TECNOLÓGICO DE MONTERREY®

Dictámen final sobre
Auditoría de Seguridad Información

Análisis de Riesgos

Descripción breve

Esta sección detalla el modelado de riesgos siguiendo la metodología NIST300-80. El reporte describe de forma cualitativa los impactos de riesgo de las plataformas involucradas.

Jesús R. González / Juan Arturo Nolazco

jrgonza@gmail.com jnolazco@itesm.mx

Índice

1 Resumen Ejecutivo 3
2 Alcances y limitaciones 3
2.1 Limitaciones 3
2.2 Audiencia 4
3 Análisis de riesgo 5
3.1 Caracterización del sistema 5
3.2 Identificación de amenazas 8
3.3 Identificación de vulnerabilidades 9
3.4 Análisis de Vulnerabilidades 12
3.4.1 Vulnerabilidades de Procesos 13
3.4.2 Riesgos Tecnológicos 15
3.5 Determinación de probabilidades 17
3.6 Análisis de impactos 17
3.7 Determinación de riesgos 18
3.8 Riesgos Procesos 20
3.9 Riesgos Tecnológicos 21
3.9.1 Riesgos en servidores 22
4 Trabajos futuros 23
Anexo 1 Claves de vulnerabilidades encontradas 24

Tabla de Ilustraciones

Ilustración 1 Tipo de análisis hecho sobre el IEC 3
Ilustración 2 Arquitectura Sistema - Nivel 1 Centro Acopio Central 5
Ilustración 3 Arquitectura Sistema - Nivel 2 Centro Acopio Remoto (Escaner) 5
Ilustración 4 Arquitectura Sistema - Nivel 3 Centro Acopio Remoto (Celular) 5
Ilustración 5 Arquitectura Sistema - Sitio Central (procesamiento) 5
Ilustración 6 Mapa de Calor 18

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 pretende presentar el análisis de riesgos que se encontró en la infraestructura de TI del IEC la cual será utilizada durante las elecciones del 2017. Este documento presentará las bases y razonamientos para llegar, en la última parte, a presentar una matriz de riesgos calificados con algunas connotaciones de estos.

2 Alcances y limitaciones

En el análisis de riesgos se tomó en cuenta la metodología de NIST basado en el documento especial 800-30 *"Guide for Conducting Risk Assessments"* con la cual se está presentando este documento.

En esta metodología no se está valorando cuantitativamente en términos económicos los impactos, se está valorando de forma cualitativa los impactos en escalas que se presentarán y definirán durante todo el documento.

2.1 Limitaciones

El análisis presentado en este documento se encuentra claramente delimitado por el alcance del nivel 3 que se muestra en la jerarquía mostrada en la figura.

Ilustración 1 Tipo de análisis hecho sobre el IEC

- Nivel 1 – El enfoque principal de este nivel es el desarrollo de una perspectiva organizacional comprensiva para el manejo y administración de riesgos
- Nivel 2 – El enfoque es la arquitectura empresarial la cual se basa en los riesgos del nivel 1
- Nivel 3 – Bajo este nivel el enfoque se basa sobre los riesgos del nivel 1 y 2 y se concentra en encontrar salvaguardas y controles en el nivel de sistemas de información

El nivel 3 se limita a los sistemas informáticos solamente y no incluye la parte de procesos de negocio o nivel estratégico. Esto no limita que alguno de los riesgos que se encuentren tenga implicaciones en los procesos de negocio o bien a nivel estratégico, pero no es el foco del análisis a realizar.

Viendo desde un punto de vista sistémico los elementos que componen todos los componentes informáticos bajo análisis, se considera para propósitos del análisis que los sistemas están en un grado terminal del ciclo de desarrollo de sistemas (SDLC).

2.2 Audiencia

Este documento está hecho recalcando riesgos encontrados en la infraestructura de TI por lo que va dirigido hacia las siguientes audiencias:

- Personal de técnico de administración de infraestructura de TI quienes sobrellevan la operación y gestión de los elementos de red y computo que componen el ambiente operativo de TI.
- 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 Caracterización del sistema

La caracterización de la infraestructura del IEC se pueda dar considerando tres niveles jerárquicos que facilitan la operación del día de las elecciones y el sitio central donde se encuentra la infraestructura de procesamiento:

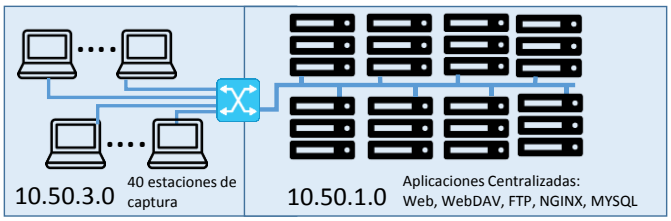

Ilustración 2 Arquitectura Sistema - Nivel 1 Centro Acopio Central

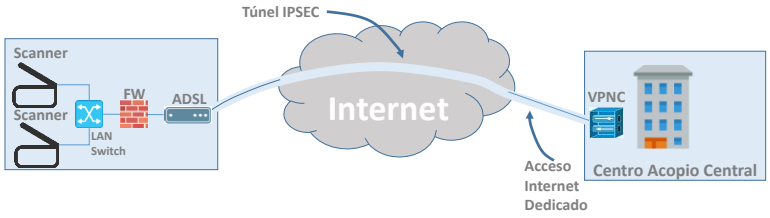

Ilustración 3 Arquitectura Sistema - Nivel 2 Centro Acopio Remoto (Escáner)

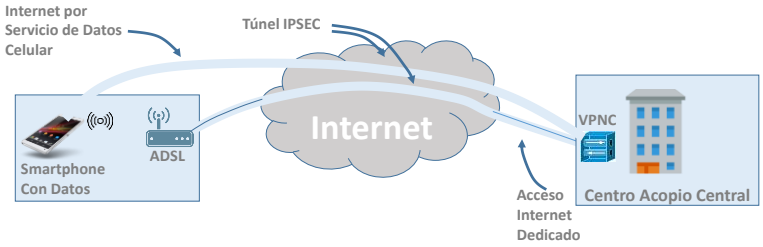

Ilustración 4 Arquitectura Sistema - Nivel 3 Centro Acopio Remoto (Celular)

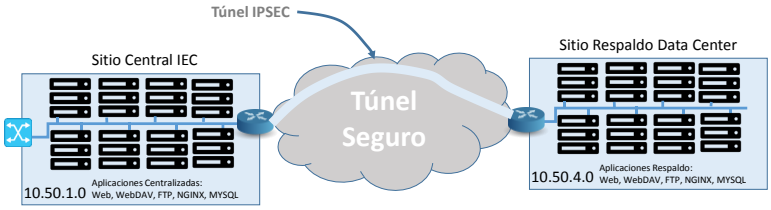

Ilustración 5 Arquitectura Sistema - Sitio Central (procesamiento)

Nivel 1 – Sitio de acopio central donde se reciben todas las actas de todos los centros de acopio para validarse y se capturan en estaciones de trabajo para contabilizar los votos.

Nivel 2 – Sitio de acopio remoto con infraestructura que permite recopilar actas y pasarlas por un escáner que las envía mediante una red conectada por medio de servicios de ADLS hacia el sitio central.

Nivel 3 – Sitio de acopio remoto provisto con un Smartphone para fotografiar el acta y enviarla al sitio central ya sea vía ADSL (si es disponible) o bien por medio de datos del celular (para lo cual cuenta con dos chips de dos compañías.

Sitio Central – Es en donde se encontrarán los distintos servidores y aplicaciones que estarán permitiendo la operación de la jornada electoral en Coahuila.
NOTA: A la fecha del análisis los servidores de respaldo no están en operación.

Esta clasificación de sitios, con variaciones en cuanto a la cantidad de elementos, es muy homogénea en todo el estado. Para descripción de flujos y funcionamiento se tiene lo siguiente:

- El sitio Nivel 2 digitaliza las imágenes de las actas por medio de escáner los cuales se conectan a una red la cual se conecta al sitio central vía un FW estableciendo un túnel de IPSEC el cual es generado por medio de un Firewall.
- El sitio Nivel 1 digitaliza las imágenes de las actas por medio de fotografía de un Smartphone en sitio. Mediante este Smartphone se establece conexión segura vía una VPN IPSEC hacia el sitio central para subir las fotografías.
    - El APP permite aislar cualquier otra imagen para evitar contaminación visual en la foto. LA conexión puede ser por medio de WiFi provisto por servicios de ADSL o bien vía servicios de datos de las compañías celulares.
    - Los smartphones son de doble chip para tener doble servicio de datos en caso que no esté disponible alguno de los servicios.
- Los sitios Nivel 2 y Nivel 3 se conectan Sitio Central el cual recibe vía FTP las transmisiones de las actas contabilizadas al finalizar el proceso electoral. La forma como lo hacen puede ser de dos modos dependiendo del nivel de sitio que sea
- El equipo del sitio Nivel 1 se encarga de contabilizar en los sistemas los votos que hubo en cada casilla y distrito para su presentación y generación de gráficos para distribución.
- La carga del conteo es procesada y se genera un gráfico para empujar a los servidores replicadores que estarán publicando la información del PREP

Los equipamientos incluidos para propósitos de medición de riesgo y vulnerabilidades son los que se muestran en la siguiente tabla:

Sitio Nivel 1	Sitio Nivel 2	Sitio Nivel 3
• 40 computadores • Switch/Router	• Escañeras • Firewall Fortinet • Router ADSL	• Smartphone MotoG4 con servicios de datos de dos carriers • Router ADSL (Si hay disponibilidad)
Los elementos conectados a esta red 10.50.3.0 solo tienen la función de captura en el sitio central y tienen acceso a la red 10.50.1.0 para validar las actas que subieron de los sitios remotos y para actualizar los conteos.	• Los elementos de los Sitios Nivel 2 y Nivel 3 se conectan de forma remota vía túneles de ISPEC al concentrador de VPN's en Internet (IP 189.201.192.30) y se les asigna direcciones de la red Interna 10.50.2.0 para transferir las imágenes de las actas. • La conexión se hace mediante IPSEC desde un Firewall (sitio Nivel 2) con una conexión de ADSL • La conexión se hace mediante IPSEC desde un Smartphone ya sea con servicios de WiFi (si los hay disponibles) o bien usando los servicios de datos de las compañías celulares.	

En el caso del sitio Nivel 1 los computadores para captura del centro de acopio central, no se encuentran disponibles al momento del escaneo. Estos están siendo configurados por lo que la red no se encontró nada que escanear o descubrir. Es debido a esto que no se tiene más información sobre las estaciones de trabajo ni nada de esa red.

Dirección IP	Pto	Aplicación
10.50.1.8	TCP/22 TCP/80 TCP/443	HP Integrated Lights-Out mpSSH 0.2.1 HPE-iLO-Server/1.30 (SSH) ssl/https HPE-iLO-Server/1.30
10.50.1.9	TCP/22 TCP/80 TCP/443	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 HPE-iLO-Server/1.30 ssl/https HPE-iLO-Server/1.30
10.50.1.10	TCP/22 TCP/80	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 Apache httpd 2.4.18
10.50.1.11	TCP/22	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1
10.50.1.100	TCP/80 TCP/22	Apache/2.4.18 (Ubuntu) OpenSSH 7.2p2 Ubuntu 4ubuntu2.1
10.50.1.101	TCP3306	MySQL 5.7.17-0ubuntu0.16.04.2
10.50.1.102	-	-
10.50.1.103	TCP/80	nginx/1.10.0 (Ubuntu)
10.50.1.104	TCP/21	vsftpd 2.0.8 or later
10.50.1.105	-	-
10.50.1.106	TCP/80	Apache httpd 2.4.18 ((Ubuntu))
10.50.1.107	-	-
10.50.1.108	TCP/8086	InfluxDB http admin 1.2.2
10.50.1.109	TCP/3000	Grafana
10.50.1.110	-	-
10.50.1.111	TCP/80	Apache httpd 2.4.18

Los guiones indican que el servidor marco como detectado, pero no indico ningún puerto o servicio en él. Todos los servidores son monitoreados desde la misma red desde una aplicación que permite llevar track tanto de los indicadores operativos (actas cargadas) como también las variables de los elementos de red:

- Carga de servidor (CPU, Memoria, Disco)
- Utilización de ancho de banda
- Monitoreo de aplicaciones (solicitudes por segundo)

Esto permite tener una fotografía así como una tendencia sobre el uso de los elementos que hacen todo el sistema de PREP del IEC.

3.2 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 qué 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.

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

3.3 Identificación de vulnerabilidades

En base a las aplicaciones encontradas y puertos descritos, se buscó las claves de vulnerabilidades para dichas aplicaciones y sus versiones. 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)

IP	Puerto	Aplicación	Id Vulnerabilidad	
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)

La amenaza para explotación de estas vulnerabilidades solo se podría hacer Interna. Dado que la infraestructura no tiene acceso de afuera, más que por túneles, entonces solo sería estando adentro de la red y por personal interno que conozca los sistemas.

Como parte de los escaneos a la red por parte de los sistemas de análisis de vulnerabilidades así como las entrevistas que se hicieron, se pudo tener la siguiente lista de vulnerabilidades en los sistemas. NOTA: Estas vulnerabilidades si consta en la evidencia que se encontraron.

El escáner utilizado OpenVAS, utiliza la base de datos de OSVD. No todas las vulnerabilidades están mapeadas a CVE, pero la descripción del potencial daño que pueden hacer esta descrito junto con el riesgo y probabilidad que tiene de poderse explotar.

10.50.1.100					
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

10.50.1.111					
ID OSVDB	**ID CVE**	**Descripción**	**Probabilidad**	**Impacto**	**Justificación**
OSVDB-3268		Índice directorio está habilitado	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: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	Remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled	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:3288		Abyss 1.03 reveals 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.
OSVDB-3233		Apache default file found	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

3.4 Análisis de Vulnerabilidades

Las vulnerabilidades se agruparon en dos partes para una mejor estructura. Estas son:

- **Procesos** – Los procesos que se operan con los sistemas que lo soportan.
- **Tecnológicos** – Vulnerabilidades que se encuentran embebidas en los sistemas de TI que soportan el proceso electoral del IEC.

OBSERVACION: Para propósitos del escaneo y análisis de los recursos tecnológicos se suavizaron los controles de modo que se pudieran hacer los escaneos y análisis para permitir un mejor conocimiento de la infraestructura. Donde aplique, se hará el comentario respecto a lo que se reforzaría crearía durante el proceso de elecciones en la sección de recomendaciones.

3.4.1 Vulnerabilidades de Procesos

Los procesos se estructuraron en tres partes y de ese modo se definieron las vulnerabilidades asociadas a estos. Conforme a eso se tiene la siguiente tabla que describe el control en su clasificación así como su análisis y/o comentario.

Captura				
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Justificación**
• 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	• PROBABILIDAD MB - por ser instalación con seguridad controlada por gobierno • IMPACTO A - Por acceso a información que no debe tener nadie hasta el PREP
	• No se valida la entrada de personal	Muy Baja	Alto	
• 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	• PROBABILIDAD B –por involucrar varias personas y lo simple de operar las apps • IMPACTO M – Por el tiempo que puede retrasar al no tener capacitación/práctica
	• Solo hay una persona que lo sabe operar	Baja	Medio	
• Acceso a la sala de captura con equipo ajeno a esta	• No tener registro de pertenencias	Media	Alto	• PROBABILIDAD M – Media por lo que estudiantes y practicantes pueden traer como dispositivos personales • IMPACTO M – Por lo que puede hacer alguien con un celular o cámara; aparte de ser distracción a un proceso.
	• No tener punto de control de entrada en el sitio de captura	Bajo	Alto	• PROBABILIDAD MB - por ser instalación con seguridad controlada por gobierno • IMPACTO A - Por acceso a información que no debe tener nadie hasta el PREP
• Brazo dañado para tomar fotografías con el teléfono	• No ha hay manuales que describan los procesos en sitio de operación	Bajo	Bajo	• PROBABILIDAD B – El brazo para fotos, se ve de material resistente • IMPACTO B – El APP para fotos, permite centrar el acta sin mayor esfuerzo
• Falta de conectividad	• Falla en los proveedores de Internet para conectar al sitio central	Bajo	Medio	• PROBABILIDAD B – Por la cobertura existente y tener dos planes de datos • IMPACTO M – Causa retraso en el PREP
• Mal uso de los teléfonos para captura	• Smartphone de captura controlado	Bajo	Alto	• PROBABILIDAD B – Smartphone es del IEC y se lleva la política de uso por el • IMPACTO A – Elemento de captura inhabilitado para día de elecciones
	• Aplicación de captura Teléfono	Bajo	Alto	• PROBABILIDAD B – IEC controla las aplicaciones instaladas en el Smartphone • IMPACTO A – Elemento de captura inhabilitado para día de elecciones
• Captura de datos no relacionados en la aplicación de captura central	• Validación de caracteres en la captura	Muy Bajo	Medio	• PROBABILIDAD B – IEC controla la aplicación y validaciones. • IMPACTO M – Posible lentitud en el proceso por consulta de captura

[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**	**Justificación**
• 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	• PROBABILIDAD M – Dado los contratos con SLAs es poco probable no tener respuesta del centro de datos externo • IMPACTO A – Retrasaría todo el PREP
	• Falla de servicio en la nube	Medio	Alto	
• Falla comunicaciones en el centro de acopio central	• Enlaces de sitios de centros de acopio remotos.	Bajo	Medio	• PROBABILIDAD M – Improbable por contar con dos planes de datos y/o acceso telefónico para captura por voz • IMPACTO M – Causa retraso en el PREP
	• Enlace de comunicación del centro acopio central	Bajo	Medio	• PROBABILIDAD M – Improbable por contar con dos enlaces a Internet y acceso a telefonía en dado caso • IMPACTO M - Causa retraso en el PREP
• Caída de los sistemas local	• Por alguna razón los sistemas de captura fallan	Medio	Alto	• PROBABILIDAD M – Los sistemas se han probado meses antes de las elecciones en varios escenarios aparte de tener redundancia local de dichos sistemas • IMPACTO A – Retrasaría todo el PREP
	• Caída eléctrica	Medio	Alto	• PROBABILIDAD M – El centro tiene planta auxiliar, aparte el flujo eléctrico en saltillo es muy estable • IMPACTO A – Retrasaría todo el PREP
	• Falla HW	Bajo	Alto	• PROBABILIDAD M – Los servidores tienen definidos tiempos muy altos de disponibilidad por lo que se ve poco probable aparte de estar en sitio adecuado para su operación. • IMPACTO A – Retrasaría todo el PREP
	• Falla de Disco por llenado	Bajo	Medio	• PROBABILIDAD M – El dimensionamiento esta sobrado (1MxArchivo) en un disco de 300G x 11,000 actas (11G a 20G). Con un uso razonable, no hay manera que se llene. Tendría que ser alguien interno que llene con intención de hacer daño • IMPACTO M – Se puede proceder a limpiar el disco y liberar espacio.
• Incidente que bloque capacidad operativa (procesamiento y captura) de actas de forma local	• Plan de contingencia	Media	Alto	• PROBABILIDAD M – Necesario contar con un plan establecido por escrito a seguir en caso de algún incidente. • IMPACTO A – No tener conocimiento de a quién recurrir en caso de evento durante las elecciones.
	• Matriz de responsables x aplicación	Media	Alto	
	• Monitoreo de la infraestructura	Medio	Medio	• PROBABILIDAD M – No detiene la operación pero no permitirá reaccionar a tiempo para tomar medidas alternas • IMPACTO M – No habría impacto en el momento, pero de no detectarse, podría ser impacto muy alto

3.4.2 Riesgos Tecnológicos

Los controles tecnológicos están configurados en la infraestructura del IEC y estos son los que nos hemos encontrado en los escaneos así como en las entrevistas ya que algunos de ellos se implementarán posteriormente al proceso de auditoría.

Se determinó solo revisar las amenazas sobre vulnerabilidades de las que se tiene evidencia ya sea en el escaneo realizado o bien mediante entrevistas que se hayan obtenido información.

Captura				
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Justificación**
• Uso inadecuado del Smartphone en sitios de acopio remotos	• Usuario controla smartphone	Bajo	Medio	• PROBABILIDAD B – Smartphone es del IEC y se lleva la política de uso por el • IMPACTO A – Elemento de captura inhabilitado para día de elecciones
	• Usuario pueda estar llamando	Medio	Medio	
• Problemas de transferencia de imágenes al sitio central de acopio	• Enlaces de sitios de centros de acopio remotos.	Bajo	Medio	• PROBABILIDAD M – Improbable por contar con dos planes de datos y/o acceso telefónico para captura por voz • IMPACTO M – Causa retraso en el PREP
	• Enlace de comunicación del centro acopio central	Bajo	Medio	• PROBABILIDAD M – Improbable por contar con dos enlaces a Internet y acceso a telefonía en dado caso • IMPACTO M - Causa retraso en el PREP
	• Imagen sale defectuosa	Bajo	Medio	• PROBABILIDAD B – El teléfono es de última generación, • IMPACTO M – La imagen puede retransmitirse siendo de bajo impacto
	• Servidor FTP para recibir imágenes	Bajo	Medio	• PROBABILIDAD B – Poco probable que se quede sin la totalidad de servidores • IMPACTO M - Causa retraso en el PREP,
	• Escáner para digitalización	Bajo	Medio	• PROBABILIDAD B – hay varios escáner, poco probable quedarse sin todos • IMPACTO M - Causa retraso en el PREP
	• Estación de captura	Medio	Medio	• PROBABILIDAD M – La PC puede tener problemas pero son más de 50 en el centro de acopio. • IMPACTO M - Causa retraso en el PREP
	• Duplicación de Imágenes	Bajo	Medio	• PROBABILIDAD B – Se toma una foto y se sube en automático al Server. Si esto se diera, al capturarse, solo se validaría resultados de la captura previa. • IMPACTO M – Solo añadiría trabajo adicional y retraso en dado caso, que está considerado.
• Error de Captura	• Error humano al capturar números o cantidades de las actas	Medio	Medio	• PROBABILIDAD M – El error humano puede darse en cualquier parte del proceso electoral • IMPACTO M – Solo añadiría trabajo adicional y retraso en dado caso, que está considerado
• Error reporte de avance	• Configuración del sistema de monitoreo GRAFANA	Bajo	Medio	• PROBABILIDAD M – La tecnología es bastante robusta y los ensayos dejarán perfeccionar la configuración • IMPACTO M – Afecta la medición, pero no el proceso en sí de captura
• Acceso a terminal de captura por personal no autorizado	• Login de acceso a las terminales de captura	Media	Alta	• PROBABILIDAD M – El área es de acceso restringido • IMPACTO A – Afecta porque cualquiera pueda tener capacidad de capturar

Operación				
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Justificación**
• Uso inadecuado de estaciones en el centro de acopio central	• Acceso al sistema operativo	Medio	Alto	• PROBABILIDAD M – Capturistas podrán acceder a programas y/o aplicaciones del sistema operativo • IMPACTO A – Elemento de mal uso y distracción durante elecciones.
	• Acceso a Internet	Medio	Medio	
• Entrada de caracteres ilegales en la plataforma de captura	• Aplicación de captura	Medio	Alto	• PROBABILIDAD M – Sistema validaría la entrada del capturista • IMPACTO A – Poder meter instrucciones al sistema vía caracteres especiales
• Ataques a la BD MYSQL ○ OSVDB-3233, OSVDB-35878, PSVDB-3092	• Acceso a la Base de datos	Bajo	Alto	• PROBABILIDAD B – Solo hay acceso directo con usuario/clave y desde la red interna, solo alguien especializado podría entrar directo a la BD • IMPACTO A – Podría alterar, borrar o dar de baja la BD que afectaría el proceso completo.
	• Cortar la operación desde la aplicación de captura para ver datos del servidor	Bajo	Alto	
• Ataque al servidor ○ OSBDV-3288, PSVDB-3233, OSBDV-119, OSVDB576	• Cortar la operación desde la aplicación de captura para ver datos del servidor	Bajo	Alto	• PROBABILIDAD B – Solo hay acceso directo con usuario/clave y desde la red interna, solo alguien especializado podría entrar directo a la BD • IMPACTO A – Podría alterar, borrar o dar de baja la BD que afectaría el proceso completo
• Falla de servidor (WebDav, Apache, MySQL)	• Caída sistema operativo	Bajo	Muy Alto	• PROBABILIDAD B – La estabilidad de los sistemas operativos y plataforma de HW hacen poco probable que esto suceda • IMPACTO A – Detendría la captura de resultados así como recopilación de imágenes de los centros de acopio
• Entrar vía el túnel de IPSEC a la red de servidores del IEC	• Permitir una configuración Split-túnel en la conexión al servicio de VPN	Medio	Alto	• PROBABILIDAD M – Al conectar la VPN se permite que se navegue por internet y se conecte a la aplicación. Esto puede traer problemas potenciales • IMPACTO A – Si se llega a encontrar como entrar, deberá haber un conocimiento para poder explotar servicios adentro de la red.
• Falla eléctrica	• Redundancia eléctrica	Medio	Alto	• PROBABILIDAD M – La electricidad siempre está sujeta a falla y es externa • IMPACTO A – Se podrían caer todos los sistemas de no haber electricidad el día de las elecciones.
• Que alguien externo pueda entrar a modificar servidores o programas	• Acceso túnel de IPSEC conectado a Internet	Bajo	Medio	• PROBABILIDAD B – Existe la posibilidad que alguien entre, pero debe conocer bien los esquemas del sistema para poder hacer algo con ellos. • IMPACTO A – Potencialmente puede ver todo y modificarlo, si puede entrar
• Quedarse sin infraestructura	• No completar cantidad de equipos para captura	Medio	Muy Alto	• PROBABILIDAD M – Se constató ya la instalación de ¾ partes de lo necesario • IMPACTO A – Podría duplicar el tiempo de captura del proceso
	• Falta de tiempo para instalación	Bajo	Muy Alto	• PROBABILIDAD M – Se constató ya la operación de ¾ partes de lo necesario • IMPACTO A – Podría duplicar el tiempo de captura del proceso

3.5 Determinación de probabilidades

Para derivar la probabilidad de que un evento ocurra, se determinó utilizar la medida genérica de Muy Alto, Alto, Medio, Bajo y Muy Bajo sobre las cuales se tiene una definición de acuerdo a lo siguiente:

Probabilidad	Definición
Muy Alto	La fuente de amenazas está muy motivada y es más que capaz para ejecutar y los controles no podrán prevenir la explotación de vulnerabilidad
Alta	La fuente de amenaza es suficientemente motivada y capaz para ejecutar y los controles para prevenir la explotación de vulnerabilidad son ineficientes
Media	La fuente de amenaza es suficientemente motivada y capaz para ejecutar pero hay controles que previenen explotación de vulnerabilidades haciéndola difícil
Baja	La fuente de amenaza carece de motivación y capacidad para ejecutar o hay controles que previenen o impiden que haya explotación de vulnerabilidades
Muy Bajo	La fuente de amenazas no tiene motivación ni capacidades o hay controles que impiden y/o desincentivan la explotación de vulnerabilidades

Estas probabilidades se determinaron basado en los siguientes factores:

- Fuente de la amenaza, su motivación y capacidades para ejecutar acciones que tengan impacto sobre la infraestructura en análisis.
- Naturaleza de las vulnerabilidades encontradas en los activos analizados
- Existencia de controles que puedan minimizar la explotación de vulnerabilidades

3.6 Análisis de impactos

El análisis de impactos resulta de una exitosa ejecución de una vulnerabilidad y del análisis cuidadoso de la información del cliente respecto a los sistemas y la infraestructura usando:

- Misión del sistema
- Criticidad del sistema y los datos
- Sensitividad de los datos y del sistema

El impacto de un evento de seguridad se puede describir en términos de pérdida o degradado uno o combinación de varios de los objetivos de seguridad:

- **Pérdida de integridad** – son los requerimientos de que la información sea protegida de modificación no autorizada ya sea de forma intencional o accidental.
- **Perdida de disponibilidad** – se refiere a la pérdida del uso de la aplicación o del sistema la cual afecta la misión y objetivos de la organización dada su indisponibilidad.
- **Pérdida de confidencialidad** - Se refiere a la protección de la información respecto a su publicación no autorizada

La definición de magnitud de impacto se tiene en la tabla de definiciones y se optó por 4 clasificaciones de impacto.

Impacto	Definición
Muy alto	Ejecutar una vulnerabilidad resulta en (1) en pérdida de activos o recursos de la organización (2) afectación muy severa de la capacidad operativa de la organización (3) resultar en pérdidas humanas o afectación de personas.
Alto	Ejecutar una vulnerabilidad puede resultar en (1) perdida costosa de activos o recursos de la organización, (2) afectar severamente la capacidad operativa de la organización (3) resultar en pérdidas humanas o afectación de personas
Medio	Ejecutar una vulnerabilidad puede resultar en (1) perdida de activos o recursos de la organización, (2) afectar severamente la capacidad operativa de la organización (3) resultar afectación de personas
Bajo	Ejecutar una vulnerabilidad puede resultar en (1) perdida de algunos activos o recursos de la organización, (2) potencialmente afectar la capacidad operativa de la organización
Muy Bajo	Ejecutar una vulnerabilidad puede resultar en (1)disminución en la capacidad de desempeño de activos (2) potencialmente disminuirá la capacidad operativa de la organización

3.7 Determinación de riesgos

La determinación del riesgo se hizo en base a la definición multiplicando la probabilidad que hay de que suceda la explotación de vulnerabilidad con el impacto que la vulnerabilidad tiene de lograr su explotación.

La determinación de riesgos se hizo sobre la base del escenario final que habrá en el ambiente de red y operación. Esto ya que para el propósito de auditoría y escaneo de redes y plataformas, se abrió el acceso para poder realizar este estudio, pero en el momento de inicio, estará filtrado con reglas en el FW y en el concentrador para limitar el flujo de información de los que se conecten para cargar fotografías de las actas.

Impacto	Riesgo				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Mul Alto	Medio	Alto	Alto	Muy Alto	Muy Alto
Alto	Bajo	Medio	Alto	Alto	Muy Alto
Medio	Bajo	Medio	Medio	Alto	Alto
Bajo	Muy Bajo	Bajo	Medio	Medio	Alto
Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo	Medio

Ilustración 6 Mapa de Calor

El resultado se basa en multiplicar el Riesgo por el impacto y el mapa de calor que se muestra, determina la calificación de riesgo (resultado en las celdas) del resultado de relacionar el impacto con el riesgo.

En base a esto se tiene las siguientes tablas que determinan los riesgos basados en la clasificación del proceso y tecnológico que se tiene:

- Captura – Esto comprende todo el proceso de captura una vez que acaba la elección
- Operación – Esto es toda la labor que se hace durante el proceso de consolidación y validación en el centro de acopio central.

3.8 Riesgos Procesos

En base a la probabilidad de ocurrencia y el impacto de la vulnerabilidad explotada, se determina el riesgo en base al cuadro de la sección 3.7 de determinación de riesgos.

Captura				
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo**
• 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
	• No se valida la entrada de personal	Muy Baja	Alto	Medio
• Ausencia de personal el día del proceso electoral a los centros de acopio o de procesamiento[2]	• No ha hay manuales que describan los procesos en sitio de operación	Baja	Medio	Medio
	• Solo hay una persona que lo sabe operar	Baja	Medio	
• Acceso a la sala de captura con equipo ajeno a esta	• No tener registro de pertenencias	Media	Alto	Alto
	• No tener punto de control de entrada en el sitio de captura	Bajo	Alto	Medio
• Brazo dañado para tomar fotografías con el teléfono	• No ha hay manuales que describan los procesos en sitio de operación	Bajo	Bajo	Bajo
• Falta de conectividad	• Falla en los proveedores de Internet para conectar al sitio central	Bajo	Medio	Medio
• Mal uso de los teléfonos para captura	• Smartphone de captura controlado	Bajo	Alto	Medio
	• Aplicación de captura Teléfono	Bajo	Alto	Medio
• Captura de datos no relacionados en la aplicación de captura central	• Validación de caracteres en la captura	Muy Bajo	Medio	Bajo

Operación Central				
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo**
• 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
	• Falla de servicio en la nube	Medio	Alto	
• Falla comunicaciones en el centro de acopio central	• Enlaces de sitios de centros de acopio remotos.	Bajo	Medio	Medio
	• Enlace de comunicación del centro acopio central	Bajo	Medio	Medio
• Caída de los sistemas local	• Por alguna razón los sistemas de captura fallan	Medio	Alto	Alto
	• Caída eléctrica	Medio	Alto	Alto
	• Falla HW	Bajo	Alto	Alto
	• Falla de Disco por llenado	Bajo	Medio	Medio
• Incidente que bloque capacidad operativa (procesamiento y captura) de actas de forma local	• Plan de contingencia	Media	Alto	Alto
	• Matriz de responsables x aplicación	Media	Alto	
	• Monitoreo de la infraestructura	Medio	Medio	Medio

[2] 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.

3.9 Riesgos Tecnológicos

Captura				
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo**
• Uso inadecuado del Smartphone en sitios de acopio remotos	• Usuario controla smartphone	**Bajo**	**Medio**	**Medio**
	• Usuario pueda estar llamando	**Medio**	**Medio**	**Medio**
• Problemas de transferencia de imágenes al sitio central de acopio	• Enlaces de sitios de centros de acopio remotos.	**Bajo**	**Medio**	**Medio**
	• Enlace de comunicación del centro acopio central	**Bajo**	**Medio**	**Medio**
	• Imagen sale defectuosa	**Bajo**	**Medio**	**Medio**
	• Servidor FTP para recibir imágenes	**Bajo**	**Medio**	**Medio**
	• Escáner para digitalización	**Bajo**	**Medio**	**Medio**
	• Estación de captura	**Medio**	**Medio**	**Medio**
	• Duplicación de Imágenes	**Bajo**	**Medio**	**Medio**
• Error de Captura	• Error humano al capturar números o cantidades de las actas	**Medio**	**Medio**	**Medio**
• Error reporte de avance	• Configuración del sistema de monitoreo GRAFANA	**Bajo**	**Medio**	**Medio**
• Acceso a terminal de captura por personal no autorizado	• Login de acceso a las terminales de captura	Media	**Alto**	**Alto**

Operación				
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo**
• Uso inadecuado de estaciones en el centro de acopio central	• Acceso al sistema operativo	**Medio**	**Alto**	**Alto**
	• Acceso a Internet	**Medio**	**Medio**	**Medio**
• Entrada de caracteres ilegales en la plataforma de captura	• Aplicación de captura	**Medio**	**Alto**	**Alto**
• Ataques a la BD MYSQL ○ OSVDB-3233, OSVDB-35878, PSVDB-3092	• Acceso a la Base de datos	**Bajo**	**Alto**	**Medio**
	• Cortar la operación desde la aplicación de captura para ver datos del servidor	**Bajo**	**Alto**	
• Ataque al servidor ○ OSBDV-3288, PSVDB-3233, OSBDV-119, OSVDB576	• Cortar la operación desde la aplicación de captura para ver datos del servidor	**Bajo**	**Alto**	**Alto**
• Falla de servidor (WebDav, Apache, MySQL)	• Caída sistema operativo	**Bajo**	**Muy Alto**	**Alto**
• 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**
• Falla eléctrica	• Redundancia eléctrica	**Medio**	**Alto**	**Alto**
• Que alguien externo pueda entrar a modificar servidores o programas	• Acceso túnel de IPSEC conectado a Internet	**Bajo**	**Medio**	**Medio**
• Quedarse sin infraestructura	• No completar cantidad de equipos para captura	**Medio**	**Muy Alto**	**Alto**
	• Falta de tiempo para instalación	**Bajo**	**Muy Alto**	**Alto**

3.9.1 Riesgos en servidores

En esta sección se describe el índice de riesgo para las vulnerabilidades encontradas en el escaneo de los distintos servidores que se encuentran en el área de operación.

10.50.1.100					
ID OSVDB	ID CVE	Descripción	Probabilidad	Impacto	Riesgo
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	Medio
OSVDB:119	CVE-1999-0269	Servidor remote puede permitir listado de directores vía web, forzando a mostrar los archivos al solicitarlo en el browser.	Medio	Medio	Medio
OSVDB:3092		/webdav/index.html: WebDAV esta habilitado.	Bajo	Bajo	Bajo
OSVDB:3288		directory listing when /'s are requested	Bajo	Medio	Medio

10.50.1.103					
ID OSVDB	ID CVE	Descripción	Probabilidad	Impacto	Riesgo
OSVDB:3092		/webdav/index.html: WebDAV esta habilitado.	Bajo	Bajo	Bajo

10.50.1.106					
ID OSVDB	ID CVE	Descripción	Probabilidad	Impacto	Riesgo
OSVDB-3233		/jsp-examples/: Apache Java Server Pages documentation	Bajo	Bajo	Bajo

10.50.1.109					
ID OSVDB	ID CVE	Descripción	Probabilidad	Impacto	Riesgo
OSVDB-35878		Modulo PHP-Nuke permite Usuarios ver usernames y claves	Bajo	Bajo	Bajo
OSVDB-3092		/webdav/index.html: WebDAV esta habilitado.	Bajo	Bajo	Bajo

10.50.1.111					
ID OSVDB	ID CVE	Descripción	Probabilidad	Impacto	Riesgo
OSVDB-3268		Ïndice directorio esta habilitado	Bajo	Bajo	Bajo
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	Medio
OSVDB:119	CVE-1999-0269	Remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled	Medio	Medio	Medio
OSVDB:3288		Abyss 1.03 reveals directory listing when /'s are requested	Bajo	Medio	Medio
OSVDB-3233		Apache default file found	Bajo	Bajo	Bajo

4 Trabajos futuros

Como parte de las recomendaciones, el análisis de riesgo efectuado, es una fotografía en el timpo de la situación, elementos y variables externas que interactúan con todos estos componentes. Es recomendable llevar este análisis aun esquema recurrente como práctica para minimizar riesgos no solo en el área de tecnología sino que a nivel procesos y organización.

El esquema recomendable para llevarlo como parte de la evolución de toda la plataforma y del sistema sería bajo un marco de referencia de riesgos basado en NIST 800-37 el cual se enfoca al nivel 3 (infraestructura de TI) y permite integrarlo a un esquema de ciclo de vida del desarrollo del sistema llevando aplicaciones hacia los niveles superiores de la jerarquía de riesgo.

Anexo 1 Claves de vulnerabilidades encontradas

Lista de vulnerabilidades NVDB. No hay evidencia de su presencia en los escaneos

Tabla de Vulnerabilidades y descripción		
Id Vulnerabilidad	**Descripción**	**Fecha de Alta**
CVE-2016-4979	The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVerifyClient require" directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation	06/Jul/2016
CVE-2016-4375	Multiple unspecified vulnerabilities in HPE Integrated Lights-Out 3 (aka iLO 3) firmware before 1.88, Integrated Lights-Out 4 (aka iLO 4) firmware before 2.44, and Integrated Lights-Out 4 (aka iLO 4) mRCA firmware before 2.32 allow remote attackers to obtain sensitive information, modify data, or cause a denial of service via unknown vectors	08/Sep/2016
CVE-2015-5435	Unspecified vulnerability in HP Integrated Lights-Out (iLO) firmware 3 before 1.85 and 4 before 2.22 allows remote authenticated users to cause a denial of service via unknown vectors.	29/sep/2015
CVE-2015-8325	The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.	30/Abr/2016
CVE-2016-3115	Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions.	22/Mar/2016
CVE-2016-1546	The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.	06/Jul/2016
CVE-2012-1180	Use-after-free vulnerability in nginx before 1.0.14 and 1.1.x before 1.1.17 allows remote HTTP servers to obtain sensitive information from process memory via a crafted backend response, in conjunction with a client request.	17/Abr/2015
CVE-2017-3600	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. Note: CVE-2017-3600 is equivalent to CVE-2016-5483. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	24/Abr/2017
CVE-2017-3599	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). NOTE: the previous information is from the April 2017 CPU. Oracle has not commented on third-party claims that this issue is an integer overflow in sql/auth/sql_authentication.cc which allows remote attackers to cause a denial of service via a crafted authentication packet	24/Abr/2017
CVE-2017-3455	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	24/Abr/2017
CVE-2017-3454	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).Abr/24/201	24/Abr/2017
CVE-2017-3453	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	24/Abr/2017

Tabla de Vulnerabilidades y descripción		
Id Vulnerabilidad	**Descripción**	**Fecha de Alta**
CVE-2017-3450	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	24/Abr/2017
CVE-2017-3331	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	24/Abr/2017
CVE-2017-3329	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Thread Pooling). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	24/Abr/2017
CVE-2017-3309	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	24/Abr/2017
CVE-2017-3308	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	24/Abr/2017

La siguiente e una lista de las vulnerabilidades encontradas en el proceso de escaneo y que están basadas en la OSVDB. Estas si se les aplico el análisis de riesgo basado en la posibilidad de explotación y afectación potencial que pudiese tener.

Clave	Definición
OSVDB:576	Requerir un drectorio con %00/, %2e/, %2f/ or %5c/ al final causa que el servidor muestre contenidos del directorio.
OSVDB:119	remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled
OSVDB:3092	**/webdav/index.html: WebDAV support is enabled.**
OSVDB:3288	directory listing when /'s are requested
OSVDB-3233	/jsp-examples/: Apache Java Server Pages documentation
OSVDB-35878	PHP-Nuke module allows user names and passwords to be viewed
OSVDB-3268	Directory indexing is enabled