TECNOLÓGICO DE MONTERREY®

Dictámen final sobre Auditoría de Seguridad Información

Recomendaciones Finales

Descripción breve

En este documento se hacen recomendaciones sobre lo que encontró en las plataformas y análisis que se les hizo durante este trabajo

Jesús R. González / Juan Arturo Nolazco

jrgonza@gmail.com jnolazco@itesm.mx

Índice

Versión	Fecha	Descripción
1.0	18 – Mayo – 2017	Documento de análisis de riesgos correspondiente a la infraestructura del conteo rápido del IEC Análisis de vulnerabilidades

Dictamen elaborado por MsC. Jesús Raúl González Hernández en coordinación con Dr. Juan Arturo Nolazco.

1 Resumen Ejecutivo

Este documento hace recomendaciones sobre medidas y controles para el tratamiento de los riesgos y amenazas que se documentaron durante el proceso de análisis de vulnerabilidades del IEC.

2 Alcances y limitaciones

Las recomendaciones se dan en base a los datos obtenidos por escaneo de los sistemas de TI así como de entrevistas que se obtuvo por personal del IEC. Dados los tiempos bajo los cuales se hizo este proyecto, se recomienda efectuar posteriormente un análisis más a detalle sobre las cuestiones de riesgos de recursos humanos así como de los procesos de la organización.

2.1 Audiencia

Las recomendaciones hechas en este documento van dirigidas hacia el personal del IEC y primordialmente hacia las siguientes personas

- personal Técnico de administración de infraestructura quienes son los responsables de tomar medidas para aminorar los impactos en los sistemas de TI y que potencialmente afectará la operación de estos.
- Personal administrativo que lleva la gestión de las áreas de TI y procesos.
- Personal con responsabilidades de la gestión de riesgos

3 Análisis de riesgo

3.1 Identificación de amenazas

La amenaza es el potencial para que una persona o situación, pueda exitosamente explotar una vulnerabilidad particular. La vulnerabilidad es una debilidad que puede ser tanto accidentalmente como intencionalmente explotada.

Para la identificación de amenazas las clasificaremos en dos fuentes y los distintos procesos del IEC que hemos visto. Las fuentes que se definen son:

Tipo Amenaza	Descripción	Comentario
Interna	Fuentes que provienen de adentro de las instalaciones del IEC	• La amenaza interna aunque puede tener un impacto alto, se ve poco probable que pueda hacer algo a menos que hubiese una persona no autorizada adentro de la red, lo cual implicaría que no hay control de acceso de personas a los sitios de captura.
Externa	Fuentes que no pertenecen al IEC y no están dentro de las instalaciones	• Las amenazas externas, aunque tienen una probabilidad alta de causar afectación (por la mayor disponibilidad de personal especializado). • Dada la configuración del sistema, el enfoque de dicha persona sería en causar daño y afectar la operación pero dado los controles y limitaciones que se tienen en los sistemas, se ve con una baja probabilidad de que esto ocurra, aunque con un alto impacto

Los procesos sobre los cuales se analizan estas amenazas son:

- Captura – Esto comprende todo el proceso de captura una vez que acaba la elección y cierra la casilla, hasta el momento del envío del acta al centro de acopio central.
- Procesamiento – Esto es toda la labor que se hace durante el proceso de consolidación y validación en el centro de acopio central.
- Publicación – Este es el proceso de empujar la información del centro de datos hacia los sitios replicantes

Las amenazas identificadas en base a los escaneos y entrevistas que se hicieron solo se clasifican para información, su calificación se llevará en el proceso

3.2 Identificación de vulnerabilidades

Como parte de la investigación hecha a las aplicaciones montadas en los servidores, se pudo revisar una lista de vulnerabilidades basada en la Base de datos Nacional de Vulnerabilidades (NVD) con sus grados de severidad (solo se incluyeron los de severidad media hacia arriba)

IP	Puerto	Aplicación		
10.50.1.8	TCP/22	HP Integrated Lights-Out mpSSH 0.2.1	-	-
	TCP/80	HPE-iLO-Server/1.30 (SSH)	CVE-2016-4375	Crítico (9.8)
			CVE-2015-5435	Medio (4.0)
	TCP/443	ssl/https HPE-iLO-Server/1.30		
10.50.1.9	TCP/22	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1	CVE-2015-8325	Alto (7.8)
			CVE-2016-3115	Medio (6.4)
	TCP/80	HPE-iLO-Server/1.30	-	-
	TCP/443	ssl/https HPE-iLO-Server/1.30	-	-
10.50.1.10	TCP/22	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1	CVE-2015-8325	Alto (7.8)
			CVE-2016-3115	Medio (6.4)
	TCP/80	Apache httpd 2.4.18	CVE-2016-4979	Alto (7.5)
			CVE-2016-1546	Medio (5.9)
10.50.1.11	TCP/22	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1	CVE-2015-8325	Alto (7.8)
			CVE-2016-3115	Medio (6.4)
10.50.1.100	TCP/80	Apache/2.4.18 (Ubuntu)	CVE-2016-4979	Alto (7.5)
			CVE-2016-1546	Medio (5.9)
	TCP/22	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1	CVE-2015-8325	Alto (7.8)
			CVE-2016-3115	Medio (6.4)
10.50.1.101	TCP3306	MySQL 5.7.17-0ubuntu0.16.04.2	CVE-2017-3600	Medio (6.6)
			CVE-2017-3599	Alto (7.5)
			CVE-2017-3455	Medio (5.5)
			CVE-2017-3454	Medio (5.4)
			CVE-2017-3453	Medio (6.5)
			CVE-2017-3450	Alto (7.5)
			CVE-2017-3331	Medio (6.5)
			CVE-2017-3329	Alto (7.5
			CVE-2017-3309	Alto (7.7)
			CVE-2017-3308	Alto (7.7)
10.50.1.102	-	Detectado pero no reporto puertos	-	-
10.50.1.103	TCP/80	nginx/1.10.0 (Ubuntu)	CVE-2012-1180	Medio (5.0)
10.50.1.104	TCP/21	vsftpd 2.0.8 or later		
10.50.1.105	-	Detectado pero no reporto puertos	-	-
10.50.1.106	TCP/80	Apache httpd 2.4.18 ((Ubuntu))	CVE-2016-4979	Alto (7.5)
			CVE-2016-1546	Medio (5.9)
10.50.1.107	-	Detectado pero no reporto puertos	-	-
10.50.1.108	TCP/8086	InfluxDB http admin 1.2.2	-	-
10.50.1.109	TCP/3000	Grafana	-	-
10.50.1.110	-	Detectado pero no reporto puertos	-	-
10.50.1.111	TCP/80	Apache httpd 2.4.18	CVE-2016-4979	Alto (7.5)
			CVE-2016-1546	Medio (5.9)

NOTA: Estas vulnerabilidades no aparecieron en los escaneos, aunque están clasificadas como tal. La razón es que o tienen parche instalado o el puerto no dejo averiguar sobre estas. (Solo se incluyeron las de medio hacia arriba)

Las vulnerabilidades identificadas en el escaneo y que están basadas en la base de datos OSVBD como la lista lo muestra, estas fueron puestas dentro del análisis de riesgo como parte de la evidencia que se encontró.

ID OSVDB	ID CVE	Descripción	Probabilidad	Impacto	Justificación
OSVDB:576	CVE-2015-1476	Requerir un directorio con %00/, %2e/, %2f/ or %5c/ al final causa que el servidor muestre contenidos del directorio.	Medio	Medio	• PROBABILIDAD M – El capturista debe conocer bien la aplicación para poder hacer esta actividad. • IMPACTO M – No podrá hacer nada ya que se maneja por entradas en las páginas para llenar datos de actas.
OSVDB:119	CVE-1999-0269	Servidor remoto puede permitir listado de directores vía web, forzando a mostrar los archivos al solicitarlo en el browser.	Medio	Medio	• PROBABILIDAD M – El capturista debe conocer bien la aplicación para poder hacer esta actividad. • IMPACTO M – No podrá hacer nada ya que se maneja por entradas en las páginas para llenar datos de actas.
OSVDB:3092		/webdav/index.html: WebDAV esta habilitado.	Bajo	Bajo	• PROBABILIAD B – Indicativo que WebDav corre en ese puerto • IMPACTO M – No podrá hacer nada ya que se maneja por entradas en las páginas para llenar datos de actas
OSVDB:3288		directory listing when /'s are requested	Bajo	Medio	• PROBABILIDAD B – El capturista debe conocer bien la aplicación para poder hacer esta actividad. • IMPACTO M – No podrá hacer nada ya que se maneja por entradas en las páginas para llenar datos de actas.

10.50.1.103					
ID OSVDB	**ID CVE**	**Descripción**	**Probabilidad**	**Impacto**	**Justificación**
OSVDB:3092		/webdav/index.html: WebDAV está habilitado.	Bajo	Bajo	• PROBABILIAD B – Indicativo que WebDav corre en ese puerto • IMPACTO M – No podrá hacer nada ya que se maneja por entradas en las páginas para llenar datos de actas

10.50.1.106					
ID OSVDB	**ID CVE**	**Descripción**	**Probabilidad**	**Impacto**	**Justificación**
OSVDB-3233		/jsp-examples/: Apache Java Server Pages documentation	Bajo	Bajo	• PROBABILIDAD B – El capturista debe conocer bien la aplicación para poder hacer esta actividad. • IMPACTO B – No podrá hacer nada ya que se maneja por entradas en las páginas para llenar datos de actas

10.50.1.109					
ID OSVDB	**ID CVE**	**Descripción**	**Probabilidad**	**Impacto**	**Justificación**
OSVDB-35878		Modulo PHP-Nuke permite Usuarios ver usuarios y claves	Bajo	Bajo	• PROBABILIDAD B – El capturista debe conocer bien la aplicación para poder hacer esta actividad. • IMPACTO B – No podrá hacer nada ya que se maneja por entradas en las páginas para llenar datos de actas
OSVDB-3092		/webdav/index.html: WebDAV esta habilitado.	Bajo	Bajo	• PROBABILIAD B – Indicativo que WebDav corre en ese puerto • IMPACTO M – No podrá hacer nada ya que se maneja por entradas en las páginas para llenar datos de actas

El análisis de los controles de estas vulnerabilidades se encuentra en la sección de controles tecnológicos agrupados con otras que comparten controles similares.

3.3 Análisis de controles

Los controles de los que se analizaron durante las entrevistas se clasifican en dos:

- **Procedurales** – Estos son los que se establecen ya sea vía una política o proceso de trabajo y se refuerza mediante la capacitación y/o supervisión físicas a personas que estarán operando el día de las elecciones.
- **Tecnológicos** – Estos son controles son aquellos que se establecen dentro de la infraestructura (cualquier elemento: ruteador, firewall, servidor, red, etc.) que restringe su uso y/o tráfico para evitar un mal uso de los recursos.

3.3.1 Controles procedurales

Los controles procedurales se estructuraron en tres partes tal como la identificación de amenazas y conforme a eso se tiene la siguiente tabla que describe el control para mitigar el riesgo y el estado de este

- Existe – El control existe y esta puesto en operación con lo que se mitiga el riesgo obtenido
- En proceso – Esta en proceso de implementarse.
- No existe – Actualmente no se tiene el control implementado

Captura						
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo**	**Controles**	**Estado**
• Acceso de personal no autorizado a las instalaciones (cualquier instalación asociada el proceso de elección)	• No hay registro de personal de captura en el centro	**Muy Baja**	**Medio**	**Bajo**	Existe un control de entrada para el personal	Existe
	• No se valida la entrada de personal	**Muy Baja**	**Alto**	**Medio**	Las personas de captura deben registrarse y sus pertenencias	Existe
• Ausencia de personal el día del proceso electoral a los centros de acopio o de procesamiento[1]	• No ha hay manuales que describan los procesos en sitio de operación	**Baja**	**Medio**	**Medio**	Imprimir manuales breves auto-explicable para que cualquier persona leyéndolo pueda tomar funciones	En proceso
	• Solo hay una persona que lo sabe operar	**Baja**	**Medio**			En proceso
• Acceso a la sala de captura con equipo ajeno a esta	• No tener registro de pertenencias	**Media**	**Alto**	**Alto**	En la entrada se debe registrar personas y sus pertenencias. Se dejan celulares y tabletas.	Existe
	• No tener punto de control de entrada en el sitio de captura	**Bajo**	**Alto**	**Medio**	Existe un control de entrada para el personal	Existe
• Brazo dañado para tomar fotografías con el teléfono	• No ha hay manuales que describan los procesos en sitio de operación	**Bajo**	**Bajo**	**Bajo**	Imprimir manuales breves auto-explicable para que cualquier persona leyéndolo pueda tomar funciones	En proceso
• Falta de conectividad	• Falla en los proveedores de Internet para conectar al sitio central	**Bajo**	**Medio**	**Medio**	En sitios con celular, tener dos chips de dos compañías En sitios con escáner tener celular y acceso vía DSL/Cable	Existe
• Mal uso de los teléfonos para captura	• Smartphone de captura controlado	**Bajo**	**Alto**	**Medio**	Aplicar restricciones en el equipo celular para evitar instalaciones de Aplicaciones innecesarias para el evento	Existe
	• Aplicación de captura Teléfono	**Bajo**	**Alto**	**Medio**		Existe
• Captura de datos no relacionados en la aplicación de captura central	• Validación de caracteres en la captura	**Muy Bajo**	**Medio**	**Bajo**	Limitar y validar los campos de captura en la aplicación para solo aceptar los caracteres que componen las actas.	Existe

[1] Para la situación de amenaza sobre la asistencia de personal no se hace ningún tipo de estudio sobre probabilidad de inasistencia por cuestiones de salud.

Operación Central						
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo**	**Controles**	**Estado**
• Falta de respuesta por proveedor de centro de datos externo en caso de caída de equipo de redundancia	• Sin respuesta por parte del equipo de soporte en el centro de datos	**Medio**	**Alto**	**Alto**	Acordar niveles de servicio con proveedores para tiempos de respuesta dentro de lo permitido para la operación de las elecciones	En desarrollo
	• Falla de servicio en la nube	**Medio**	**Alto**			En desarrollo
• Falla comunicaciones en el centro de acopio central	• Enlaces de sitios de centros de acopio remotos.	**Bajo**	**Medio**	**Medio**	Redundancia con planes de celulares de más de una empresa celular y/o DSL en caso que el enlace sea vía DSL.	Existe
	• Enlace de comunicación del centro acopio central	**Bajo**	**Medio**	**Medio**	Por ser sitio central, se tendrá o proveedor alterno de comunicaciones o con el proveedor de la nube.	Existe
• Caída de los sistemas local	• Por alguna razón los sistemas de captura fallan	**Medio**	**Alto**	**Alto**	Plan alterno en la nube	En desarrollo
	• Caída eléctrica	**Medio**	**Alto**	**Alto**	Planta eléctrica y Plan alterno en la nube	Existe
	• Falla HW	**Bajo**	**Alto**	**Alto**	Plan alterno en la nube	Existe
	• Falla de Disco por llenado	**Bajo**	**Medio**	**Medio**	Agregar cuotas por sitio y Plan alterno en la nube	En desarrollo
• Incidente que bloque capacidad operativa (procesamiento y captura) de actas de forma local	• Plan de contingencia	**Media**	**Alto**	**Alto**	Revisar contactos y tomar lista externo clave así como mantener en sitio al personal clave	En desarrollo
	• Matriz de responsables x aplicación	**Media**	**Alto**			Existe
	• Monitoreo de la infraestructura	**Medio**	**Medio**	**Medio**	Aparte del sistema de monitoreo, tener método manual de acceso para revisión de avance de captura	Existe

3.3.2 Controles Tecnológicos

Los controles tecnológicos están configurados en la infraestructura del IEC y estos son los que no se han encontrado en los escaneos así como en las entrevistas ya que algunos de ellos se implementarán posteriormente al proceso de auditoría.

- Existe – El control existe y esta puesto en operación con lo que se mitiga el riesgo obtenido
- En proceso – Esta en proceso de implementarse.
- No existe – Actualmente no se tiene el control implementado

Captura						
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo**	**Control**	**Estado**
• Uso inadecuado del Smartphone en sitios de acopio remotos	• Usuario controla Smartphone	**Bajo**	**Medio**	**Medio**	Aplicar restricciones en el equipo celular para evitar instalaciones de Aplicaciones innecesarias para el evento	Existe
	• Usuario pueda estar llamando	**Medio**	**Medio**	**Medio**	Restringir llamadas o solicitar solo plan de datos	Existe
• Problemas de transferencia de imágenes al sitio central de acopio	• Enlaces de sitios de centros de acopio remotos.	**Bajo**	**Medio**	**Medio**	Redundancia con planes de celulares de más de una empresa celular y/o DSL en caso que el enlace sea vía DSL.	Existe
	• Enlace de comunicación del centro acopio central	**Bajo**	**Medio**	**Medio**	Redundancia en proveedores de comunicación. Definir y describir plan en la nube para redundancia	Existe
	• Imagen sale defectuosa	**Bajo**	**Medio**	**Medio**	Retomar la fotografía	Existe
	• Servidor FTP para recibir imágenes	**Bajo**	**Medio**	**Medio**	Plan alterno en la nube	En desarrollo
	• Escáner para digitalización	**Bajo**	**Medio**	**Medio**	Planear tener teléfonos en caso de caída de escáner (si solo es un escáner el que hay en el sitio	Existe
	• Estación de captura	**Medio**	**Medio**	**Medio**	Reiniciar estación para resetearla.	Existe
	• Duplicación de Imágenes	**Bajo**	**Medio**	**Medio**	En el proceso de recaptura validaría que esta ya validada la captura	Existe
• Error de Captura	• Error humano al capturar números o cantidades de las actas	**Medio**	**Medio**	**Medio**	Se vuelve a capturar como proceso para validar valores	Existe
• Error reporte de avance	• Configuración del sistema de monitoreo GRAFANA	**Bajo**	**Medio**	**Medio**	Aparte del sistema de monitoreo, tener método manual de acceso para revisión de avance de captura	Existe
• Acceso a terminal de captura por personal no autorizado	• Login de acceso a las terminales de captura	Media	**Alto**	**Alto**	Asignar usuario y clave a cada capturista para tener seguimiento de actividades y/o manera de investigar cualquier incidente.	En desarrollo

En el proceso de operación se agruparon algunas vulnerabilidades que se encontraron en el escaneo sobre las que se tiene evidencia.

Operación						
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo**	**Control**	**Estado**
• Uso inadecuado de estaciones en el centro de acopio central	• Acceso al sistema operativo	**Medio**	**Alto**	**Alto**	Limitar acceso del usuario al sistema operativo o fuera de la aplicación de captura que debe utilizar	En desarrollo
	• Acceso a Internet	**Medio**	**Medio**	**Medio**	No permitir el acceso a Internet desde las estaciones de captura	En desarrollo
• Entrada de caracteres ilegales en la plataforma de captura	• Aplicación de captura	**Medio**	**Alto**	**Alto**	Validación y limitación de caracteres que no tienen que ver con los que contienen las actas	Existe
• Ataques a la BD MYSQL	• Acceso a la Base de datos ○ OSVDB-3233, OSVDB-35878, PSVDB-3092	**Bajo**	**Alto**	**Medio**	Acceso directo a la BD con usuario/clave solo para el administrador. Todos los demás son vía la interface de captura	Existe
	• Cortar la operación desde la aplicación de captura para ver datos del servidor	**Bajo**	**Alto**		Limitar acceso del usuario al sistema operativo o fuera de la aplicación de captura que debe utilizar	En desarrollo
• Ataque al servidor	• Cortar la operación desde la aplicación de captura para ver datos del servidor ○ OSBDV-3288, OSVDB-3233, OSBDV-119, OSVDB576	**Bajo**	**Alto**	**Medio**	Limitar acceso del usuario al sistema operativo o fuera de la aplicación de captura que debe utilizar Configurar avisos de fallas para no mostrar ninguna información	En desarrollo
• Falla de servidor (WebDav, Apache, MySQL)	• Caída sistema operativo	**Bajo**	**Muy Alto**	**Alto**	Definir y describir plan en la nube para redundancia	En desarrollo
• Entrar vía el túnel de IPSEC a la red de servidores del IEC	• Permitir una configuración Split-tunnel en la conexión al servicio de VPN	**Medio**	**Alto**	**Alto**	Configurar No-Split tunnel en el VPNC3000 para evitar navegación en Internet y captura de fotos de forma simultánea	En desarrollo
• Falla eléctrica	• Redundancia eléctrica	**Medio**	**Alto**	**Alto**	Tener una planta eléctrica en sitio para alimentación de redundancia	Existe
• Que alguien externo pueda entrar a modificar servidores o programas	• Acceso túnel de IPSEC conectado a Internet	**Bajo**	**Medio**	**Medio**	Datos de configuración IPSEC en equipos sin que el usuario tenga acceso a ella. Acceso a aplicaciones limitado a solo a un usuario con administrador	Existe
• Quedarse sin infraestructura	• No completar cantidad de equipos para captura	**Medio**	**Muy Alto**	**Alto**	Acuerdos de renta de equipos con la configuración requerida	En desarrollo
	• Falta de tiempo para instalación	**Bajo**	**Muy Alto**	**Alto**		En desarrollo

4 Recomendaciones adicionales

Como parte del trabajo se lista algunas recomendaciones adicionales sobre las plataformas e infraestructura que se resaltan y, que aunque posiblemente fueron mencionadas en los controles, dada su importancia se recomienda prestar particular atención a ellas.

4.1 Recomendaciones Procesos

1. Punto de revisión al entrar en las salas de captura – Aunque esta puesto y se aseguró que durante el evento estará cuidado por guardias y se tomará la lista y pertenencias, es importante recalcar que adentro del cuarto de captura del centro central de acopio no haya ningún dispositivo que permita la comunicación hacia afuera. Esto incluye celulares, cámaras y estaciones de trabajo.
2. Restringir el acceso con artículos personales – Cuando se recomienda esto se hacer referencia principalmente a artículos como equipos de telefonía celular con cámaras, tabletas etc. para evitar situaciones de fuga de información mediante fotografías de pantallas, conexiones ilegales a Internet (vía celular)
3. Diademas para los capturistas que toman llamadas – Esta situación se observó en el ensayo y sería algo que, en adición a la comodidad de los capturistas, evitaría pérdidas de tiempo al estar tomando la llamada y capturando valores en las pantallas por cuestiones de acomodar el teléfono para poder capturar datos en la aplicación
4. Aseguramiento de acuerdos de nivel de servicio – El proveedor de los servicios en la nube, cuyo procedimiento esta aún en desarrollo, debe mantener un acuerdo de servicio e IEC debe asegurar la operación bajo los niveles que requiere durante el día de las elecciones para mantener el flujo de información y el conteo de forma adecuada y en los tiempos estimados.
5. Matriz de responsables – La matriz de personas o equipos responsables de las aplicaciones debe mantenerse a la mano en todo el tiempo que dure el evento de las elecciones para asegurar cualquier tipo de incidente con dichas aplicaciones. De preferencia las personas o equipos deberán estar en sitio para poder dar soporte a las aplicaciones en caso que algún incidente se llegara a presentar.

4.2 Recomendaciones Tecnológicas

1. Configuración de túnel – Durante algunas de las pruebas se pudo detectar que al mismo tiempo que esta uno conectado en el túnel de IPSEC, es posible salir hacia Internet haciendo uso de la misma conexión. Esto potencialmente puede presentar un riesgo y se sugiere que se cancele. Esto como parte de las políticas del túnel para evitar que haya salida hacia otra red que no sea la del IEC mientras esta el túnel puesto.
2. Mantener la protección de los puertos vía FIXUP PROTOCOL: Mediante este comando se puede proteger los puertos usados en las aplicaciones del IEC para verificar los comandos enviados a dichos puertos en función de quien los envía y que es lo que solicita o envía.

Los puertos a cubrir con esto serían: TCP/22, TCP/80, TCP/443, TCP/3306. Esto permitirá cubrir abusos que se quiera hacer de forma directa hacia los puertos de las aplicaciones. Esta configuración en el VPNC no permitió hacer explotación de puertos o de aplicaciones debido a que restringe las operaciones en los puertos/aplicaciones.

3. Aunque en la fecha del desarrollo se nos aseguró que se estaba en el proceso de implementar una alternativa en un sitio de un centro de datos para tener dicha opción, al día de la revisión aún no estaba en función dicho plan y no pudo verificarse. Existe la seguridad y certeza que el plan estará implementado antes del día de las elecciones. Se sugiere de manera enfática que este plan e implementación se haga a más tardar una semana antes del evento de las elecciones para dar tiempo a revisarlo, probarlo y ver cómo funcionará.
4. Monitoreo – como parte del proceso de monitoreo vía la herramienta GRAFANA que también se escaneo, se recomienda crear "marcas de agua", valores pre-establecidos en los sistemas de monitoreo, los cuales cuando se presenten permitan tomar decisiones al equipo sobre un potencial mal funcionamiento durante las etapas en ciertas variables cuando se alcancen valores que se evalúen en el comité. Esto dará tiempo a una reacción y planear con anticipación una reacción sobre algún evento que se esté monitoreando ya sea, llenado de disco, lentitud en el procesamiento, intermitencia en algún servicio o plataforma.
5. Plataformas de captura – Se sugirió usar en vez de sistema operativo Windows para las estaciones de captura un sistema tipo quiosco como MOBILOCK, PORTEUS (que es de código fuente abierto), entre otros. Este software al cargarlo crea un ambiente en el cual solo permite cargar el software que el usuario estará operando sin permitir la operación de otro software. En el caso del IEC el capturista solo podría operar la plataforma de captura, sin dar acceso al sistema operativo al usuario y elimina los USB's, haciendo la estación más ágil y más seguro evitando distracciones o facilidad de que el capturista use alguna otra aplicación.
6. Salida a Internet – Durante el ensayo/simulación se pudo apreciar que terminales con acceso a Internet. Se aseguró que durante el evento esto estaría cerrado y no habría acceso a Internet desde las estaciones de trabajo. Esto es de suma importancia por situaciones de seguridad, se vuelve una situación en donde el usuario pueda detonar algún tipo de virus, malware o ransomware que se propague a la red afectando a otras estaciones. Esto en adición a la distracción que puede causar al capturista durante el evento de las elecciones.
7. Equipamiento en riesgo por obsolescencia – El acceso del *VPN Concentrator 3000* mediante el cual se tuvo acceso a la red para hacer escaneos de la red y sus elementos, es un equipo que CISCO retiro de venta desde el 2004 y aunque aún es soportado, conviene considerar hacer una actualización que permita tener un mayor nivel de soporte por parte del fabricante.

(http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/prod_eol_notice09186a00801c599d.html)

8. Vulnerabilidades sin evidencia – Aunque su existencia no está evidenciada en el estudio ni en el análisis (no salieron en ninguna parte del escaneo) por lo que no se corroboro si estaban o no. Estas vulnerabilidades están documentadas como parte de las aplicaciones y servicios que están instalados en los servidores. La recomendación para estas vulnerabilidades, aunque su riesgo de explotación no es alto, es actualizar o instalar los parches en indicados en cada una de las recomendaciones de la vulnerabilidad de la base de datos (NVD) https://nvd.nist.gov