AUDITORÍA DE SOFTWARE DEL PREP PARA LAS ELECCIONES 2018 EN EL ESTADO DE CAMPECHE

SEGUNDO REPORTE DE AUDITORÍA A LOS SISTEMAS INFORMÁTICOS PREP Y PREP CASILLA

Programa de Resultados Electorales 2018

IEEC- ITESCAM- PROISI

RESPONSABLE: DR. JOSE LUIS LIRA TURRIZA
DRA. YAQUELINE PECH HUH
DR. JOSE MANUEL LIRA TURRIZA
ING. CARLOS URUÑUELA VASALLO

27 DE ABRIL DE 2018

Tabla de contenido

1. GLOSARIO

Centro de Captura y Verificación (CCV):

Lugar donde se realizan las actividades de captura y verificación de los datos e imágenes de las Actas PREP.

Centro de Acopio y Transmisión de Datos (CATD):

Lugar donde se reciben físicamente y se digitalizan las Actas PREP.

Los Organismos Públicos Locales (OPL):

Son los encargados de la organización de las elecciones en su entidad federativa para la designación de: Gobernadores, Diputados locales, Presidentes municipales, Integrantes de ayuntamientos, Jefes delegacionales, Jefe de gobierno, Entre otros.

2. ANTECEDENTES

En el proceso electoral estatal Ordinario 2018, en cumplimiento a la normatividad se contrató a quien lleve a cabo el Programa de Resultados Electorales Preliminares (PREP), que está sujeto a los Lineamientos del Programa de Resultados Electorales Preliminares, emitidos por Consejo General del Instituto Nacional Electoral. En el diseño, instalación e implementación del PREP se deberá de cumplir con los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad, en el ejercicio de la función electoral. De acuerdo a lo que establecen los Lineamientos, la auditoría de verificación y análisis del sistema informático que será utilizado en la implementación y operación del PREP, se deberá realizar con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente. Así mismo se deberán incorporar en el desarrollo de su sistema informático, la función requerida para la generación y el almacenamiento de bitácoras que faciliten los procedimientos de verificación, análisis y auditoría del sistema.

De acuerdo con los lineamientos vigentes del instituto nacional electoral (INE) donde se establece los Requisitos Mínimos para la elaboración del anexo técnico para la contratación de servicios de auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares, se señala que se deben considerar al menos las siguientes líneas de trabajo:

- Pruebas Funcionales de Caja Negra y Revisión de código fuente
- Validación del sistema informático del PREP y de sus bases de datos
- Análisis de Vulnerabilidades a la Infraestructura tecnológica
- Pruebas de Denegación del servicio al sitio web del PREP y al sitio principal del IEEC.

Es por ello que, en Marzo de 2018, el Instituto Electoral del Estado de Campeche (IEEC) y el Instituto Tecnológico Superior de Calkiní en el Estado de Campeche (ITESCAM) suscribieron un convenio específico de colaboración con el objetivo de realizar la Auditoría de software al Sistema del Programa de

Resultados Electorales Preliminares (PREP y PREP CASILLA) que se utilizarán para las elecciones en el Estado de Campeche de la cual se desprende este informe.

Para la realización de esta auditoría, participó por parte del IEEC el personal técnico de la empresa Grupo PROISI S.A de C.V, por parte del ITESCAM, personal de la Dirección Académica de las Carreras de Ingeniería Informática y Sistemas Computacionales al que denominaremos Equipo Auditor.

La revisión debe realizarse desde el punto de vista de la calidad, consistente del grado en el que el software satisface una serie de requisitos de operación preestablecidos, los estándares de desarrollo especificados con anterioridad y las características inherentes a todo producto de software desarrollado de manera profesional[1], ante las expectativas del cliente en una solución, la auditoría debe validar que ésta cumpla con las especificaciones definidas generando certeza en los datos publicados. Para la ejecución de la auditoría es indispensable utilizar un conjunto de estándares, técnicas, métodos y tecnologías de la información que permitan lograr que los sistemas sean correctamente auditados.

Existen 3 estándares formulados por la IEEE que apoyan a la ejecución del proceso de auditoría:

El estándar para la revisión y auditoría de software IEEE 1028TM 2008 en el que se define cinco tipos de revisiones y auditorías de software, junto con los procedimientos necesarios para la ejecución de cada tipo. Los tipos de revisión incluyen revisiones de gestión, revisiones técnicas, inspecciones, y walk-throughs. Es aplicada en cualquier modelo de ciclo de vida del software seleccionado y proporciona un estándar contra el cual se pueden preparar y evaluar los planes de revisión y auditoría de software.

El estándar de clasificación de anomalías de software IEEE1044-2009 1.1 proporciona el conjunto básico de atributos para la clasificación de fallas y defectos. Este estándar es aplicable a cualquier software (incluidos sistemas operativos, sistemas de administración de bases de datos, aplicaciones, software de prueba, firmware y software integrado) y a cualquier fase del proyecto, producto o ciclo de vida del sistema[4].

El estándar para desarrollar un proyecto de software en el proceso de ciclo de vida IEEE 1074 en el que se explica como el aseguramiento de calidad del software debe apoyarse o relacionarse estrechamente con las siguientes actividades [2]:

- Verificación: Básicamente revisiones y auditorías de configuración y calidad.
- Validación: Todos los niveles y fases de prueba de ejecución de software.
- Gestión de Configuración: Como medio de control de los productos generados.
- Medición de software: Contempla la necesidad de marcar objetivos y asociar métricas a los objetivos.

En estas actividades se resalta la verificación o auditoría del software y la medición a través de objetivos. Esta auditoría debe ser planificada y llevada por las personas asignadas para tal fin, no puede olvidarse ningún detalle y siempre se deben tener en mente los siguientes objetivos:

- Encontrar tempranamente los defectos.
- Prevenir el mal funcionamiento.
- Proporcionar mejoras.

3. OBJETIVOS DE LA AUDITORÍA

El objetivo general de la auditoría es revisar el proceso de aplicación de los sistemas informáticos de apoyo para la jornada electoral del Instituto Electoral del estado de Campeche y generar un informe imparcial que sirva para la mejora de dicho proceso.

OBJETIVOS ESPECÍFICOS

1. Revisar el cumplimiento de los lineamientos del Programa de Resultados Electorales Preliminares.

2. Evaluar la integridad y exactitud, del sistema informático del PREP en el procesamiento de información, generación y presentación de resultados.

3. Analizar la vulnerabilidad en la infraestructura tecnológica del PREP.

4. Elaborar un informe con los resultados de la auditoría

5. Elaborar recomendaciones relativas a las vulnerabilidades y riesgos detectados en la Auditoría

4. METODOLOGÍA DE LA AUDITORÍA

A) Modelo

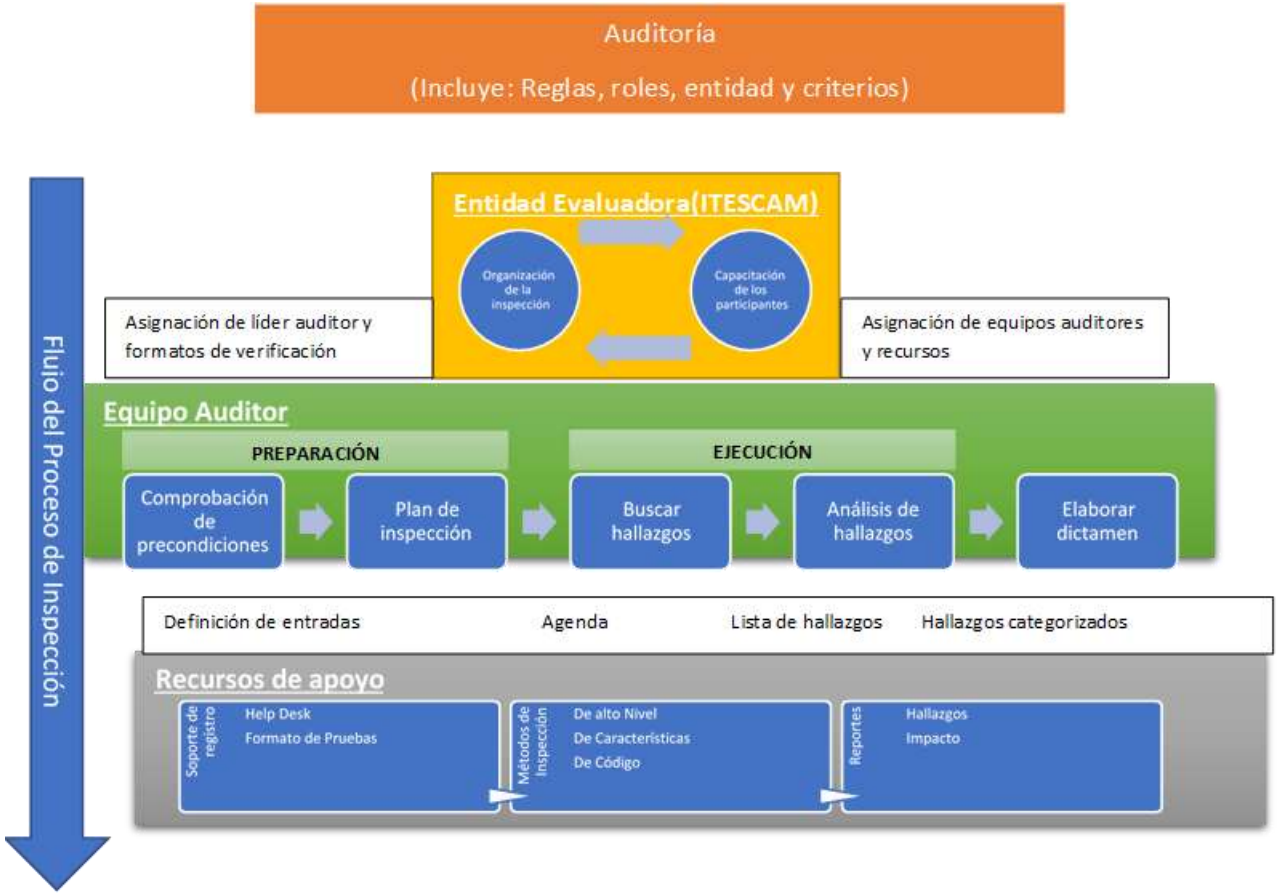

Figura 1. Modelo de flujo de actividades de auditoría

Para llevar a cabo el proceso de auditoría se ha planteado un modelo del proceso que engloba a los responsables y actividades que se llevarán a cabo durante el desarrollo de ésta. A continuación, se describe el modelo presentado en la Figura 1. La Entidad Evaluadora es la encargada de organizar la auditoría, determinar los roles de los participantes, y monitorear el cumplimento de los planes. Antes de iniciar se definen los formatos de acuerdo con los métodos de inspección que se utilizarán. Por último, se definen los equipos auditores considerando los roles y se capacitan para llevar a cabo las actividades.
Es responsabilidad del equipo auditor llevar a cabo las actividades de la auditoría y a través del auditor líder planear una agenda, darle seguimiento y generar un dictamen con los hallazgos encontrados y clasificados de acuerdo con su impacto.

Para la realización de la auditoría el modelo propone el uso de un conjunto de Recursos de Apoyo a través de aplicaciones de Help Desk para la comunicación de los hallazgos con el cliente y un Plan de pruebas para el proceso auditado, la definición de los métodos de inspección y un grupo de reportes que permitan monitorear los hallazgos durante y al final del proceso. Como se mencionó antes, el equipo auditor es el

responsable de llevar a cabo las actividades propias de la auditoría, es por ello que se considera importante describir dichas actividades y para lo que se planteó un modelo a bloques que se detalla en la Figura 2. Ahí se pueden observar las tres fases que componen el proceso de auditoría: Preparación, ejecución y dictamen.

Durante la preparación es necesario tener un primer contacto con el ente a auditar para ello se agenda una visita preliminar cuyo propósito es el de conocer de manera general los aspectos del sistema que se va a auditar. En base a la visita se procede a generar la planeación de la auditoría para dar cumplimiento a los lineamientos de auditoría de verificación y análisis del sistema informático indicados en el anexo 13 capítulo III referente a la auditoría del sistema informático del reglamento de elecciones. En este punto se identifican los miembros que conformarán el equipo auditor, las actividades, fechas, horarios y responsabilidades necesarias para llevarla a cabo. Posteriormente se inicia la preparación de la auditoría durante la que, el Líder de auditoría elabora las listas de la documentación, las reglas, los estándares, programa reuniones con el equipo auditor, da instrucciones a los miembros del equipo, del material a ser asignado y asigna roles a cada integrante. Igualmente, cada miembro del equipo tendrá la tarea de estudiar el material y prepararse para desempeñar un papel satisfactorio. De acuerdo con la documentación presentada por las empresas, cada integrante tendrá asignado un conjunto de casos de uso del sistema, con lo que construirá un banco de pruebas a aplicar que permitan verificar la funcionalidad del aplicativo de acuerdo con lo establecido en las especificaciones. Se debe realizar una reunión donde cada participante entienda su función como parte del equipo y se acuerden los compromisos de entrega de sus reportes de actividad.

Durante la ejecución se deben realizar las acciones programadas, aplicando los instrumentos y herramientas (ANEXO EXCEL DE CAPTURA DE PRUEBAS) identificando desviaciones a la funcionalidad establecida y registrándola en el Help Desk instalado para este propósito. Existen distintos métodos de inspección para un desarrollo completo o para un atributo de calidad [3], durante esta etapa se aplican tres métodos de inspección: a) de alto nivel: que utiliza los requisitos de software, las especificaciones de la interfaz y sobre estos realiza la inspección, b) de código: dirigida fundamentalmente a encontrar rutinas de código que puedan alterar la funcionalidad del producto de software. c) de características: que buscan analizar el conjunto de características determinadas del producto de acuerdo con los escenarios proporcionados por los usuarios, con la finalidad de obtener hallazgos relacionados al uso de productos de software. Una vez que han sido revisados los sistemas y registrado los hallazgos en el Help Desk se procede a realizar un análisis para asignarles su impacto y darle un seguimiento al estatus. Previamente antes del dictamen se realiza una reunión con el equipo auditor para identificar posibles situaciones no ligadas directamente al producto de software auditado pero que se pudieran dar durante la ejecución de la auditoría y que no tengan registro en el sistema. Con toda la información se realiza un resumen de los hallazgos de acuerdo con su impacto, se describen los mecanismos de seguimiento y se elabora los informes (Parciales y finales) según corresponda.

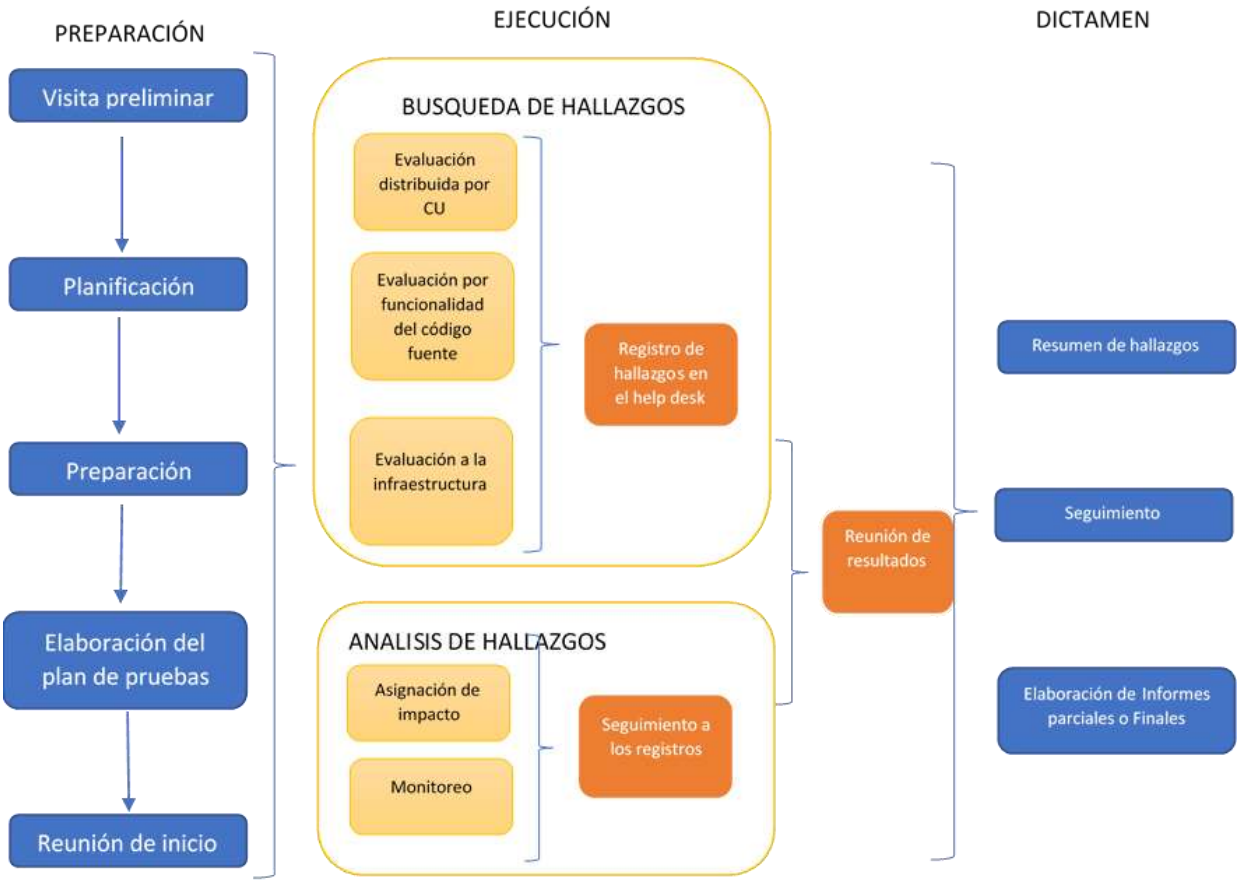

Figura 2. Modelo de desarrollo de actividades de la auditoría

B) Roles y participación

- Líder de auditoría: Es el responsable de las tareas administrativas relativas a la auditoría, la planeación y preparación, verificando que la auditoría se lleve a cabo de manera ordenada y que cumpla con los objetivos y de la recopilación de datos. Presenta los dictámenes al evaluado.

- Documentador: Es el responsable del registro y descripción de las anomalías, elementos de acción, las decisiones y recomendaciones formuladas por el equipo auditor. Registra los datos requeridos para el análisis de los procesos, el líder puede realizar esta función.

- Auditor: Tiene la responsabilidad de estudiar y comprender el material y la documentación de apoyo entregado por parte de la empresa auditada.
  Identificar y describir anomalías del producto
  Registrar en las herramientas de software los hallazgos encontrados de acuerdo a los formatos establecidos para este propósito.

- Jefe de auditores: Se encarga de llevar a cabo una reunión con el equipo de trabajo para acordar los elementos a auditar por cada integrante.
  Apoyar a los auditores en la detección de defectos
  Verificar que se siguen los estándares y reglas establecidas para la inspección

Verificar que se cumpla la agenda planeada.

- Auditado: Tiene la responsabilidad de facilitar y distribuir la información y documentación al equipo auditor. Recomendar o no la realización de una sesión de presentación y explicación del sistema, este rol lo realiza una persona externa a la entidad evaluadora.

Cada uno de los integrantes del equipo auditor juega un rol importante dentro de la auditoría. En la tabla 1.1 se observa la participación de los actores en las distintas fases de la auditoría.

Etapas	Líder	Documentador	Auditor	Jefe de Auditoría	Auditado
Visita preliminar	X				X
Planificación	X	X		X	X
Preparación	X			X	
Elaboración del plan de pruebas	X	X	X	X	
Reunión de inicio	X	X	X	X	
Búsqueda de hallazgos		X	X	X	
Registro de hallazgos		X	X		
Análisis de hallazgos	X	X	X	X	
Seguimiento de hallazgos	X	X		X	
Integración de los hallazgos	X	X		X	
Elaboración de los informes parciales	X	X		X	

Tabla 1.1 Roles y Actividades

5. ALCANCES DE LA AUDITORÍA

De acuerdo con las líneas de trabajo definidas por el Instituto electoral del estado de Campeche y para dar cumplimento al artículo 347, numeral 1, inciso a) del Reglamento de Elecciones el alcance de la auditoría aplicará para los módulos y las bases de datos del sistema informático del PREP, PREP CASILLA a utilizarse en las elecciones del 1ro de Julio de 2018 como se describe a continuación:

A. Pruebas funcionales de caja negra al sistema informático del PREP.
    a. Se validará el proceso técnico operativo de los siguientes módulos:
        i. Módulo de Digitalización, Captura y Validación que inicia con la obtención de la imagen digital del acta, captura de la información contenida en las Actas PREP y finaliza con la validación de la información capturada.
        ii. Módulo de Publicación de Resultados que consiste en la revisión de la obtención de los resultados, así como de la emisión de reportes y su despliegue, de acuerdo con la documentación técnica y la normatividad aplicable por el INE.

       Las actividades de validación se realizan de acuerdo con el flujo completo establecido e interacción entre los diversos módulos identificando posibles alteraciones al proceso.
    b. Se validará el cumplimiento de las especificaciones funcionales y requerimientos del sistema de acuerdo con la documentación técnica y la normatividad, inspeccionando el código en la búsqueda de posibles rutinas y/o código malicioso que pudiera alterar el resultado el día de las elecciones.
    c. Se validará la correspondencia de los datos capturados en las actas PREP con los presentados en la publicación, mediante los distintos tipos de reportes desplegados por el PREP, considerando datos, imágenes y bases de datos.
B. Validación del sistema informático del PREP y de sus bases de datos.
    a. Se verificará que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del sistema informático PREP, así como que la base de datos se encuentre debidamente inicializada de acuerdo con el diagrama de flujo acordado conjuntamente entre el IEEC y el ITESCAM.
    b. Se generarán y validará las huellas criptográficas utilizando el algoritmo SHA-256 del software PREP auditado contra los códigos generados del sistema instalado en el ambiente de producción que operará el día de la jornada electoral.
C. Pruebas a la infraestructura de los sistemas informáticos.

6. EJECUCIÓN DE LA AUDITORÍA

A) Criterios utilizados

La finalidad de la auditoría es detectar e identificar anomalías en los sistemas informáticos a utilizarse durante las elecciones de julio de 2018. Este es un examen sistemático entre iguales que:

a) verifica que los sistemas utilizados cumplen con sus especificaciones
b) verifica que los sistemas satisfacen especificaciones y atributos de Seguridad
c) verifica que los sistemas se ajustan a los procedimientos, normas, directrices, planes y reglamentos aplicables por el INE y el IEEC
d) identifica códigos y/o software malicioso que pudiera afectar los resultados

B) Metodología para clasificar los hallazgos

Las anomalías se categorizaron basados en las especificaciones del estándar IEEE 1044-2009.

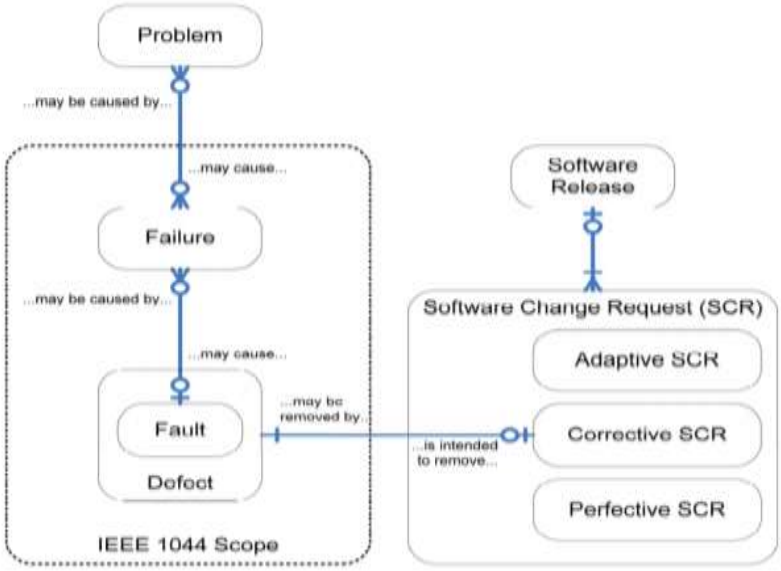

Figura 3. Modelo de relación entre causas y efectos para la detección y corrección de errores.

Las clases de anomalía proporcionan evidencia de inconformidad y las clasificamos:
a) falta.
b) extra (superfluo).
c) ambiguo.
d) inconsistente.
e) mejora deseable.
f) no se ajusta a las normas.
g) propensa a riesgos.

Las anomalías pueden ordenarse por el impacto potencial sobre los sistemas y las dividimos en tres niveles:

Alto impacto: Anomalías que tienen como resultado una disminución considerable en la percepción de los usuarios finales, es decir que alteren los resultados publicados. Estas anomalías afectan al mayor grupo de usuarios (público en general) generados por uno o más procesos erróneos.

Mediano impacto: Anomalías de los sistemas que a pesar de presentarse y generar un fallo permiten la continuidad de las operaciones.

Bajo impacto: Anomalías que difieran de las especificaciones pertinentes, pero no causará la falla de los sistemas de software o una salida observable en el rendimiento

C) Hallazgos identificados en el primer informe y que no han sido atendidos.

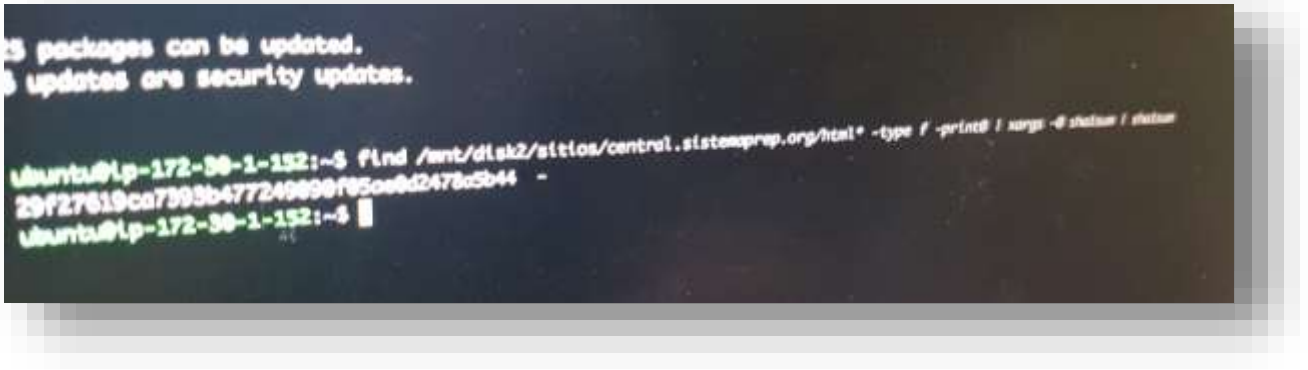

Figura 1. Cálculo Hash del sistema prep

Para dar cumplimiento a lo solicitado por el IEEC los hallazgos descritos son relacionados a las pruebas funcionales de caja negra, validación del sistema informático y de sus bases de datos, y pruebas a la infraestructura de los sistemas informáticos. En cada uno de ellos se maneja un estado (no atendido, en atención, atendido) para determinar su situación, dando un seguimiento desde la plataforma de incidencias implementada para monitorear y verificar su estado al momento de rendir el informe.

No. de caso de uso	Caso de uso o aplicativo	Descripción del hallazgo	Impacto	Estado
1	Inicio de sesión CATD	Al intentar acceder con una contraseña errónea por más de 3 intentos el sistema envía una notificación de actualización (NO SE PUDO ABRIR EL ARCHIVO, DESEA DESCARGARLO DE NUEVO) y descarga una actualización. El usuario que accede después de ocurrido esto no puede realizar alguna otra actividad (CAPTURAR, GUARDAR, ENVIAR) debido a que el sistema le indica que el acta ha sido capturada por otro usuario.	Medio	Atendido
4	Captura de actas CATD	El sistema permite ingresar un número de votos por encima de total expresado en la	Medio	Atendido

		lista nominal.		
4	Captura de actas CATD	El sistema debe verificar la suma de las boletas sobrantes y el resultado de la votación, está debe ser igual a las boletas entregadas pero el sistema no realiza esta verificación.	Medio	**No atendido** La empresa argumenta que los cálculos solicitados por la auditoría se realizan manualmente contrario a lo que se recomienda en la observación.
5	Marcar inconsistencias	El sistema presenta la opción de inconsistencia sin acta, sin embargo, no aparecen las opciones completamente ilegible y completamente sin dato por lo que no se puede probar su funcionalidad.	Bajo	Atendida
13	Captura de actas CCV	En el campo fecha permite capturar cualquier tipo de dato y no valida que sea una fecha en realidad.	Medio	Atendida
13	Captura de actas CCV	Al solicitar traer actas capturadas en PREP Casilla no siempre devuelve el acta que se capturó, la ventana necesitaba muchas veces pedirlo una segunda o tercera vez.	Medio	Atendida
4	Captura de actas en CATD	El sistema valida la fecha y hora de acopio en base a los datos que tiene la PC y en un rango no mayor a éste, lo que puede dar el caso de que la fecha y hora actual de la PC sea incorrecta y no permita asignar estos datos de forma correcta. Se sugiere que sea directamente tomada de internet.	Bajo	**No Atendida.** El sistema depende de la fecha y hora actual del sistema local y que tiene como vulnerabilidad el usuario.
4	Captura de actas en CCV	Se sugiere que el acta escaneada sea validada solo por el código QR para evitar que existan actas capturadas en casillas que no le corresponde.	Bajo	
13	Captura de actas en	Se pueden capturar más de una vez las actas para una casilla.	Medio	

	CCV			
4	Captura de Actas en CATD	Existe en la interfaz de captura un campo editable nombrado acta en curso que en caso de modificarse genera errores que ya no permiten volver a visualizar el acta de ese distrito. (CORROMPE LA RELACIÓN). Se sugiere quitar los permisos de edición.	Medio	Atendida
4	Captura de Actas en CATD	En la ventana detalle de acta el campo id de acta es editable y en caso modificaciones genera errores que ya no permiten volver a visualizar el acta. Se sugiere quitar los permisos de edición.	Medio	Atendida
4	Captura de Actas en CATD	No existe evidencia de una notificación vía sistema de que un acta ha sido reiniciada por el validador 2 por lo que existe el riesgo de que el acta no sea procesada adecuadamente.	Alta	Atendida
SN	Notificación de lista nominal	Si el número de votos excede la lista nominal el sistema muestra notificaciones al capturista para que las considere, cuando el acta llega al validador 1 no le muestra ninguna notificación.	Medio	
SN	Validadores	Cuando las actas solicitadas por los validadores 1 o 2 aparecen en pantalla y se pierde la conexión o se actualiza la página el acta se pierde y no se puede recuperar. Ante esta situación los conteos no son modificados y el acta no es contabilizada.	Alto	**No Atendida.** No se pudo verificar que el acta regresara a un validador. La empresa argumenta que no puede ser definido el tiempo de liberación del acta hasta que el IEEC lo establezca.
SN	Validadores	Cuando se produce una notificación de error en los validadores 1 y 2, se despliegan en la parte superior de la página y no son visibles para el usuario. Se recomienda que la notificación se muestre en el área de trabajo en donde se encuentre el usuario.	Medio	**No Atendida.** Esta observación fue encontrada al momento de la revisión al código fuente.

SN	Datos del acta	Cuando excede la lista nominal la información de total de votos que aparece en el capturista no es la misma que aparece en el validador 1.	Medio	Atendida
SN	Editar acta /reiniciar acta	Al momento de darle clic al botón no se hace ninguna confirmación de la acción, es decir, si por error se rechaza un acta no hay un mecanismo que evite que suceda la acción, se sugiere entonces poner una validación o confirmación en el botón DENEGAR, o REINICIAR. Se recomienda que exista una ventana de confirmación para cuando se presione el botón de editar acta o de reiniciar acta.	Medio	**No Atendida**. para el validador 1
22	Publicación	Cuando dos o más partidos tienen el mismo número de votos el sistema declara ganador a uno de ellos.	Medio	Atendida
22	Publicación	Cuando el capturista coloca un valor distinto de votos con respecto a la suma de los votos por partido, el sistema suma correctamente los votos reales, pero al momento de publicarlos muestra el valor capturado en el campo total de votos que no es coincidente con lo reales.	Alto	Atendida
SN	Revisión de código fuente	No se pudo realizar la inspección del código fuente.	Alto	Atendida
SN	Reportes	No se pudo realizar una inspección visual a los datos que se almacenan en la base de datos.	Alto	Atendida

II. Validación del sistema informático del PREP y de sus bases de datos.

No. de caso de uso	Caso de uso o aplicativo	Descripción del hallazgo	Impacto	Estado

SN	Control y administración de usuarios (digitalizadores , capturistas y publicadores) del PREP.	No se puede realizar la verificación porque no se tuvo acceso al módulo desarrollado, ni el caso de uso descrito.	Medio	Atendida.
SN	Monitoreo y control de los capturistas.	No se puede realizar la verificación porque no se tuvo acceso al módulo desarrollado, ni el caso de uso descrito.	Medio	Atendida
SN	Módulo de Consulta de Bitácoras (Aplicación y Base de Datos)	No se puede realizar la verificación porque no se tuvo acceso al módulo desarrollado, aunque en los casos de uso se describe el registro de las acciones en la bitácora.	Medio	Atendida
SN	Base de datos	Cuando se produce una inconsistencia que llega hasta el validador 2 y éste coloca valores excediendo la lista nominal el sistema le reporta el error al usuario e indica “El acta se liberará más tarde” pero en la base de datos el status se mantiene como “Con inconsistencia” cuando debería marcarse como Acta no procesada o reiniciada.	Alto	**No atendida.** Esta observación fue identificada en la revisión a código fuente.
SN	Estadístico de rendimiento de digitalizadores y capturistas.	No se puede realizar la verificación porque no se tuvo acceso al módulo desarrollado, ni el caso de uso descrito.	Medio	**No atendida**.
SN	Generación de huellas criptográficas	No se pudieron generar las firmas digitales para los códigos auditados debido a que la empresa no permitió realizar este proceso por motivos de actualizaciones frecuentes a los archivos durante la auditoría lo que no permite dar certeza a la versión auditada.	Alto	**No atendida.** Aunque se pudo generar el hash con los programadores el sistema sigue teniendo cambios por lo que no se puede garantizar la validez del software utilizado en el simulacro.

D) Recomendaciones.

Es importante exhortar a las partes auditadas la necesidad de tener una versión auditable de los módulos y que se mantenga sin cambios durante el proceso de auditoría, se exhorta a la empresa que durante el proceso de auditoría se notifiquen los momentos definidos para la realización de pruebas internas, tratando de evitar situaciones en donde se reporten hallazgos por situaciones de operaciones en paralelo entre el equipo auditor y el equipo de pruebas con la finalidad de que las pruebas aplicadas den certeza en el cumplimiento de las especificaciones.

Se recomienda que las personas a auditar conozcan plenamente el proceso a aplicar el día de la jornada y que sean capaces de transmitir dicha información al ente auditor para evitar ambigüedades y llevar a cabo la correcta validación de dicho proceso. Es importante que se presente evidencia documental donde se describa el proceso y las funciones de cada uno de los participantes dentro de los CATD y CCV.

Existen actividades dentro de los procesos en donde el usuario de acuerdo con su criterio o su poder de observación toma decisiones, es importante que existan mecanismos que permitan apoyar estos procesos de manera automática dentro del software para minimizar irregularidades, ambigüedades o errores humanos.

Con la finalidad de agilizar el proceso de auditoría es necesario contar con al menos dos réplicas completas del ambiente de operación que contemple todos y cada uno de los periféricos, aditamentos, y conectividad entre los sistemas involucrados, para realizar las pruebas necesarias, sobre todo la validación de ingreso de usuarios en paralelo.

En la revisión del código fuente se pudo constatar que los cálculos realizados para los conteos y algunos procesos de control se realizan en procedimientos almacenados en la base de datos. Se recomienda que dicha base de datos cuente con sistemas alternos de respaldo que aseguren la continuidad del servicio en caso de que éste quede no disponible por alguna contingencia.

En la revisión de bitácoras, la empresa presenta un mecanismo basado en JSON para obtener la información generada y argumenta que el encargado de desarrollar la plataforma para consultar y mostrar informes sobre dicha información es el IEEC. Es necesario que las dos partes IEEC y Empresa determinen dicho mecanismo para que sea funcional el día de los simulacros y jornada electoral.

Para garantizar la autenticidad y validez de la aplicación utilizada en los simulacros y el día electoral es importante utilizar los mecanismos solicitados por el IEEC que son la firma a través del cifrado del directorio donde se encuentran instalados los aplicativos. Hasta el momento la parte auditada no ha podido solventar este requerimiento por lo que se recomienda buscar la realización esta tarea.

Referencias Bibliográficas

[1] Gabriel Buades
Universidad de las Illes Balears,
Departamento de Ciencias Matemáticas e Informática,
http://dmi.uib.es/~bbuades/calidad/sld010.htm
España.
Año: 2002.

[2] Jose Javiar Dorado y Luis Fernandez Sanz
Medición para la Gestión de la Ingeniería de Software,
Ra-Ma,
Año: 2000.

[3] Gordon Schulmeryer and James McManus,
Handkook of Software Quality Assurance,
Prentice Hall
Año: 1999

[4] IEEE Computer Society,
IEEE Standard Classification for Software Anomalies
Institute of Electrical and Electronics Engineers,
Año: 2010