KUNAK
CONSULTING

Risk Management

Servicio de Auditoría del Proceso de Voto Electrónico

ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES

Informe Final de Auditoria

Documento en versión final

Clark Stanley Velando Leiva
Gerente General
KUNAK CONSULTING SAC

Historial de Versiones

Fecha	Versión	Descripción	Autor
20/12/2016	1.0	Elaboración del documento	Gleny Fernández
18/01/2017	2.0	Documentación adicional y recomendaciones	Ricardo Ramos
19/01/2016	3.0	Revisión y corrección del documento	Stanley Velando

Tabla de Contenido

1. INTRODUCCION

La Oficina Nacional de Procesos Electorales (ONPE) ha contratado los servicios profesionales de KUNAK CONSULTING SAC para llevar a cabo una auditoría a las soluciones tecnológicas de voto electrónico. El objetivo del servicio consiste en detectar posibles brechas de seguridad y determinar el comportamiento del sistema bajo un nivel de exigencia de ataques controlados.

2. ALCANCE

El alcance de esta auditoría se realiza en el marco de las Elecciones Universitarias a las cuales la ONPE brinda asistencia técnica.

Este servicio comprende el análisis de terminales *Windows* (laptop de transmisión) y *Android* (*tablet*s instaladas en la Estación de Comprobación de Identidad ECI y la Cabina de Votación Electrónica CVE), así como el análisis de vulnerabilidades en el sufragio, y finalmente el análisis del proceso de transmisión de información. Es preciso indicar que, para efectos de organización y cumplimiento del presente servicio, se ha visto a bien llevar a cabo la ejecución de las pruebas de la siguiente manera:

1. Prueba de acceso a las *tablets* de la Estación de Comprobación de Identidad (ECI) y Cabina de Voto Electrónico (CVE).
2. Intento de acceso en modo *recovery* a las *tablets*.
3. Pruebas sobre la computadora de transmisión de datos:
    a. Revisión de usuarios del computador.
    b. Revisión de puertos TCP/UDP abiertos en el computador.
    c. Revisión de "share administrativo".
4. Instalación de *sniffing* de red para evaluar la información que es transmitida al realizar la transmisión de votos.
5. Revisión de información transferida en las tarjetas de configuración (tarjeta morada), administración (tarjeta verde) y activación (tarjeta azul).
6. Reemplazo de contenido del USB de "Transmisión de Resultados".
7. Crear un código de barra de identificación de DNI falso con una inyección de código SQL.
8. Pruebas de acceso inalámbrico a las *tablets*.
9. Pruebas sobre el proceso de grabado de datos en la cabina de votación.
10. Prueba de revisión de código de las aplicaciones utilizadas en la Estación de Comprobación de Identidad (ECI) y Cabina de Voto Electrónico (CVE).
11. Prueba de revisión de "versiones" de la app instalada versus la app "autorizada" en el proceso de voto electrónico.

KUNAK CONSULTING S.A.C. V°B°

3. ENTENDIMIENTO DE PROCESO

Para poder realizar la revisión a los dispositivos y aplicaciones utilizadas en el proceso del voto electrónico fue necesario:

- Habilitar un ambiente en las oficinas de la ONPE, donde se simuló la instalación de una mesa de sufragio, la emisión del voto electrónico y proceso de envío de información desde el Punto de Transmisión.

- Entender el proceso del voto electrónico desde la configuración y diagnóstico de la Estación de Comprobación de Identidad (ECI) y Cabina de Votación Electrónica (CVE), hasta el envío de los resultados desde el Punto de Transmisión.

- Efectuar múltiples simulaciones referidas a la instalación de las mesas de sufragio, a la emisión de votos, al cierre de mesa, y finalmente el envío de datos, con lo cual se buscó identificar vulnerabilidades, puntos de mejora e interrogantes, las cuales serán detallas en el Ítem 5, Detalle de las Pruebas, del presente informe.

- Revisión física de los módulos de la Estación de Comprobación de Identidad (ECI) y la Cabina de Voto Electrónico (CVE), con la finalidad de entender y probar el adecuado funcionamiento de los dispositivos utilizados en el proceso electrónico.

- El personal de ONPE nos proporcionó todas las herramientas necesarias para llevar cabo el presente servicio de auditoría. Estas herramientas permitieron revisar la información que se almacena y transfiere en las tarjetas de configuración, administración y activación.

- El personal de ONPE nos dio acceso a la documentación del proceso de voto electrónico, que incluía la *Cartilla de miembros de mesa* y el *Instructivo de Instalación, Sufragio y Escrutinio – Voto Electrónico N06-GOECOR/JEL.*

4. RESUMEN DE LAS PRUEBAS Y HALLAZGOS

N°	Prueba	Complejidad	Resultado
1	Prueba de acceso a las *tablets* de la Estación de Comprobación de Identidad (ECI) y Cabina de Votación Electrónica (CVE)	MEDIA	NEGATIVO
2	Intento de acceso en modo *recovery* a las *tablets*	MEDIA	NEGATIVO
3	Pruebas sobre la computadora de transmisión de datos:		
3.1	Revisión de usuarios del computador.	MEDIA	NEGATIVO
3.2	Revisión de puertos TCP/UDP abiertos en el computador.	MEDIA	NEGATIVO
3.3	Revisión de "share administrativo".	MEDIA	NEGATIVO
4	Instalación de *sniffing* de red para evaluar la información que es transmitida al realizar la transmisión de datos.	ALTA	NEGATIVO
5	Revisión de información transferida en las tarjetas de configuración (tarjeta morada), administración (tarjeta verde) y activación (tarjeta azul).	ALTA	NEGATIVO
6	Reemplazo de contenido del USB de "Transmisión de Resultados".	MEDIA	NEGATIVO
7	Crear un código de barra de identificación de DNI falso con una inyección de código SQL.	MEDIA	NEGATIVO
8	Pruebas de acceso inalámbrico a las *tablets*	MEDIA	NEGATIVO
9	Pruebas sobre el proceso de grabado de datos en la cabina de votación.	ALTA	NEGATIVO
10	Prueba de revisión de código de las aplicaciones utilizadas en la Estación de Comprobación de Identidad (ECI) y Cabina de Votación Electrónica (CVE).	ALTA	NEGATIVO
11	Prueba de revisión de "versiones" de la app instalada versus la app "autorizada" en el proceso de voto electrónico.	N/A	NEGATIVO

Mapeo de las pruebas vs. Las categorias

Pruebas relacionadas a la ECI y a la CVE:

N°	Prueba	Complejidad	Resultado
1	Prueba de acceso a las *tablets* de la Estación de Comprobación de Identidad (ECI) y Cabina de Votación Electrónica (CVE)	MEDIA	NEGATIVO
2	Intento de acceso en modo *recovery* a las *tablets*	MEDIA	NEGATIVO
5	Revisión de información transferida en las tarjetas de configuración (tarjeta morada), administración (tarjeta verde) y activación (tarjeta azul).	ALTA	NEGATIVO
7	Crear un código de barra de identificación de DNI falso con una inyección de código SQL.	MEDIA	NEGATIVO
8	Pruebas de acceso inalámbrico a las *tablets*	MEDIA	NEGATIVO
9	Pruebas sobre el proceso de grabado de datos en la cabina de votación.	ALTA	NEGATIVO

10	Prueba de revisión de código de las aplicaciones utilizadas en la Estación de Comprobación de Identidad (ECI) y Cabina de Votación Electrónica (CVE).	ALTA	NEGATIVO

Pruebas relacionadas al proceso de transmisión:

N°	Prueba	Complejidad	Resultado
3	Pruebas sobre la computadora de transmisión de datos:		
3.1	Revisión de usuarios del computador.	MEDIA	NEGATIVO
3.2	Revisión de puertos TCP/UDP abiertos en el computador.	MEDIA	NEGATIVO
3.3	Revisión de "share administrativo".	MEDIA	NEGATIVO
4	Instalación de *sniffing* de red para evaluar la información que es transmitida al realizar la transmisión de datos.	ALTA	NEGATIVO
6	Reemplazo de contenido del USB de "Transmisión de Resultados".	MEDIA	NEGATIVO

Pruebas relacionadas al temas procedimentales:

N°	Prueba	Complejidad	Resultado
11	Prueba de revisión de "versiones" de la app instalada versus la app "autorizada" en el proceso de voto electrónico.	N/A	NEGATIVO

5. DETALLE DE LAS PRUEBAS

La **leyenda** de las pruebas se muestra a continuación:

Titulo	Descripción
Prueba	Describe la prueba a realizar.
Proceso	Describe el proceso de ejecución de la prueba.
Complejidad	Describe la complejidad de llevar a cabo la prueba de seguridad planteada: - Alta: Es muy difícil llevar a cabo la prueba planteada, se requiere de alto *expertise* técnico y/o la colusión de varias personas. - Media: Es difícil llevar a cabo la prueba planteada, se requiere un *expertise* técnico medio y/o la colusión de algunas personas. - Baja: Es posible realizar la prueba con expertise técnico bajo y sin la colusión de personas.
Resultado de la Prueba o Hallazgo	Describe el hallazgo o punto de mejora identificado.
Riesgo	Describe el riesgo, en caso de que la amenaza se materialice.
Recomendación	Describe la recomendación ad-hoc para la prueba descrita.
Comentario de ONPE	Describe la respuesta, descargo o comentario de ONPE sobre la prueba realizada.

Se llevaron a cabo las siguientes pruebas:

5.1. Prueba de acceso a las *tablets* de la Estación de Comprobación de Identidad (ECI) y Cabina de Votación Electrónica (CVE).

Titulo	Descripción
Prueba	Acceso a las *tablets* de la Estación de Comprobación de Identidad (ECI) y Cabina de Votación Electrónica (CVE), a través de computadores con la finalidad de acceder a la información almacenada en estos dispositivos.
Proceso	Se precedió a efectuar las siguientes actividades: - Por medio de un cable de "conexión USB" se conectaron las *tablets* a una laptop. - Posteriormente, procedimos a verificar el reconocimiento de la *tablet* en la PC, sin éxito. - Finalmente, validamos también que la *tablet* no reconocía a la PC conectada.
Complejidad	**MEDIA** Para llevar a cabo esta prueba fue necesario acceder al interior de los módulos de la Estación de Comprobación de Identidad (ECI) y Cabina de Voto Electrónico (CVE), siendo este acceso restringido por una llave física a la cual tiene acceso única y exclusivamente el Coordinador Técnico de Mesa (CTM).
Resultado de la Prueba o Hallazgo	Identificamos que la ONPE ha implementado medidas de seguridad necesarias a fin de evitar el acceso a la información contenida en las *tablets*. Por tal motivo, podemos concluir que el resultado de **la prueba es negativa**.

Riesgo	N/A
Recomendación	N/A
Comentario de ONPE	N/A

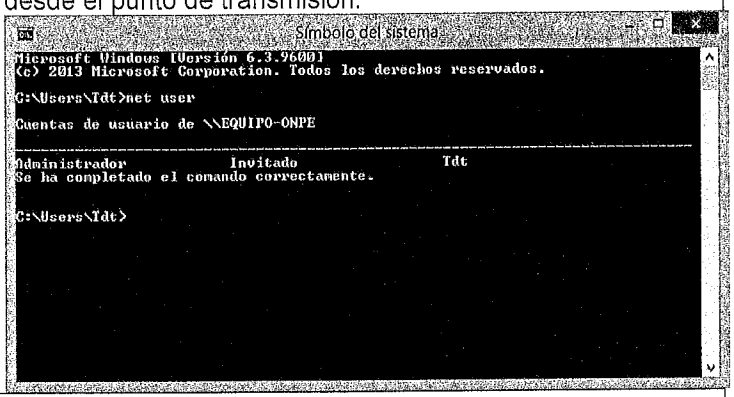
5.2. Intento de acceso en modo *recovery* a las *tablets*

Titulo	Descripción
Prueba	Ingresar en modo *recovery* (modo recuperación) a las *tablets*, con la finalidad de acceder a información sensible almacenada en estos dispositivos.
Proceso	- Se intentó acceder a la *tablet* en "modo recuperación", siguiendo las instrucciones del fabricante, sin éxito. - Haciendo uso de un cable de "conexión USB" se conectaron las *tablets* a una laptop, con la finalidad de determinar si la laptop puede detectar a la *tablet* haciendo uso del software *Samsung Kies 3*, obteniéndose como resultado negativo la ejecución de la prueba. - Adicionalmente se intentó usar el puerto Ethernet del adaptador LAN USB Hub para proporcionarle una dirección IP a las tablets y así intentar acceder a ellas, sin embargo, luego de conectarlas a una red aislada, éstas no obtuvieron ninguna dirección IP por lo que no fue posible obtener acceso.
Complejidad	**MEDIA** Para llevar a cabo esta prueba fue necesario: - Presionar el botón de apagado de la *tablet* e intentar acceder al dispositivo siguiendo las instrucciones del fabricante. - Acceder al interior de los módulos de la Estación de Comprobación de Identidad (ECI) y Cabina de Voto Electrónico (CVE), siendo este acceso restringido por una llave física a la cual tiene acceso única y exclusivamente el Coordinador Técnico de Mesa (CTM).
Resultado de la Prueba o Hallazgo	Se verificó que los puertos de acceso a *tablets* se encuentran bloqueados, lo cual impide que la *tablet* reconozca o sea reconocida por otro dispositivo. Por tal motivo, podemos concluir que el resultado de **la prueba es negativa**.
Riesgo	N/A
Recomendación	N/A
Comentario de ONPE	N/A

5.3. Pruebas sobre la computadora de transmisión de datos.

a. Revisión de usuarios del computador.

Titulo	Descripción
Prueba	Revisión de usuarios y sus accesos en la PC utilizada para la transmisión de datos.
Proceso	Para poder efectuar esta prueba se llevó a cabo lo siguiente: - Mediante la consola CMD, con un usuario ADMINISTRADOR, se ejecutó el comando ***net user,*** del cual

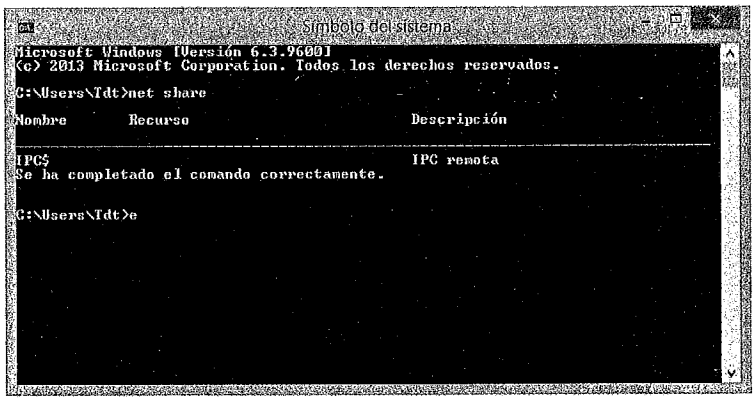
	se obtuvo como resultado tres de usuarios: *Administrador*, *Invitado* y *Tdt*. - Posteriormente, validamos que las cuentas Administrador e Invitado, son cuentas de usuario por defecto de la PC; sin embargo el usuario Tdt es una cuenta local sin privilegios administrativos sobre el equipo, que es creada en el equipo de transmisión por el personal de ONPE, y es usado durante el proceso de envío de información en el proceso de electoral desde el punto de transmisión. 
Complejidad	**MEDIA** Para poder ejecutar esta prueba fue necesario contar con la contraseña de ADMINISTRACIÓN la cual NO ES conocida por el Técnico de Transmisión (TDT). Asimismo, fue necesario conocer los comandos que se deben ejecutar para poder identificar los usuarios locales en el equipo.
Resultado de la Prueba o Hallazgo	Se verificó que solo el usuario *Tdt* cuenta con los permisos correspondientes para llevar a cabo el envío de la información. Por tal motivo, podemos concluir que el resultado de **la prueba es negativa**.
Riesgo	N/A
Recomendación	N/A
Comentario de ONPE	N/A

b. Revisión de puertos TCP/UDP abiertos en el computador.

Titulo	Descripción
Prueba	Revisión de puertos TCP/UDP abiertos en la PC utilizada para la transmisión de votos.
Proceso	Para poder llevar a cabo esta prueba se realizaron las siguientes actividades: - Se intentó realizar el escaneo e identificación de los puertos TCP/UDP sin éxito, dado que el antivirus bloquea estas actividades. - Se intentó deshabilitar el antivirus sin éxito, dado que con el usuario limitado con el que se accede no es posible deshabilitar el antivirus. Por tales motivos, podemos concluir que el resultado de **la prueba es negativa**.
Complejidad	**MEDIA** Para poder ejecutar esta prueba fue necesario contar con la contraseña de acceso a la PC, la cual es conocida solo por el Técnico de Transmisión. Asimismo, es necesario

	deshabilitar el antivirus y finalmente realizar el procedimiento de escaneo de puertos.
Resultado de la Prueba o Hallazgo	No se pudo escanear por puertos abiertos debido al antivirus y dado que el antivirus no se puede deshabilitar podemos concluir que el resultado de **la prueba es negativa**.
Riesgo	N/A
Recomendación	N/A
Comentario de ONPE	N/A

c. Revisión del "share administrativo".

Titulo	Descripción
Prueba	Revisión de recursos compartidos en la PC utilizada para la transmisión de datos.
Proceso	Para poder efectuar esta prueba se llevó a cabo lo siguiente: - Mediante la consola CMD, con un usuario ADMINISTRADOR, se ejecutó el comando ***net share,*** del cual se obtuvo como resultado que los recursos compartidos por defecto, como el **C$ y ADMIN$** no se encuentran habilitados, estando de acuerdo a las recomendaciones de buenas prácticas de seguridad, que señalan que estos recursos deberían encontrarse deshabilitados. 
Complejidad	**MEDIA** Para poder ejecutar esta prueba fue necesario contar con la contraseña de ADMINISTRACIÓN la cual NO ES conocida por el Técnico de Transmisión (TDT). Asimismo, fue necesario conocer y saber que comandos ejecutar para poder identificar los recursos habilitados por defecto.
Resultado de la Prueba o Hallazgo	Como resultado de la ejecución de la prueba, verificamos que los recursos compartidos por defecto **C$ y ADMIN$,** no se encuentran habilitados. Por tal motivo, podemos concluir que el resultado de **la prueba es negativa**.
Riesgo	N/A
Recomendación	N/A
Comentario de ONPE	N/A

5.4. Instalación de *sniffing* de red para evaluar la información que es transmitida al realizar la transmisión de datos.

Titulo	Descripción
Prueba	Instalación de *sniffing* de red que permita evaluar el tipo de información que es transmitida al realizar la transmisión de datos.
Proceso	Se instaló la herramienta Wireshark en el equipo de transmisión, con la finalidad de poder analizar el tráfico que es enviado desde la aplicación de transmisión hacia el sistema central. Se conectó el equipo a Internet usando el dispositivo USB de acceso y se procedió a cargar la herramienta Wireshark en iniciar el proceso de captura de datos, luego se ejecutó la aplicación de trasmisión de votos, se inició sesión en la aplicación de transmisión usando las credenciales proporcionadas por el personal de la ONPE y se realizó las transmisión de los datos. Finalizado el proceso se detuvo la captura de tráfico y se guardó la información generada.
Complejidad	**ALTA** Para realizar esta prueba es necesario contar con accesos administrativos sobre el equipo, requeridos para instalar aplicaciones. Dichos accesos no son accesibles desde el perfil que utiliza el TDT (Técnico de transmisión).
Resultado de la Prueba o Hallazgo	Se identificó que el tráfico de información desde la estación de transmisión hacia el sistema central de la ONPE, cuya URL pública es https://sea.onpe.gob.pe, se encuentra cifrado, lo cual hace imposible que se pueda comprometer o alterar dicha información.
Riesgo	N/A
Recomendación	Para la transmisión de los resultados del proceso de votación, la ONPE ha diseñado una infraestructura que consta de un equipo de cómputo instalado en cada centro de votación, que cuenta con un software que permite la lectura y transmisión de la información contenida en los dispositivos USB generados por cada mesa de sufragio y un sistema que se encuentra público en Internet que recibe los resultados de los centros de votación. La información viaja de manera cifrada e imposibilita la interceptación y modificación de la misma. Sin embargo, recomendamos evaluar la posibilidad de que ninguna de las partes del sistema esté publicada en Internet, sino que los equipos deberían conectarse a una VPN, y antes de poder iniciar la transmisión, cada equipo deberá ser analizado y de encontrarse conforme, se le permita el acceso al sistema.
Comentario de ONPE	La ONPE cuenta con equipos de transmisión tipo BGAN con los que configura VPNS's desde el local de votación a la sede central para la transmisión de la información. Adicionalmente al conectarse el sistema remoto a la sede central se realiza una validación automática del hash, la cual, de no ser validada, no permite la conexión. Cabe precisar que la ONPE se adecúa a las mejores tecnologías posibles y coberturas disponibles de los servicios de telecomunicaciones en las zonas donde se encuentran los locales de vocación.

5.5. Revisión de información transferida en las tarjetas de configuración (tarjeta morada), administración (tarjeta verde) y activación (tarjeta azul).

Título	Descripción
Prueba	Revisión de información transferida en las tarjetas configuración (tarjeta morada), administración (tarjeta verde) y activación (tarjeta azul). Para llevar a cabo la revisión del contenido de las tarjetas se hará uso de una lectora de tarjetas inteligentes proporciona por la ONPE.
Proceso	Se procedió a llevar a cabo las siguientes actividades: **1. Revisión de la "Tarjeta de Activación"** - Inicialmente, se activaron las credenciales del votante en la tarjeta de color azul. • **Prueba 01:** DNI 46672497 • **Prueba 02:** DNI 76355521 • **Prueba 03:** DNI 76619579 - Luego, con el uso de una lectora de tarjetas procedimos a analizar la información generada al activar las credenciales, obteniéndose lo siguiente: • **Prueba 01:** ONPE-ACT-000036-3-1-gDcoPSITHZVweF+ASUzoAg==#0000# • **Prueba 02:** ONPE-ACT-000036-3-1-Ev8ChpbsuIrSxZ4cPj8QiA==#0000# • **Prueba 03:** ONPE-ACT-000036-3-1-l6Hb6+xT9SUAIKEAO9rPAQ==#0000# De las pruebas de simulación efectuadas, podemos validar que el código generado al activar las credenciales del votante es un código cifrado. **2. Revisión de la "Tarjeta de Administración"** - Se llevaron a cabo simulaciones de "Puesta en Cero" en las mesas de sufragio N° 0036 y N° 0047, con la finalidad de validar el tipo de información que se almacena y transfiere en la tarjeta de color verde, obteniendo como resultado lo siguiente: • Línea 01: datos conocidos como Semilla. Se trata de un *"hash de cifrado"*, que hace posible el cifrado de toda la información grabada en la tarjeta. • Línea 02: datos que hacen referencia al proceso electoral que se está desarrollando, como por ejemplo: el tipo de elección y la fecha. • Línea 03: información que hace referencia al registro histórico de las actividades efectuadas por los miembros de mesa, actividades tales como: fecha y hora de la instalación de la mesa de sufragio, fecha y hora de la puesta en cero de la mesa de sufragio, fecha y hora del cierre de la mesa de sufragio, entre otros. • Línea 04: información referente al conteo de votos emitidos en la Cabina de Voto Electrónico (CVE). • Línea 05: protocolo que permite la administración y asociación de las claves generadas en la Estación de Comprobación de Identidad (ECI) y en la Cabina de Voto Electrónico (CVE), al momento de instalar la mesa de sufragio.

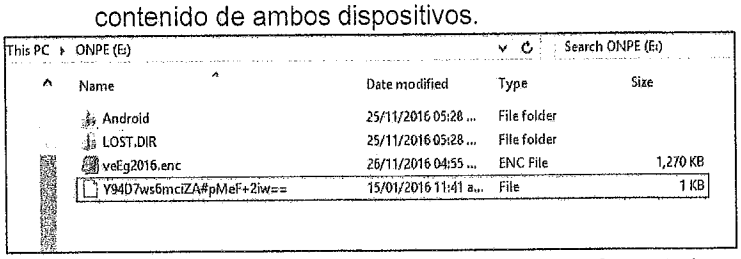
	3. Revisión de la "Tarjeta de Configuración - Se simuló la instalación de una mesa de sufragio, partiendo desde la configuración inicial de las *tablets* en la Estación de Comprobación de Identidad (ECI) y Cabina de Votación Electrónica (CVE). Para poder realizar dicha configuración se utilizó la tarjeta de color morado, seguidamente, se procedió a analizar la información que se almacena y transfiere en dicha tarjeta, dónde se verificó la existencia de un "código cifrado" el cual hace posible la conexión y configuración entre las *tablets*. Asimismo, según lo relevado con el personal de ONPE, el código identificado en realidad es una llave cifrada, la cual es generada por única vez para cada proceso electoral. Es preciso mencionar que para poder realizar la lectura de la información almacenada en las tarjetas de administración y configuración se utilizó una aplicación, denominada "ver contenido", proporcionado por la ONPE.
Complejidad	**ALTA** Para llevar a cabo esta prueba fue necesario: - Contar con las tarjetas de configuración, administración y activación. - Contar con un lector de tarjetas. - Contar con la aplicación, denominada "ver contenido", el cual permite efectuar la lectura de la información almacenada en las tarjetas verde y morada. Debido a que el acceso a las tarjetas está restringido sólo para el Coordinador Técnico de Mesa (CTM) y para los miembros de mesa, es poco probable que un usuario externo pueda llevar a cabo esta prueba de forma exitosa.
Resultado de la Prueba o Hallazgo	Identificamos que al momento de realizar la transmisión de información, la ONPE ha implementado mecanismos de cifrado de datos, lo cual imposibilita la lectura de dicha información. Por tal motivo, podemos concluir que el resultado de **la prueba es negativa**.
Riesgo	N/A
Recomendación	N/A
Comentario de ONPE	N/A

5.6. Reemplazo del contenido del USB de "Transmisión de Resultados".

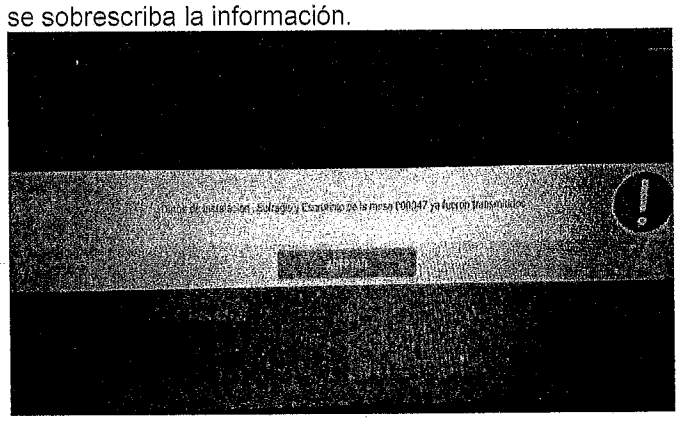
Titulo	Descripción
Prueba	Modificar o reemplazar los archivos del USB de "Transmisión de Resultados" con la finalidad de manipular los datos que son enviados desde el punto de transmisión hacia la sede central.
Proceso	Se procedió a llevar a cabo las siguientes actividades: 1. Se realizó el proceso de apertura, votación y cierre de dos mesas de sufragio. Al finalizar este proceso se generaron los USB con la información de transmisión. 2. Para verificar que la información era correcta, se insertó ambos dispositivos USB en el equipo de transmisión y se

mostró el número de la mesa a la que estaba asociado cada dispositivo.

3. Se revisó el contenido de ambos dispositivos, encontrándose la misma estructura de archivos. Adicionalmente se obtuvo una copia de respaldo del contenido de ambos dispositivos.



4. Se usó un tercer USB que previamente se formateó, y se procedió a copiar el archivo *veEg2016.enc* que se obtuvo de uno de los dispositivos USB correspondientes a una de las dos mesas de votación.
5. Este USB se insertó en el equipo de transmisión y fue detectado por el software de transmisión de votos. Aquí pudimos determinar que los archivos y carpetas restantes no son necesarios para que el software de transmisión lea el archivo conteniendo el resumen del escrutinio.
6. Se procedió realizar el proceso de transmisión los votos, el cual fue exitoso.
7. Una vez finalizado el proceso, se verificó nuevamente el contenido del USB en un equipo, se logró determinar que la fecha de modificación de éste había cambiado. Lo que nos indica que el sistema de transmisión modifica el archivo de transmisión, para marcarlo como un archivo ya transmitido.
8. Se volvió a copiar en el USB de transmisión el archivo *veEg2016.enc* el cual se había respaldado anteriormente. Se insertó el USB en el equipo de transmisión, se activó la opción para iniciar la transmisión de los votos y se intentó realizar nuevamente éste proceso, pero apareció un mensaje con el texto "*Datos de instalación, Sufragio y Escrutinio de la mesa ya fueron transmitidos*", lo cual indica que al momento de enviar la información a la ONPE, el sistema valida si ya existe información del escrutinio en el sistema, de ser este caso, éste impide que se sobrescriba la información.



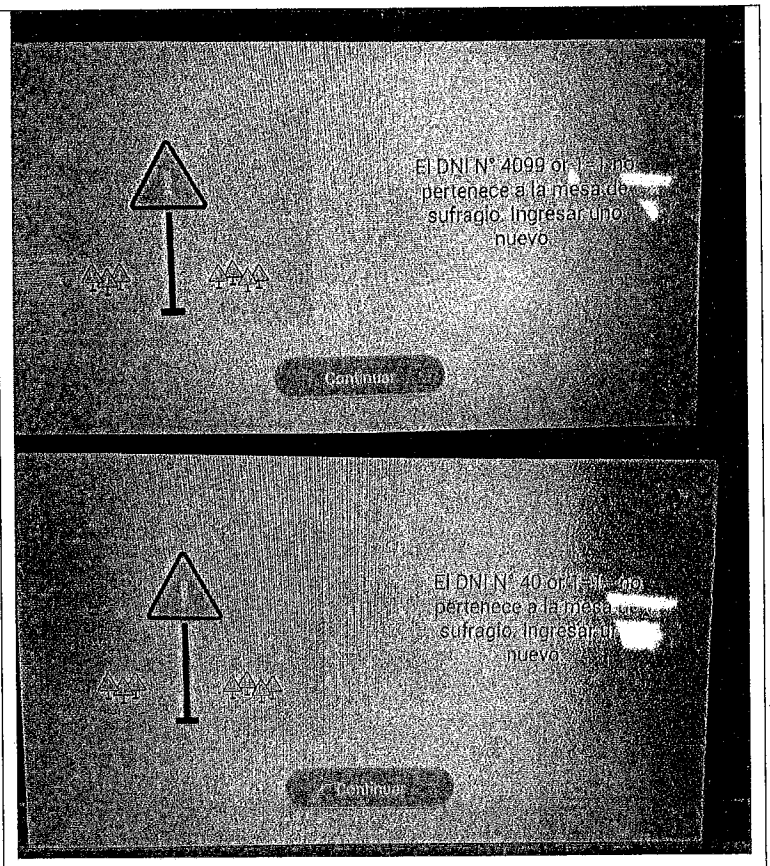
Complejidad	**ALTA**

Resultado de la Prueba o Hallazgo	Se determinó que el sistema está preparado para evitar que se sobrescriba la información del escrutinio de las mesas. El resultado de esta prueba es **negativa**.
Riesgo	N/A
Recomendación	Luego de entender el proceso de voto electrónico desarrollado por la ONPE, identificamos que uno de los puntos a mejorar es el proceso de transmisión de los resultados de escrutinio. Recomendamos evaluar que la persona designada para trasladar el dispositivo USB de transmisión desde la mesa de votación al Punto de Transmisión, deba ser supervisada.
Comentario de ONPE	El traslado del dispositivo de transmisión (USB) se realiza a través de una cadena de custodia, donde se registran y suscriben las personas que participan (Coordinador técnico de mesa, miembro de mesa y Técnico de transmisión). Adicionalmente la información impresa de las actas, que es entregada a los personeros y JNE, puede ser revisada y contrastada en Internet, en la página web de la ONPE.

O

5.7. Crear un código de barras de identificación de DNI falso con una inyección de código SQL.

Titulo	Descripción
Prueba	Crear un código de barras de identificación de DNI falso con una inyección de código SQL.
Proceso	La finalidad de ésta prueba era determinar si se podía obtener acceso a la base de datos de la Estación de Comprobación de Identidad, para ello se generaron códigos de barra usando números de DNI a los cuales se les agregó los parámetros usados para la inyección de código SQL, como por ejemplo: "XXXXXXX or 1=1". Luego, en la Estación de Comprobación de Identidad, en la opción de Identificación del Elector se procedió a escanear los códigos con la lectora de códigos de barras, pero se obtuvo un mensaje de error indicando que el código ingresado no correspondía a un DNI perteneciente a la mesa de sufragio.

	
Complejidad	**MEDIA** Para poder realizar esta prueba fue necesario determinar qué tipo de código de barras se había usado en el padrón que nos habían proporcionado.
Resultado de la Prueba o Hallazgo	Se determinó que el sistema de votación está preparando para soportar un intento de inyección de código SQL, impidiendo el acceso a un usuario externo a los datos (Listado de votantes) contenidos en la Tablet. El resultado de la prueba es **negativo**.
Riesgo	N/A
Recomendación	N/A
Comentario de ONPE	N/A

5.8. Pruebas de acceso inalámbrico a la *tablets*.

Titulo	Descripción
Prueba	Verificar si los accesos vía *bluetooth y wifi* están bloqueados en las *tablet*as de la cabina de votación y de la cabina de identificación.
Proceso	- Inicialmente, se intentó acceder a la configuración de las *tablets* haciendo uso de los permisos de las tarjetas morada, verde y azul, verificándose que no era posible. - Posteriormente, mediante el uso de diferentes dispositivos (celulares y laptops), se procedió a hacer un reconocimiento vía *bluetooth* a las *tablet*as de cabina de votación y de la cabina de identificación, sin éxito.

Complejidad	**MEDIA** Para poder realizar la prueba, fue necesario contar con las tarjetas de acceso, y conocer la clave del usuario administrador, sin embargo se verificó que la *tablet* estaba configurada para no permitir la conexión vía *bluetooth y wifi.*
Resultado de la Prueba o Hallazgo	Identificamos que la ONPE ha bloqueado los accesos a las *tablet*as vía bluetooh y *wifi.* Por tal motivo, podemos concluir que el resultado de **la prueba es negativa**.
Riesgo	N/A
Recomendación	N/A
Comentario de ONPE	N/A

5.9. Pruebas sobre el proceso de grabado de datos en la cabina de votación para validar la confidencialidad del voto.

Titulo	Descripción
Prueba	Prueba sobre el proceso de grabado de datos en la cabina de votación para validar la confidencialidad del voto. El objetivo el realizar esta prueba es conocer el mecanismo de grabado de los datos en la Cabina de Voto Electrónico (CVE), para saber si existe alguna manera de ligar la votación al votante.
Proceso	Con la finalidad de entender el proceso de grabado de datos en la Cabina de Voto Electrónico, se llevó a cabo una reunión con el personal de ONPE, donde se relevó lo siguiente: - Cuando se activan las credenciales del votante por medio del uso de la tarjeta azul en la Estación de Comprobación de Identidad (ECI), se generan códigos cifrados los cuales serán reconocidos en Cabina de Voto Electrónico (CVE); solo una vez reconocido este código cifrado será posible la emisión del voto (tipo desafío). - En la *tablet* de la CVE existen dos tablas, una de credenciales (que es donde se almacena los códigos generados por la ECI por cada elector) y otra de votos (que es donde se almacena los votos). Es importante indicar que estas tablas inicialmente no cuentan con ningún dato pre-cargado. - Cuando se registra el voto, se generan dos registros aleatorios, uno en la tabla de votos y otro en la tabla de credenciales. - Se relevó también que se graban logs de todas las actividades realizadas en la *tablet* de la Cabina de Voto Electrónico (CVE) en otra tabla, sin embargo no se registra la credencial ni el voto emitido por el elector. - Dado que en el ambiente en producción, todos los contenidos están cifrados, para poder validar lo anterior, se solicitó una versión especial del software en la CVE que permitía visualizar el contenido de las tablas mencionadas, validando que efectivamente la información es grabada de manera aleatoria y no es posible vincular el votante con el voto.
Complejidad	**ALTA** Para poder entender el funcionamiento del grabado de datos fue necesario el apoyo del personal de la ONPE involucrado

	en el desarrollo del proyecto, y verificándose que son las únicas personas autorizadas que cuentan con acceso al código fuente. Así mismo fue necesario que el personal de desarrollo de ONPE genere una versión especial del software de la CVE que permitía visualizar la información almacenada (sin cifrar), por tal motivo sería muy complicado llevar a cabo esta prueba en un proceso de elecciones real.
Resultado de la Prueba o Hallazgo	Para entender en funcionamiento técnico de la aplicación es necesario tener los conocimientos necesarios de programación, y adicionalmente, conocer correctamente el flujo y proceso del voto electrónico. Adicionalmente se validó que los datos del votante y los datos del voto son almacenados en tablas diferentes, de manera aleatoria, garantizando con ello la confidencialidad del voto. Por tal motivo, podemos concluir que el resultado de **la prueba es negativa**.
Riesgo	N/A
Recomendación	N/A
Comentario de ONPE	N/A

5.10. Prueba de revisión de código de las aplicaciones utilizadas en la Estación de Comprobación de Identidad (ECI) y Cabina de Voto Electrónico (CVE).

Titulo	Descripción
Prueba	Prueba de revisión de código fuente de las aplicaciones utilizadas en la Estación de Comprobación de Identidad (ECI) y Cabina de Voto Electrónico (CVE). El objetivo es identificar que no haya código escondido que ante alguna combinación de *taps* en las pantallas se active y pueda existir algún tipo de manipulación de los datos.
Proceso	Con la finalidad de revisar y entender el funcionamiento del código fuente de las aplicaciones, se llevó a cabo una reunión con el personal de ONPE, donde se visualizó el código fuente y se relevó lo siguiente: - El lenguaje utilizado en el desarrollo de la app del proceso de voto electrónico es JAVA. La base de datos de la *tablet* de la Cabina de Voto Electrónico (CVE) se encuentra en formato XML cifrado. Adicionalmente, fue posible identificar que el *framework* utilizado para el proyecto en cuestión es *ANDROID STUDIO 2.2.3.* - Se nos informó que por cada versión de la aplicación utilizada en un proceso electoral vinculante se genera una copia del código fuente para el Jurado Nacional de Elecciones (JNE), quien se encargará de validar el correcto funcionamiento y el uso de la versión oficial del *app* en el día de las elecciones. Adicionalmente, el personal del Jurado Nacional de Elecciones (JNE) hace visitas y revisiones periódicas del código de la aplicación desarrollado por los programadores de la ONPE.
Complejidad	**ALTA** Para poder entender el funcionamiento técnico de la aplicación fue necesario el apoyo del personal de la ONPE involucrado en el desarrollo del proyecto, y verificándose que son las únicas personas autorizadas que cuentan con acceso al código fuente, por tal motivo sería complicado que un

	usuario externo vulnere o altere el desarrollo debido a su complejidad.
Resultado de la Prueba o Hallazgo	Para entender en funcionamiento técnico de la aplicación es necesario tener los conocimientos necesarios de programación, y adicionalmente, conocer correctamente el flujo y proceso del voto electrónico. Por tal motivo, podemos concluir que el resultado de **la prueba es negativa**.
Riesgo	N/A
Recomendación	N/A
Comentario de ONPE	N/A

5.11. Prueba de revisión de "versiones" de la app instalada versus la app "autorizada" en el proceso de voto electrónico.

Titulo	Descripción
Prueba	Prueba de revisión de "versiones" de la app instalada versus la app "autorizada". La finalidad es conocer el mecanismo mediante el cual la ONPE se asegura de que se está haciendo uso de la versión oficial del software autorizado en todas las mesas de sufragio donde se aplica el voto electrónico.
Proceso	Se planteó la consulta al personal de ONPE referente al uso de la versión oficial del software en el proceso de voto electrónico, y nos informaron que el Jurado Nacional de Elecciones (JNE) asigna fiscalizadores en las mesas de sufragio, quienes son los encargados de validar el uso de la versión autorizada del app. Es importante mencionar que para poder efectuar esta validación, el fiscalizador cuenta con el *hash* del software a utilizar el día proceso electoral. Por otro lado, durante el proceso de "puesta en cero" de las *tablets*, fue posible identificar la versión de la app en la parte superior derecha de la *tablet*.
Complejidad	N/A
Resultado de la Prueba o Hallazgo	En base a la información relevada e identificada podemos indicar que la ONPE ha establecido ciertos mecanismos de validación a fin de garantizar el uso de la versión de la app autorizada en el proceso de voto electrónico, por tal motivo se concluye que la ejecución de la presente prueba es **negativa**.
Riesgo	N/A
Recomendación	N/A
Comentario de ONPE	N/A

6. CONCLUSIÓN Y RESULTADOS

Tomando en cuenta nuestro entendimiento del proceso y todas las pruebas realizadas podemos concluir que el proceso revisado de Voto Electrónico de la ONPE a Enero del 2017 es razonablemente SEGURO a nivel de ataques informáticos. No nos fue posible vulnerar, alterar, acceder, modificar o eliminar ningún dato en el proceso mencionado.

7. RECOMENDACIONES FINALES

Se identificaron algunas recomendaciones mencionadas a lo largo del informe cuya aplicabilidad corresponde ser evaluada por la ONPE.

Clark Stanley Velando Leiva
Gerente General
KUNAK CONSULTING SAC