as specified in the command description.

The SELECTED state is defined in section 6.2.8. The system design ensures that only one ST25TVxxxC can be in the SELECTED state at a given time.

Non-Addressed mode (broadcast request)

When Address_flag and Select_flag are set to 0 (Non-Addressed mode), the request frame does not contain a UID field.

Several VICC may answer to a request in Non-Addressed mode, unlike the Addressed and Select modes where at most one VICC is expected to answer.

6.2.8

ISO15693 states

- POWER-OFF
- READY
- QUIET
- SELECTED

Transitions between these states are specified in [Figure 9. ISO15693 state transition diagram](#).

POWER-OFF state

The ST25TVxxxC is in RF POWER-OFF state when it does not receive enough energy from the VCD.

READY state

The ST25TVxxxC boots in READY state when it receives enough energy from the VCD.

When in the READY state, the ST25TVxxxC processes requests in Addressed, or Non-Addressed mode, or with Inventory_flag set to 1. Requests in Select mode are ignored.

QUIET state

When in the QUIET state, the ST25TVxxxC processes any request in Addressed mode. Requests in Select or Non-Addressed mode are ignored (except the ResetToReady command in Non-Addressed mode). Requests with Inventory_flag set to 1 are ignored.

SELECTED state

In the SELECTED state, the ST25TVxxxC processes requests in any addressing mode:

- Request in Select mode
- Request in Addressed mode
- Request in Non-Addressed mode
- Request with Inventory_flag set to 1

Table 95. Request_flags values depending on addressing mode

Request_flags	Non-Addressed	Select	Addressed ⁽¹⁾	Inventory ⁽¹⁾
Inventory_flag	0	0	0	1
Select_flag	0	1	0	-
Address_flag	0	0	1	-

1. assuming UID and Inventory parameter values matching the ST25TVxxxC register values.

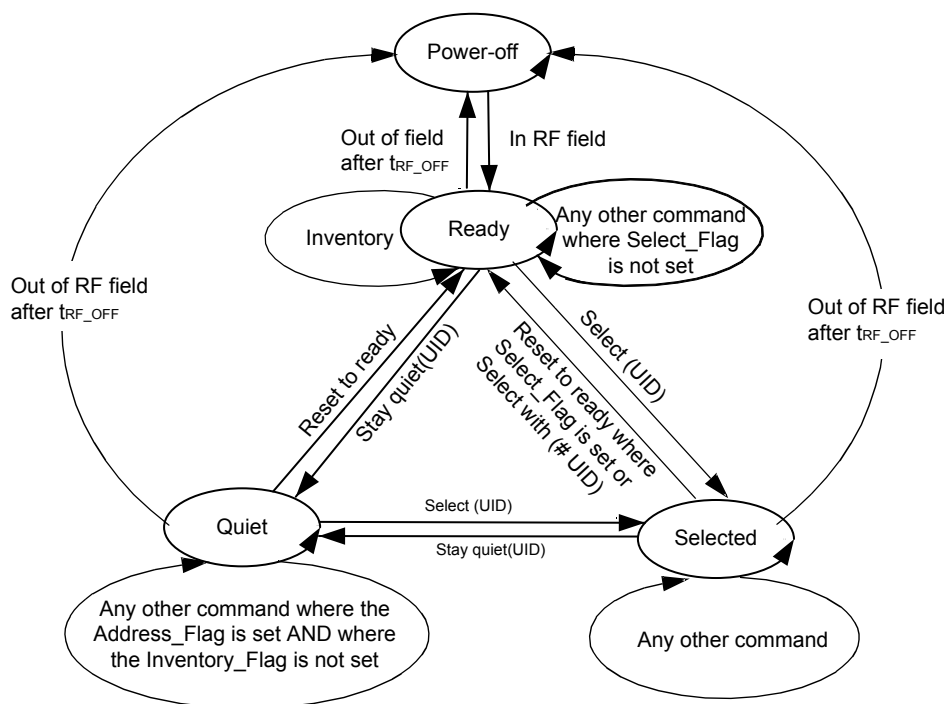
Table 96. Device response depending on state and addressing mode

ISO15693 state	Non-Addressed	Select	Addressed ⁽¹⁾	Inventory ⁽¹⁾
READY	X	-	X	X
SELECTED	X	X	X	X
QUIET	-(2)	-	X	-

1. assuming UID and Inventory parameter values matching the ST25TVxxxC register values.

2. All Non-Addressed requests are ignored in QUIET state, except the Non-Addressed ResetToReady request.

Figure 9. ISO15693 state transition diagram



The ST25TVxxxC returns to the POWER-OFF state if the tag is out of the field for at least t_{RF_OFF} . The intention of the state transition method is that only one ST25TVxxxC must be in the SELECTED state at any given time.

6.2.9 Custom states

In addition to the ISO15693 states described in the previous section, the ST25TVxxxC supports two custom states :

- UNTRACEABLE
- KILLED

Transitions with these states are specified in Figure 10.

UNTRACEABLE state

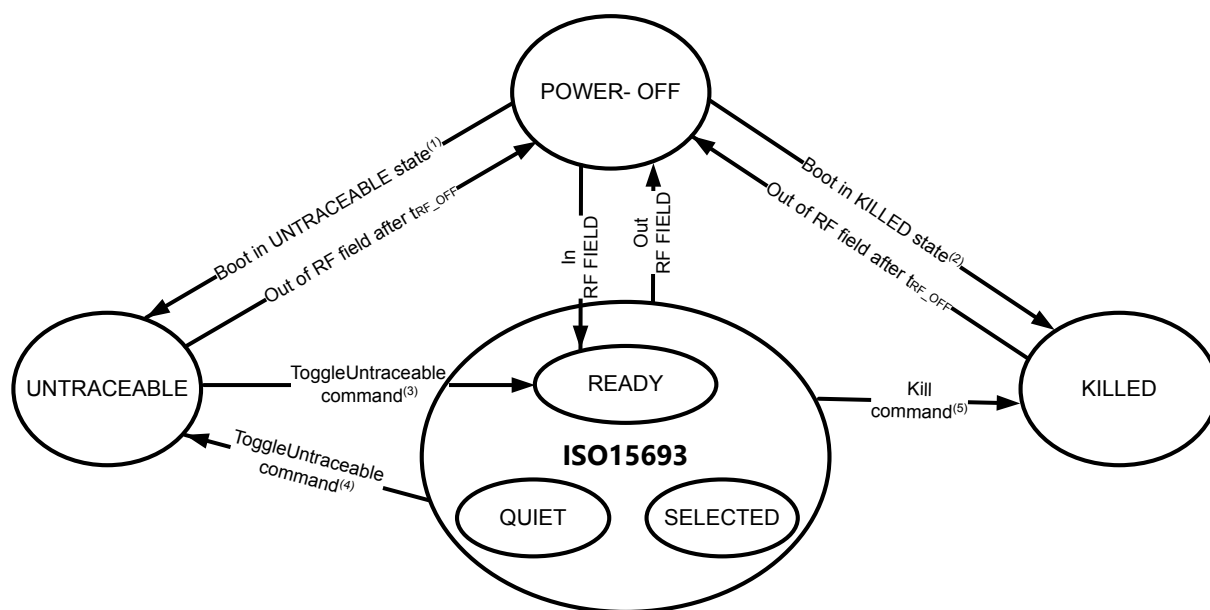
When in UNTRACEABLE state, the ST25TVxxxC ignores all incoming requests except :

- the GetRandomNumber request in Non-Addressed mode
- the ToggleUntraceable request in Non-Addressed mode
- the Inventory request if value of DIS_INV register at boot-time was 0b
- the ReadSingleBlock request in Addressed mode if value of DIS_INV register at boot-time was 0b and Block_number parameter is set to 00h

KILLED state

When in KILLED state, the ST25TVxxxC ignores all incoming requests.

Figure 10. ST25TVxxxC state transition diagram



1. ST25TVxxxC boots in UNTRACEABLE state when:

- in RF field
- the value of KILL_CMD register is 0b
- either of the following conditions is met :
 - the value of UNTR_CMD register is 1b
 - the value of UNTR_DFT register is 01b
 - the value of UNTR_DFT register is 10b with tamper loop closed
 - the value of UNTR_DFT register is 11b with tamper loop open

2. ST25TVxxxC boots in KILLED state when:
 - in RF field
 - the value of KILL_CMD register is 1b
3. ST25TVxxxC goes from UNTRACEABLE to READY state on a successful ToggleUntraceable command requested in Non-addressed mode which sets UNTR_CMD register to 0b
4. ST25TVxxxC goes from READY/SELECTED/QUIET to UNTRACEABLE state on a successful ToggleUntraceable command requested in Addressed mode which sets UNTR_CMD register to 1b
5. ST25TVxxxC goes from READY/SELECTED/QUIET to KILLED state on a successful Kill command requested in Addressed mode which permanently sets KILL_CMD register to 1b

When the ST25TVxxxC boots in **UNTRACEABLE** state, the value of UID register is masked (except in the response to a ReadConfiguration request (FID=FEh, PID=01h) where the content of the UID register is always returned without masking.) with the Untraceable UID value specified in section 7.1 until it **returns to POWER-OFF state**,

When the ST25TVxxxC boots in **READY** state and enters the UNTRACEABLE state with an explicit ToggleUntraceable command, the value of UID register is masked with the Untraceable UID value specified in [Section 7.1 Untraceable UID](#) until it **leaves the UNTRACEABLE state**.

While the ST25TV02KC is in UNTRACEABLE state:

- the value of AFI register is masked with 00h
- the value of DSFID register is masked with 00h

Note: When UID and/or AFI registers are masked, the resulting values have to be used:

- in Mask_value and AFI parameters of requests with Inventory_flag=1b
- in UID parameter of requests with Inventory_flag=0b and Address_flag=1b

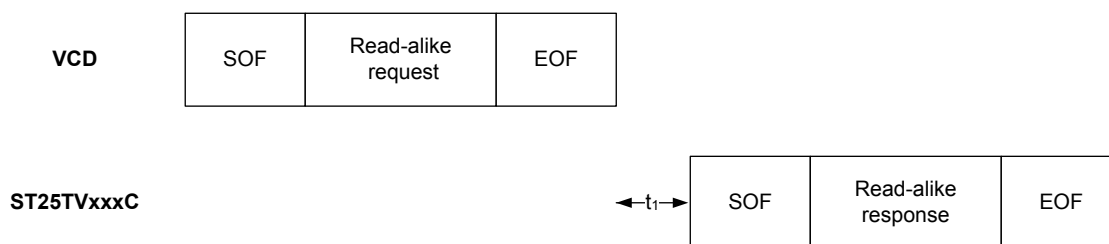
6.3 Timing definition

Note: The tolerance on a specific timing is $\pm 32/f_C$

t₁: VICC response delay for read-alike commands

For a read-alike command - example a command not invoking a programming of the EEPROM - the VICC waits for a time t₁ starting at the rising edge of the EOF in the request received from the VCD, before transmitting its response. Values of t₁ are given in [Table 97. Timing values](#).

Figure 11. Read-alike frame exchange between VCD and ST25TVxxxC



t₂: VCD new request delay

t₂ is the time after which the VCD may send an EOF to switch to the next slot when one or more VICC responses have been received after an Inventory request with Nb_slots_flag set to 0. It starts from the reception of the EOF from the VICCs.

The EOF sent by the VCD may be either 10% or 100% modulated regardless of the modulation index used for transmitting the VCD request to the VICC.

t_2 is also the time after which the VCD may send a new request to the VICC, as described in [Figure 8. ISO15693 protocol timing](#).

Values of t_2 are given in [Table 97. Timing values](#).

t_3 : VCD new request delay when no response is received from the VICC

t_3 is the time after which the VCD may send an EOF to switch to the next slot when no response has been received from the VICC after an Inventory request with Nb_slots_flag set to 0.

The EOF sent by the VCD may be either 10% or 100% modulated regardless of the modulation index used for transmitting the VCD request to the VICC.

Starting from the rising edge of the request EOF sent by the VCD:

- If this EOF is 100% modulated, the VCD waits for a time at least equal to t_{3min} for 100% modulation before sending a new EOF.
- If this EOF is 10% modulated, the VCD waits for a time at least equal to t_{3min} for 10% modulation before sending a new EOF.

Table 97. Timing values

-	Minimum (min) values		Nominal (nom) values	Maximum (max) values
	100% modulation	10% modulation		
t_1	4320 / $f_C = 318.6 \mu s$		4352 / $f_C = 320.9 \mu s$	4384 / $f_C = 323.3 \mu s^{(1)}$
t_2	4192 / $f_C = 309.2 \mu s$		No	No
t_3	$t_{1max}^{(2)} + t_{SOF}^{(3)}$	$t_{1max}^{(2)} + t_{NRT}^{(4)} + t_{2min}$	No t_{3nom}	No t_{3max}
t_{EOF}	10 ms	No	t_{EOFnom}	20 ms

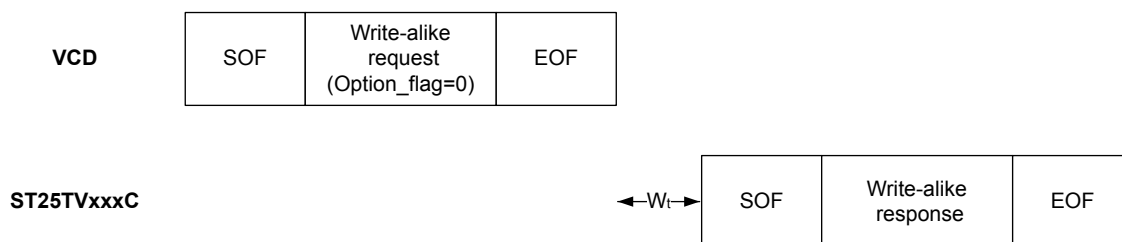
1. VCD request is not interpreted during the first milliseconds following the field rising.
2. t_{1max} does not apply for write-alike commands. Specific timing constraints for write-alike commands are defined by W_t and t_{EOF} (see below).
3. t_{SOF} is the time taken by the VICC to transmit an SOF to the VCD. t_{SOF} depends on the response data rate: High data rate or Low data rate.
4. t_{NRT} is the nominal response time of the VICC. t_{NRT} depends on the response data rate, the subcarrier modulation mode, and the size of expected response frame.

W_t : VICC response delay for write-alike commands with Option_flag=0

For a write-alike command with option_flag=0, for instance a command involving a programming of the EEPROM, the VICC waits for a time W_t starting at the rising edge of the EOF in the request received from the VCD, before transmitting its response.

The W_t time is equal to $t_{1nom} + a \text{ multiple of } 4096 / f_C (= 302 \mu s)$.

Figure 12. Write-alike frame exchange between VCD and ST25TVxxxC when Option_flag=0

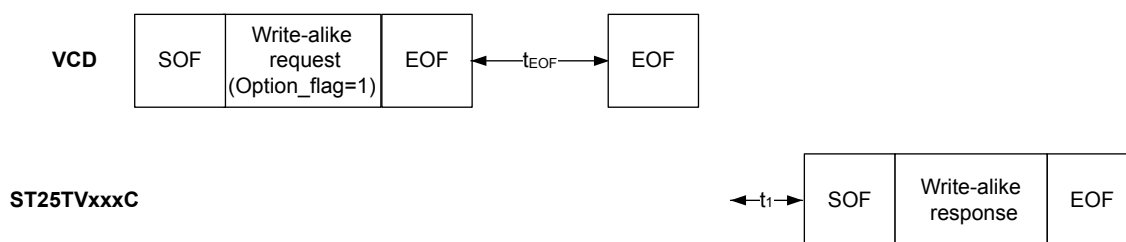


t_{EOF} : EOF request delay for write-alike commands with Option_flag=1

For a write-alike command with Option_flag=1, the VCD waits for a time t_{EOF} starting at the rising edge of the EOF in the request frame, before sending an isolated EOF request which triggers the response of the VICC. Upon reception of the isolated EOF request, the VICC waits for a time t_1 starting at the rising edge of the isolated EOF request, before transmitting its response.

Authorized values of t_{EOF} are given in [Table 97. Timing values.](#)

Figure 13. Write-alike frame exchange between VCD and ST25TVxxxC when Option_flag=1



6.4 RF commands

The ST25TVxxxC supports the following RF command set:

- **Inventory**, used to perform the anticollision sequence.
- **StayQuiet**, used to put the ST25TVxxxC in QUIET state, where it responds only to commands in Addressed mode.
- **ReadSingleBlock**, used to read the 32 bits of a block and its locking status.
- **WriteSingleBlock**, used to write and verify the new content for an update of a 32 bits block, provided that the write access is granted.
- **LockBlock**, used to permanently forbid the write access to the selected block.
- **ReadMultipleBlocks**, used to read the content of a range of blocks and their locking status.
- **Select**, used to put the ST25TVxxxC in SELECTED state. After this command, the ST25TVxxxC processes all commands requested with Select_flag set.
- **ResetToReady**, used to put the ST25TVxxxC in the READY state.
- **WriteAFI**, used to write an 8-bit value in the AFI register.
- **LockAFI**, used to lock the AFI register.
- **WriteDSFID**, used to write an 8-bit value in the DSFID register.
- **LockDSFID**, used to lock the DSFID register.
- **GetSystemInfo** and **ExtendedGetSystemInfo**, used to read the standard system information values.
- **GetMultipleBlockSecurityStatus**, used to read the security status of a range blocks.
- **ReadConfig**, used to read configuration registers.
- **WriteConfig**, used to write configuration registers.
- **Kill**, used to permanently deactivate the tag by entering the KILLED state.
- **WritePassword**, used to change password of an open security session.
- **PresentPassword**, used to open a security session.
- **GetRandomNumber**, used to generate a 16 bit number.
- **ToggleUntraceable**, used to enter or leave the UNTRACEABLE state.
- **Initiate**, used to set the Initiate_flag register to 1.
- **InventoryInitiated**, used to perform the anticollision sequence on ST25TVxxxC with Initiate_flag set to 1.

Their codes are given in [Table 98](#).

Table 98. Command code

Opcode	Command	Opcode	Command
01h	Inventory	2Bh	GetSystemInfo
02h	StayQuiet	2Ch	GetMultipleBlockSecurityStatus
20h	ReadSingleBlock	3Bh	ExtendedGetSystemInfo
21h	WriteSingleBlock	A0h	ReadConfig
22h	LockBlock	A1h	WriteConfig
23h	ReadMultipleBlocks	A6h	Kill
25h	Select	B1h	WritePassword
26h	ResetToReady	B3h	PresentPassword
27h	WriteAFI	B4h	GetRandomNumber
28h	LockAFI	BAh	ToggleUntraceable
29h	WriteDSFID	D1h	InventoryInitiated
2Ah	LockDSFID	D2h	Initiate

6.4.1 Inventory

When receiving the Inventory request, the ST25TVxxxC sends a response if the parameters match the values of the UID and AFI registers.

Inventory_flag is set to 1 : bits 4 and 5 of Request_flags respectively code AFI_flag and Nb_slots_flag.

Option_flag is set to 0 : no option supported.

Table 99. Inventory request format

SOF	Request_flags	Opcode	AFI ⁽¹⁾	Mask_length	Mask_value	CRC_B	EOF
-	00xx01xxb	01h	8 bits	8 bits	0-64 bits	16 bits	-

1. AFI field present when Request_flags=00x101xxb.

Request parameters and data include:

- AFI parameter if AFI_flag is set to 1
- Mask_length in bits, ≤ 60 when Nb_slots_flag = 0b, ≤ 64 when Nb_slots_flag = 1b
- Mask_value, size in bytes is $(\text{Mask_length} + 7)/8$, not present if Mask_length = 00h

Table 100. Inventory response format

SOF	Response_flags	DSFID	UID	CRC_B	EOF
-	00h	8 bits	64 bits	16 bits	-

When Error_flag is set to 0, response data include:

- DSFID register value
- UID register value

The ST25TVxxxC does not generate any answer in case of error.

When the VICC responds to an Inventory request, the timing of the frame exchange is that of a read-alike command as depicted in [Figure 11. Read-alike frame exchange between VCD and ST25TVxxxC](#).

When Nb_slots_flag is set to 0, the VCD issues 15 EOF requests after the initial request from [Table 99. Inventory request format](#), with the following timings described in [Section 6.3 Timing definition](#):

- if the VICC responds to an EOF request, the timing of the frame exchange is that of a read-alike command
- if the VCD receives a response from one or more VICCs, it waits for a time t_2 before sending the next EOF request
- if the VCD does not receive a response from any VICC, it waits for a time t_3 before sending the next EOF request

6.4.2 StayQuiet

When receiving the StayQuiet request:

- the ST25TVxxxC enters the QUIET state if no error occurs, and does NOT send back a response.
- there is NO response to the StayQuiet command even if an error occurs.

Select_flag is set to 0 and Address_flag is set to 1 : the StayQuiet request must be issued in Addressed mode.

Option_flag is set to 0 : no option supported.

Table 101. StayQuiet request format

SOF	Request_flags	Opcode	UID	CRC_B	EOF
-	001000xxb	02h	64 bits	16 bits	-

Request parameters and data include :

- UID parameter

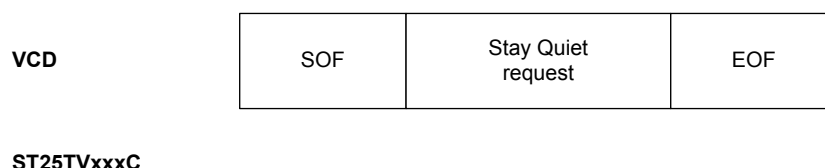
When in QUIET state:

- the ST25TVxxxC does not process any request if Inventory_flag is set to 1,
- the ST25TVxxxC processes only requests with Address_flag set to 1.

The ST25TVxxxC exits the QUIET state:

- when it is reset (power off).
- on a successful Select request, it then goes to the SELECTED state.
- on a successful ResetToReady request, it then goes to the READY state.

Figure 14. Stay Quiet frame



6.4.3 ReadSingleBlock

When receiving the ReadSingleBlock request, the ST25TVxxxC reads the requested block and sends back its 32-bit value in the response.

ReadSingleBlock command is applicable and successful, if and only if the requested block is available and has granted read access (ie, parent area not protected in Read or security session open).

When Option_flag is set to 1, the Block Security Status of the requested block is included in the response.

Table 102. ReadSingleBlock request format

SOF	Request_flags	Opcode	UID ⁽¹⁾	Block_number	CRC_B	EOF
-	0xxx00xxb	20h	64 bits	8 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb.

Request parameters and data include :

- UID parameter if Address_flag is set to 1
- Block_number coded on 1 byte

Table 103. ReadSingleBlock response format when Error_flag equals 0

SOF	Response_flags	BSS ⁽¹⁾	Data	CRC_B	EOF
-	00h	8 bits	32 bits	16 bits	-

1. BSS field present when Request_flags=01xx00xxb.

When Error_flag is set to 0, response data include :

- Block security status if Option_flag is set to 1 (see [Table 31. Block security status](#))
- Four bytes of block data

Note: The Data field from [Table 103](#) may be impacted by the ANDEF feature (see [Section 5.4.2 Augmented NDEF description](#))

When Error_flag is set to 1, Error_code field may take the values of [Table 104](#) in a ReadSingleBlock response.

Table 104. ReadSingleBlock error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value
10h	Requested block not available
15h	Read access to requested block is protected and security session is closed

When the VICC responds to a ReadSingleBlock request, the timing of the frame exchange is that of a read-alike command as depicted in [Figure 11. Read-alike frame exchange between VCD and ST25TVxxxC](#).

6.4.4 WriteSingleBlock

When receiving the WriteSingleBlock request, the ST25TVxxxC writes the data contained in the request to the targeted block and reports whether the write operation was successful in the response.

WriteSingleBlock command is applicable and successful, if and only if the requested block is available and has granted write access (ie, the block is not locked, area not protected in Write or security session open).

When Option_flag is set to 1, the response is postponed to the subsequent EOF request.

Table 105. WriteSingleBlock request format

SOF	Request_flags	Opcode	UID ⁽¹⁾	Block_number	Data	CRC_B	EOF
-	0xxx00xxb	21h	64 bits	8 bits	32 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb.

Request parameters and data include :

- UID parameter if Address_flag is set to 1
- Block_number coded on 1 byte
- Four bytes of block data

Note: The Data field from [Table 105](#) is not impacted by the ANDEF feature (see [Section 5.4.2 Augmented NDEF description](#))

Table 106. WriteSingleBlock response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0, no data is inserted between the Response_flags and CRC_B fields.

When Error_flag is set to 1, Error_code field may take the values of [Table 107](#) in a WriteSingleBlock response.

Table 107. WriteSingleBlock error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value
10h	Requested block not available
12h	Write access to requested block is protected and security session is closed
13h	Programming of requested block failed

When the VICC responds to a WriteSingleBlock request, the timing of the frame exchange is that of a write-alike command as depicted in [Figure 12](#) and [Figure 13](#).

During the RF write cycle W_t , there should be no modulation (neither 100% nor 10%), otherwise the ST25TVxxxC may not correctly program the data into the memory.

6.4.5 LockBlock

When receiving the LockBlock request, the ST25TVxxxC locks the corresponding block value permanently to protect its content against new writing.

LockBlock command is applicable and successful, if and only if the requested block is available and has granted write access (ie, the block is not locked, area not protected in Write or security session open).

When Option_flag is set to 1, the response is postponed to the subsequent EOF request.

Table 108. LockBlock request format

SOF	Request_flags	Opcode	UID ⁽¹⁾	Block_number	CRC_B	EOF
-	0xxx00xxb	22h	64 bits	8 bits	16 bits	-

1. UID field present when Request_flags = 0x1000xxb.

Request parameters and data include :

- UID parameter if Address_flag is set to 1
- Block_number coded on 1 byte

Table 109. LockBlock response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0, no data is inserted between the Response_flags and CRC_B fields.

When Error_flag is set to 1, Error_code field may take the values of Table 110 in a LockBlock response.

Table 110. LockBlock error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value
10h	Requested block not available
11h	Requested block is already locked
12h	Write access to requested block is protected and security session is closed
14h	Lock of requested block failed

When the VICC responds to a LockBlock request, the timing of the frame exchange is that of a write-alike command as depicted in Figure 12 and Figure 13.

During the RF write cycle W_t , there should be no modulation (neither 100% nor 10%), otherwise the ST25TVxxxC may not correctly program the LCK_BLOCK register into the memory.

6.4.6 ReadMultipleBlocks

When receiving the ReadMultipleBlocks request, the ST25TVxxxC reads the selected blocks and sends back their value in multiples of 32 bits in the response.

ReadMultipleBlocks command is applicable and successful, if and only if the first block requested is available and has granted read access (ie, parent area not protected in Read or security session open).

When the requested range of blocks ends beyond the user memory or in an area without read access authorized, the range of blocks used for the response data is truncated before the first block not available / not readable.

When Option_flag is set to 1, the Block Security Status of the blocks read are included in the response.

Table 111. ReadMultipleBlocks request format

SOF	Request_flags	Opcode	UID ⁽¹⁾	Block_number	Additional_blocks	CRC_B	EOF
-	0xxx00xxb	23h	64 bits	8 bits	8 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb.

Request parameters and data include :

- UID parameter if Address_flag is set to 1
- Block_number coded on 1 byte, requested range of blocks starts at Block_number
- Additional_blocks coded on 1 byte, requested range of blocks ends at Block_number + Additional_blocks

Table 112. ReadMultipleBlocks response format when Error_flag equals 0

SOF	Response_flags	BSS ⁽¹⁾	Data	CRC_B	EOF
-	00h	8 bits ⁽²⁾	32 bits ⁽²⁾	16 bits	-

1. BSS field present when Request_flags=01xx00xxb

2. Repeated as needed.

When Error_flag is set to 0, response data include for each block :

- Block security status if Option_flag is set to 1 (see [Table 31. Block security status](#))
- Four bytes of block data

Note:

The Data field from [Table 112](#) may be impacted by the ANDEF feature (see [Section 5.4.2 Augmented NDEF description](#))

When Error_flag is set to 1, Error_code field may take the values of [Table 113](#) in a ReadMultipleBlocks response.

Table 113. ReadMultipleBlocks error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value
10h	Requested block not available
15h	Read access to requested block is protected and security session is closed

When the VICC responds to a ReadMultipleBlocks request, the timing of the frame exchange is that of a read-alike command as depicted in [Figure 11. Read-alike frame exchange between VCD and ST25TVxxxC](#).

6.4.7

Select

When receiving the Select request:

- If the UID parameter matches its own UID, the ST25TVxxxC enters or stays in the SELECTED state and sends a response.
- If the UID parameter does not match its own UID, the selected ST25TVxxxC returns to the READY state and does not send a response.
- If an error occurs, the ST25TVxxxC remains in its current state.

Select_flag is set to 0 and Address_flag is set to 1 : the Select request must be issued in Addressed mode.

Option_flag is set to 0 : no option supported.

Table 114. Select request format

SOF	Request_flags	Opcode	UID	CRC_B	EOF
-	001000xxb	25h	64 bits	16 bits	-

Request parameters and data include :

- UID parameter

Table 115. Select response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

- When Error_flag is set to 0, no data is inserted between the Response_flags and CRC_B fields.
- When Error_flag is set to 1, Error_code field may take the values of [Table 116](#) in a Select response.

Table 116. Select error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value

When the VICC responds to a Select request, the timing of the frame exchange is that of a read-alike command as depicted in [Figure 11. Read-alike frame exchange between VCD and ST25TVxxxC](#).

6.4.8

ResetToReady

When receiving the ResetToReady request:

- the ST25TVxxxC enters or stays in the READY state if no error occurs.
- in SELECTED state, the ST25TVxxxC responds an error when Addressed mode is used.
- in QUIET state, the ST25TVxxxC handles the request even if Non-addressed mode is used.
- If an error occurs, the ST25TVxxxC remains in its current state.

Option_flag is set to 0 : no option supported.

Table 117. ResetToReady request format

SOF	Request_flags	Opcode	UID ⁽¹⁾	CRC_B	EOF
-	00xx00xxb	26h	64 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb.

Request parameters and data include:

- UID parameter if Address_flag is set to 1

Table 118. ResetToReady response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0, no data is inserted between the Response_flags and CRC_B fields.

When Error_flag is set to 1, Error_code field may take the values of [Table 119](#) in a ResetToReady response.

Table 119. ResetToReady error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value

When the VICC responds to a ResetToReady request, the timing of the frame exchange is that of a read-alike command as depicted in [Figure 11. Read-alike frame exchange between VCD and ST25TVxxxC](#).

6.4.9

WriteAFI

When receiving the WriteAFI request, the ST25TVxxxC programs the 8-bit AFI register.

WriteAFI command is applicable and successful, if and only if the WriteAFI command is allowed (ie, AFI is not locked, AFI_PROT=0b or AREA1 security session open).

When Option_flag is set to 1, the response is postponed to the subsequent EOF request.

Table 120. WriteAFI request format

SOF	Request_flags	Opcode	UID ⁽¹⁾	AFI	CRC_B	EOF
-	0xxx00xxb	27h	64 bits	8 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb.

Request parameters and data include:

- UID parameter if Address_flag is set to 1
- AFI parameter coded on 1 byte, used to program the AFI register

Table 121. WriteAFI response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0, no data is inserted between the Response_flags and CRC_B fields.

When Error_flag is set to 1, Error_code field may take the values of [Table 122](#) in a WriteAFI response.

Table 122. WriteAFI error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value
12h	LCK_AFI=1b or (AFI_PROT=1b and AREA1 security session is closed)
13h	Programming of AFI register failed

When the VICC responds to a WriteAFI request, the timing of the frame exchange is that of a write-alike command as depicted in [Figure 12](#) and [Figure 13](#).

During the RF write cycle Wt, there should be no modulation (neither 100% nor 10%), otherwise the ST25TVxxxC may not correctly program the AFI register into the memory.

6.4.10

LockAFI

When receiving the LockAFI request, the ST25TVxxxC locks the AFI register permanently.

LockAFI command is applicable and successful, if and only if the LockAFI command is allowed (ie, AFI not already locked, AFI_PROT=0b or AREA1 security session open).

When Option_flag is set to 1, the response is postponed to the subsequent EOF request.

Table 123. LockAFI request format

SOF	Request_flags	Opcode	UID ⁽¹⁾	CRC_B	EOF
-	0xxx00xxb	28h	64 bits	16 bits	-

1. *UID field present when Request_flags=0x1000xxb.*

Request parameters and data include :

- UID parameter if Address_flag is set to 1

Table 124. LockAFI response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0, no data is inserted between the Response_flags and CRC_B fields.

When Error_flag is set to 1, Error_code field may take the values of Table 125 in a LockAFI response.

Table 125. LockAFI error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value
11h	LCK_AFI=1b : Successful LockAFI command already occurred
12h	AFI_PROT=1b and AREA1 security session is closed
14h	Programming of LCK_AFI register failed

When the VICC responds to a LockAFI request, the timing of the frame exchange is that of a write-alike command as described in Figure 12 and Figure 13.

During the RF write cycle Wt, there should be no modulation (neither 100% nor 10%), otherwise the ST25TVxxxC may not correctly program the LCK_AFI register into the memory.

6.4.11

WriteDSFID

When receiving the WriteDSFID request, the ST25TVxxxC programs the 8-bit DSFID register. WriteDSFID command is applicable and successful, if and only if the DSFID register is not locked (LCK_DSFID=0b).

When Option_flag is set to 1, the response is postponed to the subsequent EOF request.

Table 126. WriteDSFID request format

SOF	Request_flags	Opcode	UID ⁽¹⁾	DSFID	CRC_B	EOF
-	0xxx00xxb	29h	64 bits	8 bits	16 bits	-

1. *UID field present when Request_flags=0x1000xxb*

Request parameters and data include:

- UID parameter if Address_flag is set to 1.
- DSFID parameter coded on 1 byte, used to program the DSFID register

Table 127. WriteDSFID response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0, no data is inserted between the Response_flags and CRC_B fields.

When Error_flag is set to 1, Error_code field may take the values of Table 128 in a WriteDSFID response.

Table 128. WriteDSFID error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value
12h	LCK_DSFID=1b : DSFID register is locked
13h	Programming of DSFID register failed

When the VICC responds to a WriteDSFID request, the timing of the frame exchange is that of a write-alike command as described in [Figure 12](#) and [Figure 13](#).

During the RF write cycle W_t , there should be no modulation (neither 100% nor 10%), otherwise the ST25TVxxxC may not correctly program the DSFID register into the memory.

6.4.12

LockDSFID

When receiving the LockDSFID request, the ST25TVxxxC locks the DSFID register permanently. LockDSFID command is applicable and successful, if and only if the DSFID register is not already locked (LCK_DSFID=0b).

When Option_flag is set to 1, the response is postponed to the subsequent EOF request.

Table 129. LockDSFID request format

SOF	Request_flags	Opcode	UID ⁽¹⁾	CRC_B	EOF
-	0xxx00xxb	2Ah	64 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb

Request parameters and data include:

- UID parameter if Address_flag is set to 1

Table 130. LockDSFID response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0, no data is inserted between the Response_flags and CRC_B fields.

When Error_flag is set to 1, Error_code field may take the values of [Table 131](#) in a LockDSFID response.

Table 131. LockDSFID error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value
11h	LCK_DSFID=1b : Successful LockDSFID command already occurred
14h	Programming of LCK_DSFID register failed

When the VICC responds to a LockDSFID request, the timing of the frame exchange is that of a write-alike command as depicted in [Figure 12](#) and [Figure 13](#).

During the RF write cycle W_t , there should be no modulation (neither 100% nor 10%), otherwise the ST25TVxxxC may not correctly program the LCK_DSFID register into the memory.

6.4.13 GetSystemInfo

When receiving the GetSystemInfo request, the ST25TVxxxC sends back its information data in the response. Option_flag is set to 0 : no option supported.

Table 132. GetSystemInfo request format

SOF	Request_flags	Opcode	UID ⁽¹⁾	CRC_B	EOF
-	00xx00xxb	2Bh	64 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb

Request parameters and data include:

- UID parameter if Address_flag is set to 1

Table 133. GetSystemInfo response

SOF	Response_flags	Information_flags	UID	DSFID	AFI	Memory_size	IC_ref	CRC_B	EOF
-	00h	0Fh	64 bits	8 bits	8 bits	16 bits	08h	16 bits	-

When Error_flag is set to 0, response data include :

- Information_flags coded on 1 byte, set to 0Fh (DSFID, AFI, Memory_size and IC_ref fields are all present).
- UID register value
- DSFID register value
- AFI register value
- Memory_size coded on 2 bytes:
 - 8-MSB (03h) = Block size in number of Bytes - 1
 - 8-LSB (END_MEM) = User memory size in number of Blocks - 1
- IC_REF register value

When Error_flag is set to 1, Error_code field may take the values of Table 134 in a GetSystemInfo response.

Table 134. GetSystemInfo error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value

When the VICC responds to a GetSystemInfo request, the timing of the frame exchange is that of a read-alike command as depicted in Figure 11.

6.4.14 GetMultipleBlockSecurityStatus

When receiving the GetMultipleBlockSecurityStatus request, the ST25TVxxxC responds the block security status of the selected blocks.

GetMultipleBlockSecurityStatus command is applicable and successful, if and only if the first block requested is available.

When the requested range of blocks ends beyond the user memory, the range of blocks used for the response data is truncated to the last block available.

Option_flag is set to 0 : no option supported.

Table 135. GetMultipleBlockSecurityStatus request format

SOF	Request_flags	Opcode	UID ⁽¹⁾	Block_number	Additional_blocks	CRC_B	EOF
-	00x00xxb	2Ch	64 bits	8 bits	8 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb

Request parameters and data include :

- UID parameter if Address_flag is set to 1
- Block_number coded on 1 byte, requested range of blocks starts at Block_number
- Additional_blocks coded on 1 byte, requested range of blocks ends at Block_number + Additional_blocks

Table 136. GetMultipleBlockSecurityStatus response format when Error_flag equals 0

SOF	Response_flags	BSS	CRC_B	EOF
-	00h	8 bits ⁽¹⁾	16 bits	-

1. Repeated as needed

When Error_flag is set to 0, response data include for each block :

- Block security status (see Table 31. Block security status)

When Error_flag is set to 1, Error_code field may take the values of Table 137 in a GetMultipleBlockSecurityStatus response.

Table 137. GetMultipleBlockSecurityStatus error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags value
10h	Requested block not available

When the VICC responds to a GetMultipleBlockSecurityStatus request, the timing of the frame exchange is that of a read-alike command as depicted in Figure 11.

6.4.15

ExtendedGetSystemInfo

When receiving the ExtendedGetSystemInfo request, the ST25TVxxxC sends back its information data in the response.

Option_flag is set to 0 : no option supported.

Table 138. ExtendedGetSystemInfo request format

SOF	Request_flags	Opcode	Information_request_list	UID ⁽¹⁾	CRC_B	EOF
-	00x00xxb	3Bh	0xx1xxxxb	64 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb

Request parameters and data include :

- Information_request_list parameter coded on 1 byte, see Table 139 below
- UID parameter if Address_flag is set to 1

Table 139. Information_request_list content

Bit	Requested information	Description
b0	DSFID	0: DSFID not requested 1: DSFID requested
b1	AFI	0: AFI not requested 1: AFI requested
b2	Memory_size	0: VICC memory size not requested 1: VICC memory size requested
b3	IC_ref	0: IC reference not requested 1: IC reference requested
b4	MOI	1: Information on MOI always returned in response flag
b5	Command_list	0: list of supported commands not requested 1: list of supported commands requested
b6	CSI information	0: CSI list not requested 1: CSI list requested
b7	Ext_list	0: size of Information_request_list is 1 byte

Table 140. ExtendedGetSystemInfo response format when Error_flag equals 0

SOF	Response_flags	Information_flags	UID	Information_fields	CRC_B	EOF
-	00h	00x0xxxxb	64 bits	up to 80 bits	16 bits	-

Table 141. Information_flags content

Bit	Responded information	Description
b0	DSFID	0: DSFID not present in Information_fields 1 : DSFID present in Information_fields
b1	AFI	0: AFI not present in Information_fields 1: AFI present in Information_fields
b2	Memory_size	0: Memory_size not present in Information_fields 1: Memory_size present in Information_fields
b3	IC_ref	0: IC_ref not present in Information_fields 1: IC_ref present in Information_fields
b4	MOI	0: 1 byte addressing
b5	Command_list	0: Command_list not present in Information_fields 1: Command_list present in Information_fields
b6	CSI_information	0: CSI list not present
b7	Ext_info	0: size of Information_flags is 1 byte

Table 142. Information_fields content

DSFID ⁽¹⁾	AFI ⁽¹⁾	Memory_size ⁽¹⁾	IC_ref ⁽¹⁾	Command_list ⁽¹⁾
8 bits	8 bits	24 bits	08h	00003FEFh

1. Presence of information fields depends on value of Information_flags

When Error_flag is set to 0, response data include :

- Information_flags coded on 1 byte, defining which fields are present (see Table 141)
- UID register value
- DSFID register value, present if Information_flags[0]=1b
- AFI register value, present if Information_flags[1]=1b
- VICC Memory size coded on 3 bytes, present if Information_flags[2]=1b
 - 8-MSB (03h) = Block size in number of Bytes - 1
 - 16-LSB (END_MEM) = User memory size in number of Blocks - 1
- IC_REF register value, present if Information_flags[3]=1b
- VICC Command list coded on 4 bytes, present if Information_flags[5]=1b

When Error_flag is set to 1, Error_code field may take the values of Table 143 in an ExtendedGetSystemInfo response.

Table 143. ExtendedGetSystemInfo error codes when Error_flag equals 1

Error code	Description
02h	Invalid request format
03h	Invalid Request_flags or Information_request_list value

When the VICC responds to an ExtendedGetSystemInfo request, the timing of the frame exchange is that of a read-alike command as depicted in Figure 11.

6.4.16

ReadConfiguration

When receiving the ReadConfiguration request, the ST25TVxxxC reads the selected configuration register and sends back its value in the response.

ReadConfiguration command is applicable and successful, if and only if the requested configuration register (identified by the FID/PID pair) is available and has granted read access (i.e. read not protected, or feature not locked and CONFIG security session open).

Option_flag is set to 0 : no option supported.

Table 144. ReadConfiguration request format

SOF	Request_flags	Opcode	IC Mfg code	UID ⁽¹⁾	FID	PID	CRC_B	EOF
-	00xx00xxb	A0h	02h	64 bits	8 bits	8 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb

Request parameters and data include :

- IC manufacturer code coded on 1 byte, value shall be 02h
- UID parameter if Address_flag is set to 1
- FID parameter coded on 1 byte
- PID parameter coded on 1 byte

Table 145. ReadConfiguration response format when Error_flag equals 0

SOF	Response_flags	Data ⁽¹⁾	CRC_B	EOF
-	00h	8 to 64 bits	16 bits	-

1. Size of data responded depends on the requested FID and PID values according to Table 4. List of configuration registers

When Error_flag is set to 0, response data include :

- Configuration register value coded on 1 to 8 bytes depending on the requested FID/PID pair (see Table 4. List of configuration registers)

Note: When a register value is coded on several bytes, it is transmitted in LSB to MSB byte order in the response to a ReadConfiguration request.

When Error_flag is set to 1, Error_code field may take the values of Table 146 in a ReadConfiguration response.

Table 146. ReadConfiguration error codes when Error_flag equals 1

Error code	Description
01h	Invalid IC Mfg code value
02h	Invalid request format
03h	Invalid Request_flags value
10h	Requested FID/PID not available
15h	Read access to requested FID/PID is protected and CONFIG security session is closed

When the VICC responds to a ReadConfiguration request, the timing of the frame exchange is that of a read-alike command as depicted in Figure 11.

6.4.17 WriteConfiguration

When receiving the WriteConfiguration request, the ST25TVxxxC writes the data contained in the request to the selected configuration register and responds an acknowledgement if the write operation was successful.

WriteConfiguration command is applicable and successful, if and only if the requested configuration register (identified by the FID/PID pair) is available and has granted write access (i.e. feature not locked and CONFIG security session open).

When Option_flag is set to 1, the response is postponed to the subsequent EOF request.

Table 147. WriteConfiguration request format

SOF	Request_flags	Opcode	IC Mfg code	UID ⁽¹⁾	FID	PID	Data	CRC_B	EOF
-	0xxx00xxb	A1h	02h	64 bits	8 bits	8 bits	8-32 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb

Request parameters and data include :

- IC manufacturer code coded on 1 byte, value shall be 02h
- UID parameter if Address_flag is set to 1
- FID parameter coded on 1 byte
- PID parameter coded on 1 byte
- New register value coded on 1 to 4 bytes depending on the requested FID/PID pair (see Table 4. List of configuration registers)

Note: When a register value is coded on several bytes, it is transmitted in LSB to MSB byte order in the WriteConfiguration request.

Table 148. WriteConfiguration response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0:

- no data is inserted between the Response_flags and CRC_B fields.
- the update of the register value into the memory is successful, and the new value is immediately readable with a ReadConfiguration request. However the effect of the new value may be active immediately or on the next RF boot sequence depending on the selected configuration (see column Activation time of Table 4. List of configuration registers).

When the effect of a new configuration register value is activated on the next RF boot sequence, the effect of the former configuration value lasts after the update of the register into the memory until the ST25TVxxxC is put in POWER-OFF state.

When Error_flag is set to 1, Error_code field may take the values of [Table 149](#) in a WriteConfiguration response.

Table 149. WriteConfiguration error codes when Error_flag equals 1

Error code	Description
01h	Invalid IC Mfg code value
02h	Invalid request format
03h	Invalid Request_flags value
10h	Requested FID/PID not available
11h	Bit of LCK_CONFIG (FID=FFh,PID=00h) already set to 1b
12h	Write access to requested FID/PID is protected and CONFIG security session is closed
13h	Programming of requested FID/PID (other than LCK_CONFIG) failed
14h	Programming of LCK_CONFIG (FID=FFh,PID=00h) failed

When the VICC responds to a WriteConfiguration request, the timing of the frame exchange is that of a write-alike command as depicted in [Figure 12](#) and [Figure 13](#).

During the RF write cycle Wt, there should be no modulation (neither 100% nor 10%), otherwise the ST25TVxxxC may not correctly program the configuration register into the memory.

6.4.18

WritePassword

When receiving the WritePassword request, the ST25TVxxxC uses the data contained in the request to modify the selected password and responds an acknowledgement if the write operation was successful.

WritePassword command is applicable and successful, if and only if it preceded by a successful PresentPassword command with same password selected. Refer to [Section 5.1.2 Password management](#) for details on password management.

When Option_flag is set to 1, the response is postponed to the subsequent EOF request.

Table 150. WritePassword request format

SOF	Request_flags	Opcode	IC Mfg code	UID ⁽¹⁾	Password_id	Password_data	CRC_B	EOF
-	0xxx00xxb	B1h	02h	64 bits	8 bits	32 or 64 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb

Request parameters and data include :

- IC manufacturer code coded on 1 byte, value shall be 02h
- UID parameter if Address_flag is set to 1
- Password_id coded on 1 byte
- Password_data coded on 4 or 8 bytes according to [Table 27. List of password registers](#)

The Password_data value is obtained from the encryption of the new plain value of the password as described in [Section 5.1.3 Password encryption](#).

Danger:

If a plain value is mistakenly used in the Password_data field of the WritePassword command, the presentation of its encrypted value with the PresentPassword command fails on the ST25TVxxxC device.

Note:

The behavior of the WritePassword command is different between the ST25TVxxx and ST25TVxxxC devices regarding the encryption of the Password_data field. The Password_data field is a plain password value on the ST25TVxxx device described in datasheet DS12074, while it is an encrypted password value on the ST25TVxxxC device described in this document.

It is recommended to issue the WritePassword request in Addressed or Select mode, in order to improve the system robustness.

This ensures that password change is only applied to a specific tag/UID.

Table 151. WritePassword response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0:

- no data is inserted between the Response_flags and CRC_B fields.
- the update of the password into the memory is successful, and the corresponding security session remains open.

When Error_flag is set to 1, Error_code field may take the values of [Table 152](#) in a WritePassword response.

Table 152. WritePassword error codes when Error_flag equals 1

Error code	Description
01h	Invalid IC Mfg code value
02h	Invalid request format, including case of invalid password size
03h	Invalid Request_flags value
10h	Invalid Password_id value
12h	Security session is closed
13h	Programming of requested password failed

When the VICC responds to a WritePassword request, the timing of the frame exchange is that of a write-alike command as depicted in [Figure 12](#) and [Figure 13](#).

During the RF write cycle Wt, there should be no modulation (neither 100% nor 10%), otherwise the ST25TVxxxC may not correctly program the password value into the memory.

There is no anti-tearing mechanism while operating the WritePassword command. Command should be applied with stable RF field, otherwise the write operation may not complete properly, and could imply a loss/corruption of password content.

The ST25TVxxxC offers a password recovery capability when such content loss/corruption occurs, see [Section 5.1.2 Password management](#).

6.4.19 PresentPassword

When receiving the PresentPassword request, the ST25TVxxxC compares the selected password register with the password coded in the request and responds an acknowledgment if the operation was successful.

After a successful PresentPassword command, the security session associated to the password is open as described in [Section 5.1 Data protection](#).

Option_flag is set to 0 : no option supported.

Table 153. PresentPassword request format

SOF	Request_flags	Opcode	IC Mfg code	UID ⁽¹⁾	Password_id	Password_data	CRC_B	EOF
-	00xx00xxb	B3h	02h	64 bits	8 bits	32 or 64 bits	16 bits	-

1. UID field present when Request_flags=001000xxb

Request parameters and data include :

- IC manufacturer code coded on 1 byte, value shall be 02h
- UID parameter if Address_flag is set to 1
- Password_id coded on 1 byte
- Password_data coded on 4 or 8 bytes according to [Table 27. List of password registers](#)

The unique valid Password_data value is obtained from the encryption of the plain password value as described in [Section 5.1.3 Password encryption](#).

It is recommended to issue the PresentPassword request in Addressed or Select mode, in order to improve the system robustness. This ensures that password presentation is only applied to a specific tag/UID.

Table 154. PresentPassword response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0:

- no data is inserted between the Response_flags and CRC_B fields.
- the presentation of the password is successful, and the corresponding security session is open.

When Error_flag is set to 1, Error_code field may take the values of [Table 155](#) in a PresentPassword response.

All security sessions are closed if an invalid value of Password_data is presented.

Warning:

After the presentation of an invalid value of Password_data with the PresentPassword / Kill / ToggleUntraceable command, the GetRandomNumber command shall be called before attempting another password presentation with the PresentPassword command as described in [Section 5.1.3 Password encryption](#).

The ST25TVxxxC offers a password attempt limit capability to protect a password against brute-force attacks, see [Section 5.1.2 Password management](#).

Table 155. PresentPassword error codes when Error_flag equals 1

Error code	Description
01h	Invalid IC Mfg code value
02h	Invalid request format, including case of invalid password size
03h	Invalid Request_flags value
0Fh	Invalid Password_data value
10h	Invalid Password_id value

When the VICC responds to a PresentPassword request, the timing of the frame exchange is that of a read-alike command as depicted in Figure 11.

6.4.20

Kill

When receiving the Kill request, the ST25TVxxxC compares register PWD_CFG with the password coded in the request and responds an acknowledgment if the operation was successful.

Kill command is applicable if and only if the DIS_KILL register is set to 0b, otherwise it is ignored. After a successful Kill command, the ST25TVxxxC permanently enters the KILLED state, where it stays mute to any request.

Select_flag is set to 0 and Address_flag is set to 1 : the Kill request must be issued in Addressed mode.

When Option_flag is set to 1, the response is postponed to the subsequent EOF request.

Table 156. Kill request format

SOF	Request_flags	Opcode	IC Mfg code	UID	Password_id	Password_data	CRC_B	EOF
-	0x1000xxb	A6h	02h	64 bits	00h	32 bits	16 bits	-

Request parameters and data include :

- IC manufacturer code coded on 1 byte, value shall be 02h
- UID parameter
- Password_id coded on 1 byte, value shall be 00h
- Password_data coded on 4 bytes

The unique valid Password_data value is obtained from the encryption of the plain password value as described in Section 5.1.3 Password encryption

Warning:

After the presentation of an invalid value of Password_data with the PresentPassword / Kill / ToggleUntraceable command, the GetRandomNumber command shall be called before attempting another password presentation with the Kill command.

Note:

The behavior of the Kill command is different between the ST25TVxxx and ST25TVxxxC devices regarding the encryption of the Password_data field. The Password_data field is a plain password value on the ST25TVxxx device described in datasheet DS12074, while it is an encrypted password value on the ST25TVxxxC device described in this document.

Table 157. Kill response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0:

- no data is inserted between the Response_flags and CRC_B fields.
- the ST25TVxxxC permanently enters the KILLED state by setting the KILL_CMD register to 1b.

When Error_flag is set to 1, Error_code field may take the values of Table 158 in a Kill response.

Table 158. Kill error codes when Error_flag equals 1

Error code	Description
01h	Invalid IC Mfg code value
02h	Invalid request format
03h	Invalid Request_flags value

Error code	Description
0Fh	Invalid Password_data value
10h	Invalid Password_id value
14h	Programming of KILL_CMD failed

When the VICC responds to a Kill request, the timing of the frame exchange is that of a write-alike command as depicted in [Figure 12](#) and [Figure 13](#).

During the RF write cycle W_t , there should be no modulation (neither 100% nor 10%), otherwise the ST25TVxxxC may not correctly program the KILL_CMD register into the memory.

6.4.21

Initiate

When receiving the Initiate request, the ST25TVxxxC sets the Initiate_flag register to 1b and sends back a response. Initiate_flag is automatically reset to 0b when the ST25TVxxxC enters the POWER-OFF state. Select_flag is set to 0 and Address_flag is set to 0 : the Initiate request must be issued in Non- addressed mode. Option_flag is set to 0 : no option supported.

Table 159. Initiate request format

SOF	Request_flags	Opcode	IC Mfg code	CRC_B	EOF
-	000000xxb	D2h	02h	16 bits	-

Request parameters and data include :

- IC manufacturer code coded on 1 byte, value shall be 02h

Table 160. Initiate response format when Error_flag equals 0

SOF	Response_flags	DSFID	UID	CRC_B	EOF
-	00h	8 bits	64 bits	16 bits	-

When Error_flag is set to 0, Initiate_flag is set to 1b response data include :

- DSFID register value
- UID register value

The ST25TVxxxC does not generate any answer in case of error.

When the VICC responds to an Initiate request, the timing of the frame exchange is that of a read- alike command as depicted in [Figure 11](#).

6.4.22

InventoryInitiated

When receiving the InventoryInitiated request, the ST25TVxxxC sends a response if Initiate_flag is set to 1b and the parameters match the values of the UID and AFI registers.

Inventory_flag is set to 1 : bits 4 and 5 of Request_flags respectively code AFI_flag and Nb_slots_flag.

Option_flag is set to 0 : no option supported.

Table 161. InventoryInitiated request format

SOF	Request_flags	Opcode	IC Mfg code	AFI ⁽¹⁾	Mask_length	Mask_value	CRC_B	EOF
-	00xx01xxb	D1h	02h	8 bits	8 bits	0-64 bits	16 bits	-

1. AFI field present when Request_flags=00x101xxb

Request parameters and data include :

- IC manufacturer code coded on 1 byte, value shall be 02h

- AFI parameter if AFI_flag is set to 1
- Mask_length in bits, ≤ 60 when Nb_slots_flag = 0b, ≤ 64 when Nb_slots_flag = 1b
- Mask_value, size in bytes is (Mask_length + 7)/8, not present if Mask_length = 00h

Table 162. InventoryInitiated response format when Error_flag equals 0

SOF	Response_flags	DSFID	UID	CRC_B	EOF
-	00h	8 bits	64 bits	16 bits	-

When Error_flag is set to 0, response data include :

- DSFID register value
- UID register value

The ST25TVxxxC does not generate any answer in case of error.

When the VICC responds to an InventoryInitiated request, the timing of the frame exchange is that of a read-alike command as depicted in [Figure 11](#).

When Nb_slots_flag is set to 0, the VCD issues 15 EOF requests after the initial request from [Table 161](#), with the following timings described in [Section 6.3 Timing definition](#):

- if the VICC responds to an EOF request, the timing of the frame exchange is that of a read-alike command
- if the VCD receives a response from one or more VICCs, it waits for a time t2 before sending the next EOF request
- if the VCD does not receive a response from any VICC, it waits for a time t3 before sending the next EOF request

6.4.23

ToggleUntraceable

When receiving the ToggleUntraceable request, the ST25TVxxxC compares register PWD_UNTR with the password coded in the request and responds an acknowledgment if the operation was successful.

ToggleUntraceable command is applicable only in the following cases, otherwise it is ignored :

- the ST25TVxxxC is in READY, SELECTED or QUIET state, and the request is issued in Addressed mode (Select_flag=0, Address_flag=1)
- the ST25TVxxxC is in UNTRACEABLE state, and the request is issued in Non-Addressed mode (Select_flag=0, Address_flag=0)

After a successful ToggleUntraceable command, the ST25TVxxxC leaves or enters (depending on the addressing mode) the UNTRACEABLE state described in [Section 6.2.9 Custom states](#).

When Option_flag is set to 1, the response is postponed to the subsequent EOF request.

Table 163. ToggleUntraceable request format

SOF	Request_flags	Opcode	IC Mfg code	UID ⁽¹⁾	Password_id	Password_data	CRC_B	EOF
-	0xx000xxb	BAh	02h	64 bits	03h	32 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb

Request parameters and data include :

- IC manufacturer code coded on 1 byte, value shall be 02h
- UID parameter if Address_flag is set to 1
- Password_id coded on 1 byte, value shall be 03h
- Password_data coded on 4 bytes

The unique valid Password_data value is obtained from the encryption of the plain password value as described in [section 5.1.3](#)

Warning:

After the presentation of an invalid value of Password_data with the PresentPassword / Kill / ToggleUntraceable command, the GetRandomNumber command shall be called before attempting another password presentation with the ToggleUntraceable command as described in Section 5.1.3 Password encryption.

Note:

Opcode value BAh is used for the EnableUntraceable command of the ST25TVxxx device described in datasheet DS12074. The EnableUntraceable command has the same request format as the ToggleUntraceable command, except for the value of the Password_id field which is 00h on the ST25TVxxx device, and 03h on the ST25TVxxx device described in this document.

Table 164. ToggleUntraceable response format when Error_flag equals 0

SOF	Response_flags	CRC_B	EOF
-	00h	16 bits	-

When Error_flag is set to 0:

- no data is inserted between the Response_flags and CRC_B fields.
- if the request was issued in Addressed mode, the ST25TVxxxC enters the UNTRACEABLE state by setting the UNTR_CMD register to 1b.
- if the request was issued in Non-addressed mode, the ST25TVxxxC enters the READY state by setting the UNTR_CMD register to 0b.

When Error_flag is set to 1, Error_code field may take the values of Table 165 in a ToggleUntraceable response.

Table 165. ToggleUntraceable error codes when Error_flag equals 1

Error code	Description
01h	Invalid IC Mfg code value
02h	Invalid request format
03h	Invalid Request_flags value
0Fh	Invalid Password_data value
10h	Invalid Password_id value
13h	Programming of UNTR_CMD failed

When the VICC responds to a ToggleUntraceable request, the timing of the frame exchange is that of a write-alike command as depicted in Figure 12 and Figure 13.

During the RF write cycle Wt, there should be no modulation (neither 100% nor 10%), otherwise the ST25TVxxxC may not correctly program the UNTR_CMD register into the memory.

6.4.24
GetRandomNumber

When receiving the GetRandomNumber request, the ST25TVxxxC responds a 16-bit random number.

When Option_flag is set to 1, the response is postponed to the subsequent EOF request.

Table 166. GetRandomNumber request format

SOF	Request_flags	Opcode	IC Mfg code	UID ⁽¹⁾	CRC_B	EOF
-	0xxx00xxb	B4h	02h	64 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb

Request parameters and data include :

- IC manufacturer code coded on 1 byte, value shall be 02h

- UID parameter if Address_flag is set to 1

Table 167. GetRandomNumber response format when Error_flag equals 0

SOF	Response_flags	RND_NUMBER	CRC_B	EOF
-	00h	16 bits	16 bits	-

When Error_flag is set to 0, a new 16-bit value has been programmed in the RND_NUMBER register, and response data include :

- RND_NUMBER register value

When Error_flag is set to 1, Error_code field may take the values of [Table 168](#) in a GetRandomNumber response.

Table 168. GetRandomNumber error codes when Error_flag equals 1

Error code	Description
01h	Invalid IC Mfg code value
02h	Invalid request format
03h	Invalid Request_flags value
13h	Programming of RND_NUMBER failed

When the VICC responds to a GetRandomNumber request, the timing of the frame exchange is that of a write-alike command as depicted in [Figure 12](#) and [Figure 13](#).

During the RF write cycle Wt, there should be no modulation (neither 100% nor 10%), otherwise the ST25TVxxxC may not correctly program the RND_NUMBER register into the memory.

7 Unique identifier (UID)

The ST25TVxxxC ICs are uniquely identified by a 64-bit unique identifier (UID). This UID complies with ISO/IEC 15693 and ISO/IEC 7816-6. The UID is a read-only code and comprises:

- 8 bytes
- magic number code E0h on 8 bits
- the IC manufacturer code "ST 02h" on 8 bits (ISO/IEC 7816-6/AM1)
- the ST25TVxxxC product code 08h on 8 bits
- a unique serial number on 40 bits

Table 169. UID format

MSB		LSB	
b63-b56	b55-b48	b47-b40	b39-b0
E0h	02h	ST product code : 08h	Unique serial number

7.1 Untraceable UID

When the ST25TVxxxC meets either of the following conditions :

- the current RF session started in UNTRACEABLE state
- the current state is UNTRACEABLE

then the UID register is masked with the content from [Table 170](#) when processing request and response frames of all commands, except in the response to a ReadConfiguration request (FID=FEh, PID=01h) where the content of the UID register is always returned without masking.

Table 170. Untraceable UID : UID value in UNTRACEABLE state

MSB		LSB	
b63-b56	b55-b48	b47-b40	b39-b0
E0h	02h	00h	0000000000h

Note: When several ST25TVxxxC tags responding UID from [Table 170](#) are present in the field of a VCD, it is not possible to discriminate them with an anticollision procedure. Only one ST25TVxxxC IC responding Untraceable UID value should be present in the field of a VCD for an application to work properly

8 Device parameters

8.1 Maximum ratings

Stressing the device above the ratings listed in Table 171. Absolute maximum ratings may permanently damage it. These are stress ratings only and operation of the device, at these or any other conditions above those indicated in the operating sections of this specification, is not implied. Exposure to absolute maximum rating conditions for extended periods may affect the device reliability. Refer also to the STMicroelectronics SURE Program and other relevant quality documents.

Table 171. Absolute maximum ratings

Symbol	Description	Min	Max	Unit
T_A	Ambient operating temperature	-40	85	°C
T_{STG_1}	Storage temperature for UFDFPN5 package	-65	150	°C
T_{STG_2}	Storage temperature for sawn wafer ⁽¹⁾	15	25	°C
t_{STG}	Sawn wafer ⁽¹⁾ storage duration counted from ST production date	-	9	months
V_{MAX_1} ⁽²⁾	Max input voltage amplitude (peak to peak) between AC0 and AC1	-	11	V
V_{ESD}	Electronic discharge voltage ⁽³⁾ on all pins	-	2000	V

1. Sawn wafer on UV tape kept in its original packing form
2. (VAC0-VAC1) peak to peak evaluated by characterization - not tested in production
3. Human body model of ANSI/ESDA/JEDEC JS-001 with $C = 100\text{ pF}$, $R = 1500\ \Omega$, $R2 = 500\ \Omega$

8.2 RF electrical parameters

This section summarizes the operating and measurement conditions, and the RF electrical parameters of the device.

The parameters in the RF characteristics table that follows are derived from tests performed under the measurement conditions summarized in the relevant tables. Designers should check that the operating conditions in their circuit match the measurement conditions when relying on the quoted parameters.

Table 172. RF characteristics

Symbol	Description	Condition ⁽¹⁾⁽²⁾	Min	Typ	Max	Unit
f_{CC} ⁽³⁾	External RF signal frequency	-	13.553	13.56	13.567	MHz
f_{SL}	Low subcarrier frequency ($f_{CC}/32$)	-	-	423.75	-	kHz
f_{SH}	High subcarrier frequency ($f_{CC}/28$)	-	-	484.28	-	kHz
MI_{10} ⁽³⁾	10% carrier modulation index	150 mA/m < H < 5 A/m	10	-	30	%
MI_{100} ⁽³⁾	100% carrier modulation index	150 mA/m < H < 5 A/m	95	-	100	%
$t_{Boot_RF_1}$ ⁽³⁾	RF boot time ⁽⁴⁾	TD_EVENT_UPDATE_EN=0b and UTC_EN=0b, from H _{FIELD_MIN}	-	-	1	ms
$t_{Boot_RF_2}$ ⁽³⁾	RF boot time ⁽⁴⁾	TD_EVENT_UPDATE_EN=1b or UTC_EN=1b, from H _{FIELD_MIN}	-	-	5	ms
t_{RF_OFF} ⁽³⁾	RF power down duration needed to reset the IC	-	2	-	-	ms

Symbol	Description	Condition ⁽¹⁾⁽²⁾	Min	Typ	Max	Unit
$t_1^{(3)}$	VICC response delay	-	318.6	320.9	323.3	μ s
$t_2^{(3)}$	VCD new request delay after a response from the VICC	-	309	311.5	314	μ s
$t_3^{(3)}$	VCD new request delay after no response from the VICC	-	323.3	-	-	μ s
$W_t^{(3)}$	Duration of write operation ⁽⁵⁾	Max 32 bits of data	-	4	-	ms
$C_{TUN_23}^{(6)}$	Input capacitance ⁽⁷⁾	$V_{pkpk} = V_{MIN_1}$	21.9	23	24.2	pF
$C_{TUN_99}^{(6)}$			94.7	99.7	104.7	pF
$V_{BACK}^{(3)}$	Minimum ISO15693 backscattering voltage	-	10	-	-	mV
$V_{MIN_1}^{(3)}$	Min input voltage amplitude (peak to peak) between AC0 and AC1	Inventory and read operations	-	4.4	-	V
$V_{MIN_2}^{(3)}$	Min input voltage amplitude (peak to peak) between AC0 and AC1	Write operations	-	4.4	-	V
$R_{closed}^{(3)}$	Resistance of closed tamper loop	TD0 and TD1 connected	-	-	50	Ω
$R_{open}^{(3)}$	Resistance of open tamper loop	TD0 and TD1 not connected	1	-	-	M Ω
$t_{RET}^{(3)}$	Retention time	$T_A \leq 55^\circ\text{C}$	60	-	-	year
Cycling ⁽³⁾	Write cycles endurance	$T_A \leq 85^\circ\text{C}$	100000	-	-	cycle

- $T_A = -40$ to 85°C unless stated otherwise.
- All timing characterizations were performed on a reference antenna with the following characteristics:
 - ISO antenna class1
 - Tuning frequency = 13.7 MHz
- Evaluated by characterization - not tested in production.
- Minimum time from carrier generation to start of first request.
- VCD request in 1 out of 4 coding, VICC response in high datarate and single subcarrier.
- Evaluated by characterization at 25°C - tested in production at 25°C by correlating industrial tester measure with characterization results.
- C_{TUN_23} and C_{TUN_99} capacitance values apply to ST25TVxxxC-xxx3 and ST25TVxxxC-xxx9 product versions respectively (see Section 10 Ordering information).

9 Package information

In order to meet environmental requirements, ST offers these devices in different grades of ECOPACK packages, depending on their level of environmental compliance. ECOPACK specifications, grade definitions and product status are available at: www.st.com. ECOPACK is an ST trademark.

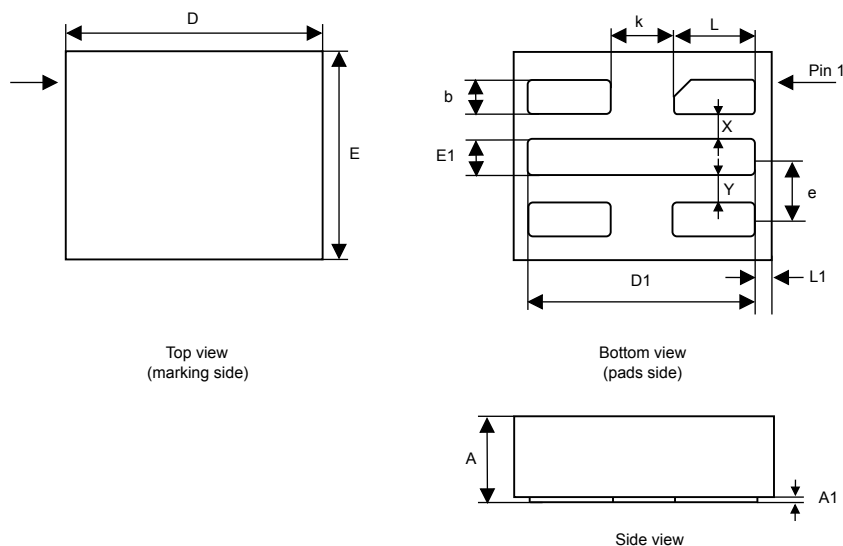
9.1 Sawn and bumped wafer

Contact your STMicroelectronics sales office to get the description document.

9.2 UFDFPN5 (DFN5) package information

UFDFPN5 is a 5-lead, 1.7×1.4 mm, 0.55 mm thickness, ultra thin fine pitch dual flat package.

Figure 15. UFDFPN5 - Outline



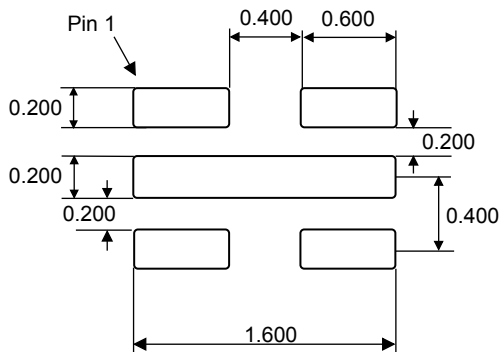
1. Maximum package warpage is 0.05 mm.
2. Exposed copper is not systematic and can appear partially or totally according to the cross section.
3. Drawing is not to scale.
4. On the bottom side, pin 1 is identified by the specific pad shape and, on the top side, pin 1 is defined from the orientation of the marking. When reading the marking, pin 1 is below the upper left package corner.

A0UK_UFDFN5_ME_V3

Table 173. UFDFPN5 - Mechanical data

Symbol	millimeters			inches		
	Min	Typ	Max	Min	Typ	Max
A	0.500	0.550	0.600	0.0197	0.0217	0.0236
A1	0.000	-	0.050	0.0000	-	0.0020
b ⁽¹⁾	0.175	0.200	0.225	0.0069	0.0079	0.0089
D	1.600	1.700	1.800	0.0630	0.0669	0.0709
D1	1.400	1.500	1.600	0.0551	0.0591	0.0630
E	1.300	1.400	1.500	0.0512	0.0551	0.0591
E1	0.175	0.200	0.225	0.0069	0.0079	0.0089
X	-	0.200	-	-	0.0079	-
Y	-	0.200	-	-	0.0079	-
e	-	0.400	-	-	0.0157	-
L	0.500	0.550	0.600	0.0197	0.0217	0.0236
L1	-	0.100	-	-	0.0039	-
k	-	0.400	-	-	0.0157	-

1. Dimension *b* applies to plated terminal and is measured between 0.15 and 0.30mm from the terminal tip.

Figure 16. UFDFPN5 - Footprint example


A0UK_UFDFN5_FP_V1

1. Dimensions are expressed in millimeters.

10 Ordering information

Table 174. Ordering information scheme

Example:	ST25TV	02K	C-	A	F	G	3
Device type							
ST25TV = NFC/RFID tag based on ISO 15693 and NFC T5T							
Memory size							
512 = 512 bits							
02K = 2560 bits							
Product version							
C = Version C							
Interface							
A = None							
T = Tamper detection							
Features							
F = Augmented NDEF							
Package							
F = 75 µm ± 10 µm bumped and sawn wafer							
G = 120 µm ± 10 µm bumped and sawn wafer							
H = UFDFPN5							
Capacitance setting							
3 = 23 pF							
9 = 99.7 pF							

Note: Parts marked as “ES” or “E” are not yet qualified and therefore not approved for use in production. ST is not responsible for any consequences resulting from such use. In no event will ST be liable for the customer using any of these engineering samples in production. ST’s Quality department must be contacted prior to any decision to use these engineering samples to run a qualification activity.

11 List of acronyms

Table 175. List of acronyms

Acronym	Definition
AFI	Application family identifier
ANDEF	Augmented NDEF
ASCII	American standard for information interchange
BSS	Block security status
CC	Capability container
CMD	Command
CRC	Cyclic redundancy check
DSFID	Data storage format identifier
EEPROM	Electrically-erasable programmable read-only memory
EOF	End of frame
FID	Feature identifier
GDPR	General data protection regulation
HZ	High impedance
IC	Integrated Circuit
Id	Identifier
NA	Not applicable
NC	Not connected
NDEF	NFC data exchange format
NFC	Near field communication
PID	Parameter identifier
POR	Power on reset
PWD	Password
RF	Radio frequency
RFID	RF identification
RFU	Reserved for future use
SOF	Start of frame
UFDFFN	Ultra thin Fine pitch Dual Flat Package No-lead
UTC	Unique tap code
TD	Tamper detection
UID	Unique identifier
VCD	Vicinity coupling device
VICC	Vicinity integrated circuit card
X	Any value in the range defined by the type ([0:1] for a bit, [0:F] for an hexadecimal nibble)

Revision history

Table 176. Document revision history

Date	Revision	Changes
15-Dec-2020	1	Initial release.
15-Jan-2021	2	Updated: - Section 5.2.2 Unique tap code description - Section 6.2.2 Request format - Section 6.2.4 Response format - Section 6.2.6 Response and error codes - Section 10 Ordering information
14-Apr-2021	3	Updated: - Section Features - Section 5.5.1 Privacy registers - Section 6.2.9 Custom states - Section 6.4.15 ExtendedGetSystemInfo - Section 6.4.19 PresentPassword
01-Jul-2021	4	Updated: - Footnote number 2 of Table 171. Absolute maximum ratings - C_{TUN} condition of Table 172. RF characteristics and its footnotes (Modified footnotes 1, 3, 4, 5 and 6 and deleted footnotes 7 and 8.)
30-Aug-2022	5	Updated: - Table 84. REV content - Figure 15. UFD5PN5 - Outline
15-Dec-2022	6	Updated: Table 172. RF characteristics

Contents

1	Description	3
1.1	Block diagram	3
1.2	Package connections	3
2	Functional overview	5
2.1	Block diagram	5
2.2	Application information	5
3	Power management.....	6
3.1	Device set	6
3.2	Device reset.....	6
4	Memory management.....	7
4.1	Memory organization	7
4.2	User memory	8
4.3	System configuration memory	9
4.3.1	System configuration registers	9
4.3.2	System registers	10
5	Specific features.....	11
5.1	Data protection	11
5.1.1	Data protection registers	11
5.1.2	Password management	16
5.1.3	Password encryption.....	19
5.1.4	User memory protection	20
5.1.5	System configuration memory protection	20
5.2	Unique tap code	21
5.2.1	Unique tap code registers	21
5.2.2	Unique tap code description	22
5.3	Tamper detection.....	22
5.3.1	Tamper detection registers	22
5.3.2	Tamper detection description	25
5.4	Augmented NDEF	26
5.4.1	Augmented NDEF registers	26

5.4.2	Augmented NDEF description	28
5.5	Consumer privacy protection	30
5.5.1	Privacy registers	30
5.5.2	Kill feature description	31
5.5.3	Untraceable feature description	32
5.6	TruST25 digital signature	32
5.7	AFI protection	33
5.7.1	AFI protection registers	33
5.7.2	AFI protection description	33
5.8	Inventory Initiated	33
5.9	Device identification registers	34
6	RF Operation	37
6.1	RF communication	37
6.1.1	Access to a ISO/IEC 15693 device	37
6.2	RF protocol	37
6.2.1	Protocol description	37
6.2.2	Request format	38
6.2.3	Request flags	38
6.2.4	Response format	39
6.2.5	Response flags	40
6.2.6	Response and error codes	40
6.2.7	Modes	41
6.2.8	ISO15693 states	41
6.2.9	Custom states	43
6.3	Timing definition	44
6.4	RF commands	47
6.4.1	Inventory	48
6.4.2	StayQuiet	48
6.4.3	ReadSingleBlock	49
6.4.4	WriteSingleBlock	50
6.4.5	LockBlock	51
6.4.6	ReadMultipleBlocks	51

6.4.7	Select	52
6.4.8	ResetToReady	53
6.4.9	WriteAFI	54
6.4.10	LockAFI	54
6.4.11	WriteDSFID	55
6.4.12	LockDSFID	56
6.4.13	GetSystemInfo	57
6.4.14	GetMultipleBlockSecurityStatus	57
6.4.15	ExtendedGetSystemInfo	58
6.4.16	ReadConfiguration	60
6.4.17	WriteConfiguration	61
6.4.18	WritePassword	62
6.4.19	PresentPassword	64
6.4.20	Kill	65
6.4.21	Initiate	66
6.4.22	InventoryInitiated	66
6.4.23	ToggleUntraceable	67
6.4.24	GetRandomNumber	68
7	Unique identifier (UID)	70
7.1	Untraceable UID	70
8	Device parameters	71
8.1	Maximum ratings	71
8.2	RF electrical parameters	71
9	Package information	73
9.1	Sawn and bumped wafer	73
9.2	UFDFPN5 package information	73
10	Ordering information	75
11	List of acronyms	76
	Revision history	77
	Contents	78
	List of tables	82



List of figures.....	86
----------------------	----

List of tables

Table 1.	Signal names	4
Table 2.	User memory in single area mode	8
Table 3.	User memory in dual area mode	8
Table 4.	List of configuration registers	9
Table 5.	List of system registers	10
Table 6.	LCK_CONFIG access	11
Table 7.	LCK_CONFIG content	12
Table 8.	LCK_BLOCK access	12
Table 9.	LCK_BLOCK content	12
Table 10.	RW_PROTECTION_A1 access	13
Table 11.	RW_PROTECTION_A1 content	13
Table 12.	END_A1 access	13
Table 13.	END_A1 content	13
Table 14.	RW_PROTECTION_A2 access	14
Table 15.	RW_PROTECTION_A2 content	14
Table 16.	PWD_CFG access	14
Table 17.	PWD_CFG content	14
Table 18.	PWD_A1 access	15
Table 19.	PWD_A1 content	15
Table 20.	PWD_A2 access	15
Table 21.	PWD_A2 content	15
Table 22.	PWD_UNTR access	15
Table 23.	PWD_UNTR content	15
Table 24.	RND_NUMBER access	16
Table 25.	RND_NUMBER content	16
Table 26.	Security session type	16
Table 27.	List of password registers	16
Table 28.	RND_NUMBER_4B	19
Table 29.	RND_NUMBER_8B	19
Table 30.	Example of 64-bit Password_data value computation	19
Table 31.	Block security status	20
Table 32.	UTC_EN access	21
Table 33.	UTC_EN content	21
Table 34.	UTC access	22
Table 35.	UTC content	22
Table 36.	TD_EVENT_UPDATE_EN access	22
Table 37.	TD_EVENT_UPDATE_EN content	23
Table 38.	TD_SEAL_MSG access	23
Table 39.	TD_SEAL_MSG content	23
Table 40.	TD_UNSEAL_MSG access	23
Table 41.	TD_UNSEAL_MSG content	23
Table 42.	TD_RESEAL_MSG access	23
Table 43.	TD_RESEAL_MSG content	24
Table 44.	TD_SHORT_MSG access	24
Table 45.	TD_SHORT_MSG content	24
Table 46.	TD_OPEN_MSG access	24
Table 47.	TD_OPEN_MSG content	24
Table 48.	TD_STATUS access	24
Table 49.	TD_STATUS content	25
Table 50.	ANDEF_EN access	26
Table 51.	ANDEF_EN content	26
Table 52.	ANDEF_CFG access	26

Table 53.	ANDEF_CFG content	26
Table 54.	ANDEF_SEP access	27
Table 55.	ANDEF_SEP content	27
Table 56.	ANDEF_CUSTOM_LSB access	27
Table 57.	ANDEF_CUSTOM_LSB content	27
Table 58.	ANDEF_CUSTOM_MSB access	27
Table 59.	ANDEF_CUSTOM_MSB content	27
Table 60.	ANDEF_UID access	27
Table 61.	ANDEF_UID content	28
Table 62.	Block data read when ANDEF feature is disabled on ST25TV02KC	28
Table 63.	Block data read when ANDEF feature is enabled on ST25TV02KC	28
Table 64.	ANDEF fields concatenated in ANDEF_MEM	29
Table 65.	KILL_CMD access	30
Table 66.	KILL_CMD content	30
Table 67.	UNTR_CMD access	31
Table 68.	UNTR_CMD content	31
Table 69.	PRIVACY access	31
Table 70.	PRIVACY content	31
Table 71.	AFI_PROT access	33
Table 72.	AFI_PROT content	33
Table 73.	LCK_DSFD access	34
Table 74.	LCK_DSFD content	34
Table 75.	LCK_AFI access	34
Table 76.	LCK_AFI content	34
Table 77.	DSFD access	34
Table 78.	DSFD content	35
Table 79.	AFI access	35
Table 80.	AFI content	35
Table 81.	IC_REF access	35
Table 82.	IC_REF content	35
Table 83.	REV access	35
Table 84.	REV content	35
Table 85.	UID access	36
Table 86.	UID content	36
Table 87.	General request format	38
Table 88.	Definition of Request_flags LSBs	39
Table 89.	Definition of Request_flags MSBs when Inventory_flag value is 0	39
Table 90.	Definition of Request_flags MSBs when Inventory_flag value is 1	39
Table 91.	General response format	40
Table 92.	Definition of Response_flags	40
Table 93.	General response format when Error_flag equals 1	40
Table 94.	Definition of response error codes	40
Table 95.	Request_flags values depending on addressing mode	42
Table 96.	Device response depending on state and addressing mode	42
Table 97.	Timing values	45
Table 98.	Command code	47
Table 99.	Inventory request format	48
Table 100.	Inventory response format	48
Table 101.	StayQuiet request format	48
Table 102.	ReadSingleBlock request format	49
Table 103.	ReadSingleBlock response format when Error_flag equals 0	49
Table 104.	ReadSingleBlock error codes when Error_flag equals 1	50
Table 105.	WriteSingleBlock request format	50
Table 106.	WriteSingleBlock response format when Error_flag equals 0	50

Table 107.	WriteSingleBlock error codes when Error_flag equals 1	50
Table 108.	LockBlock request format	51
Table 109.	LockBlock response format when Error_flag equals 0	51
Table 110.	LockBlock error codes when Error_flag equals 1	51
Table 111.	ReadMultipleBlocks request format	52
Table 112.	ReadMultipleBlocks response format when Error_flag equals 0	52
Table 113.	ReadMultipleBlocks error codes when Error_flag equals 1	52
Table 114.	Select request format	52
Table 115.	Select response format when Error_flag equals 0	53
Table 116.	Select error codes when Error_flag equals 1	53
Table 117.	ResetToReady request format	53
Table 118.	ResetToReady response format when Error_flag equals 0	53
Table 119.	ResetToReady error codes when Error_flag equals 1	53
Table 120.	WriteAFI request format	54
Table 121.	WriteAFI response format when Error_flag equals 0	54
Table 122.	WriteAFI error codes when Error_flag equals 1	54
Table 123.	LockAFI request format	54
Table 124.	LockAFI response format when Error_flag equals 0	55
Table 125.	LockAFI error codes when Error_flag equals 1	55
Table 126.	WriteDSFID request format	55
Table 127.	WriteDSFID response format when Error_flag equals 0	55
Table 128.	WriteDSFID error codes when Error_flag equals 1	56
Table 129.	LockDSFID request format	56
Table 130.	LockDSFID response format when Error_flag equals 0	56
Table 131.	LockDSFID error codes when Error_flag equals 1	56
Table 132.	GetSystemInfo request format	57
Table 133.	GetSystemInfo response	57
Table 134.	GetSystemInfo error codes when Error_flag equals 1	57
Table 135.	GetMultipleBlockSecurityStatus request format	58
Table 136.	GetMultipleBlockSecurityStatus response format when Error_flag equals 0	58
Table 137.	GetMultipleBlockSecurityStatus error codes when Error_flag equals 1	58
Table 138.	ExtendedGetSystemInfo request format	58
Table 139.	Information_request_list content	59
Table 140.	ExtendedGetSystemInfo response format when Error_flag equals 0	59
Table 141.	Information_flags content	59
Table 142.	Information_fields content	59
Table 143.	ExtendedGetSystemInfo error codes when Error_flag equals 1	60
Table 144.	ReadConfiguration request format	60
Table 145.	ReadConfiguration response format when Error_flag equals 0	60
Table 146.	ReadConfiguration error codes when Error_flag equals 1	61
Table 147.	WriteConfiguration request format	61
Table 148.	WriteConfiguration response format when Error_flag equals 0	61
Table 149.	WriteConfiguration error codes when Error_flag equals 1	62
Table 150.	WritePassword request format	62
Table 151.	WritePassword response format when Error_flag equals 0	63
Table 152.	WritePassword error codes when Error_flag equals 1	63
Table 153.	PresentPassword request format	64
Table 154.	PresentPassword response format when Error_flag equals 0	64
Table 155.	PresentPassword error codes when Error_flag equals 1	64
Table 156.	Kill request format	65
Table 157.	Kill response format when Error_flag equals 0	65
Table 158.	Kill error codes when Error_flag equals 1	65
Table 159.	Initiate request format	66
Table 160.	Initiate response format when Error_flag equals 0	66

Table 161.	InventoryInitiated request format	66
Table 162.	InventoryInitiated response format when Error_flag equals 0	67
Table 163.	ToggleUntraceable request format	67
Table 164.	ToggleUntraceable response format when Error_flag equals 0	68
Table 165.	ToggleUntraceable error codes when Error_flag equals 1	68
Table 166.	GetRandomNumber request format	68
Table 167.	GetRandomNumber response format when Error_flag equals 0	69
Table 168.	GetRandomNumber error codes when Error_flag equals 1	69
Table 169.	UID format	70
Table 170.	Untraceable UID : UID value in UNTRACEABLE state	70
Table 171.	Absolute maximum ratings	71
Table 172.	RF characteristics	71
Table 173.	UFDFPN5 - Mechanical data	74
Table 174.	Ordering information scheme.	75
Table 175.	List of acronyms	76
Table 176.	Document revision history	77

List of figures

Figure 1.	ST25TVxxxC block diagram	3
Figure 2.	UFDFPN5 package connections	4
Figure 3.	Die connections for sawn and bumped wafer	4
Figure 4.	RF power-up sequence	6
Figure 5.	Memory organization	7
Figure 6.	Security sessions management	18
Figure 7.	Example of augmented NDEF message on ST25TV02KC-T	30
Figure 8.	ISO15693 protocol timing	38
Figure 9.	ISO15693 state transition diagram	42
Figure 10.	ST25TVxxxC state transition diagram	43
Figure 11.	Read-alike frame exchange between VCD and ST25TVxxxC	44
Figure 12.	Write-alike frame exchange between VCD and ST25TVxxxC when Option_flag=0	45
Figure 13.	Write-alike frame exchange between VCD and ST25TVxxxC when Option_flag=1	46
Figure 14.	Stay Quiet frame	49
Figure 15.	UFDFPN5 - Outline	73
Figure 16.	UFDFPN5 - Footprint example	74

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST's terms and conditions of sale in place at the time of order acknowledgment.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of purchasers' products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2022 STMicroelectronics – All rights reserved



AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA PARA LAS ELECCIONES GENERALES PARAGUAY 2023



CUESTIONARIO SOBRE LA REVISIÓN DEL SOFTWARE

Objetivo General: Revisión detallada del diseño de software, documentación técnica, documentación de usuario, casos de uso, casos de prueba, QA, sistema operativo, parametrización, control de versiones, control de cambios, custodia de código, pruebas y simulacros.

Objetivos Específicos:

- Evaluar los procedimientos de diseño, desarrollo y versionado son adecuados.
- Evaluar que los aplicativos desarrollados se encuentren individualizados e identificados en un catálogo que permite validar su integridad.
- Evaluar los esquemas y estándares de seguridad utilizados.
- Evaluar que las capacidades de parametrización se adecúan a los requerimientos.
- Evaluar que se realice una adecuada gestión y control de cambios.
- Evaluar los procesos de control de calidad y pruebas.
- Evaluar que los casos de uso estén completos, detallados y acordes a las necesidades del proceso.
- Evaluar que los casos de prueba sean exhaustivos y estén acordes a los casos de uso.
- Evaluar el análisis de los sistemas desde una perspectiva de desarrollo de software, de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.
- Evaluar la integridad y la consistencia de los datos, de la información transmitida desde las máquinas de votación a las boletas de votación.

No.	Concepto	SI	NO	Cantidades/Detalles/ Observaciones / Fuentes de Información
I. SOFTWARE				
1	¿Existen varios fabricantes que les proveen los chips?	SI		
2	¿Cuántas marcas y modelos de chips se utilizan?			Existen 2 marcas (NXP y ST) y 3 (NXP/SLIX NXP/SLIX2S, ST25TV02KC, modelos de chips
3	¿Existe una ficha de datos técnicos para cada uno de los modelos de chips?	SI		
4	¿Existe algún chip que contenga alguna información que venga desde su fabricación, cual es la marca y modelo y cuál es el formato de texto de la información?	SI		Marca ST modelo ST25TV02KC, en Hexadecimal y ASCII, https://www.st.com/en/nfc/st25tv02kc.html



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



CUESTIONARIO SOBRE LA REVISIÓN DEL SOFTWARE

5	¿En el caso de existir información en los chips, existe alguna herramienta que permita verificar esta información contra lo descrito en la hoja de datos técnicos?	SI		El proveedor Grupo MSA desarrolló un script siguiendo los pasos descritos en el documento AN5580 (Documento que es confidencial por parte del fabricante)
6	¿En el caso de existir información en los chips, esta información se mantiene de manera perpetua o cambia en algún momento del proceso de votación?			Al momento de grabar la información de votación, la información de los bloques donde se encuentra la firma digital, queda en un valor de cero (0)
7	¿En el caso de existir información en los chips, en cuales bloques del chio se encuentra esta información?			La firma digital Trust25 se encuentra en los bloques 63 al 79.
8				
9				
10				
11				
12				
13				
14				
15				
16				

Firma y sello

Cargo

Nombre Empresa



**AUDITORÍA TÉCNICA DEL SISTEMA DE VOTACIÓN ELECTRÓNICA
PARA LAS ELECCIONES GENERALES PARAGUAY 2023**



CUESTIONARIO SOBRE LA REVISIÓN DEL SOFTWARE

Lugar y fecha