Xalapa, Veracruz; 11 de agosto de 2023

Transmitimos valores para construir democracia

INFORME QUE EMITE LA UNIDAD TÉCNICA DE SERVICIOS DE INFORMÁTICA RESPECTO A LA INCIDENCIA DETECTADA EN EL SISTEMA DE CONTABILIDAD EN LÍNEA EL 7 DE AGOSTO DE 2023.

Presidencia del Consejo General
OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL
RECIBIDO
Fecha 11/08/23 Hora 10:37

a) Motivos que originaron los cambios en la programación del SiCLi

El día lunes 7 de agosto de 2023, aproximadamente a las 14:45 horas, a través de una video llamada llevada a cabo entre la Unidad de Fiscalización y esta Unidad Técnica de Servicios Informáticos, se hizo la petición a esta UTSI consistente en modificar el módulo de datos generales a efecto de que se pudiera editar la información contenida en el Sistema de Contabilidad en Línea (SiCLi),

La Unidad de Fiscalización expresó que la razón de tal modificación consistía específicamente en permitir que la Asociación Política Estatal Ganemos México la Confianza pudiera modificar los datos del Titular del Órgano Interno. Es oportuno mencionar que, la UF también dijo que la actualización de esa información, es responsabilidad de la propia APE, quien tenía la obligación de haber hecho tal indicación en el sistema desde el mes de enero del presente año.

Concretamente, ante el requerimiento de la Unidad de Fiscalización y atendiendo a las indicaciones que esta Unidad Técnica recibió de brindar todas las facilidades para atender las adecuaciones al SiCLi que se requieran, es que se procedió a comentar algunas opciones para atender el requerimiento.

Ante las opciones, conjuntamente se acordó hacer la habilitación momentánea y posterior a la actualización referida regresar al estado anterior del sistema. Concluyendo la videollamada, se procedió a realizar las siguientes actividades.

b) Hechos sucedidos en la perdida de información

- La UTSI trabajó en la actualización del SiCLi en una versión del sistema instalada en una computadora, a fin de no afectar directamente al Sistema que estaba trabajando en los servidores hasta tener la certeza de que realizaba lo que había solicitado.
- Se realizan varias pruebas para corroborar que la actualización permitía modificar específicamente la información solicitada, es decir, al Titular del Órgano Interno y aproximadamente a las 15:10 horas del 7 de agosto de 2023, se subió la actualización al sistema en producción para que la Asociación Política Estatal pudiera hacer la captura.
- La APE, ingresó al SiCLi y realizó la modificación, situación que la Unidad de Fiscalización hizo del conocimiento del programador.
- En consecuencia, se procedió a realizar la nueva actualización del SiCLi, para dar reversa y dejar el sistema en el estado anterior a la modificación, es oportuno mencionar que la modificación en el sistema fue en cuanto a lo que debe y no debe hacer el sistema y no involucró a la información contenida en el Sistema, es decir, el permiso para poder modificar un campo o valor, y volver a impedir que un campo o valor pueda ser modificado.
- Las actualizaciones a la forma en que debe actuar el SiCLi se concluyeron, es decir, nuevamente el Sistema impedía que se modificara al Titular del Órgano Interno.
- Desde que se realizó la primera actualización mencionada, se recibieron reportes vía WhatsApp por parte del equipo contable de la Unidad de Fiscalización, donde referían que dejaron de ver las evidencias que las APE´s habían cargado al SiCLi.
- Ante dicha situación la UTSI se dio a la tarea de revisar las posibles causas de la situación reportada y al revisar la consola del Servidor en el que se encuentra alojado el SiCLi, la UTSI advirtió que la carpeta ***storage*** se encontraba vacía.

La situación que se presentó en el SiCLi fue que se utilizaron dos *ramas* diferentes de lo que se encuentra respaldo en el sitio de gitlab.com, provocando con esto discrepancias en la información contenida en la carpeta ***storage***, motivo por el cual la información perdió consistencia y se volvieron ilegibles.

Las *ramas* son versiones diferentes del sistema, se ocupan para tener control de lo que trabajan en su caso mas de un programador, en el caso del SiCLi la *rama* "Master" contiene una configuración inicial que se dejó a manera de respaldo antes de hacer la reingeniería del sistema en el año 2022, actualmente esa *rama* permanece en ese estado; la segunda rama es la que tiene la versión vigente y se ocupa para hacer todas las actualizaciones. Al actualizar la versión del SICLI para lo solicitado se invocó a la rama Master y al ser diferente en muchos aspectos del sistema ocasionó la incidencia descrita en el presente documento, el repositorio tiene la posibilidad de revertir el movimiento, lo cual se hizo, pero la carpeta ***storage*** quedó inaccesible.

c) Acciones implementadas por la UTSI para restablecer la visualización de la información en el SICLI

A fin de encontrar una solución a la problemática detectada, el Departamento de Desarrollo dio aviso de lo sucedido al Departamento de Infraestructura, ambos de esta UTSI, y solicitó su apoyo para la restablecer la información. Esto se materializó realizando una clonación del servidor en el que se encuentra el SiCLi para tener una copia sin alteraciones y poder ejecutar tareas de restablecimiento sin afectar la operatividad de los demás sistemas alojados en el servidor mencionado.

De manera inmediata se recurrió a todo el personal de recursos humanos con los que cuenta el Departamento de Desarrollo, sin poder lograr la restauración de la integridad de los archivos. Asimismo, el Departamento de Infraestructura instaló en el servidor dos herramientas denominadas *test disk y reverter forense* para intentar revertir los cambios hechos por el SiCLi y solucionar la incidencia, sin embargo, las herramientas tecnológicas no pudieron recuperar la integridad de los archivos.

Durante el periodo comprendido del 7 de agosto a las 15:30 horas hasta esta fecha, el Departamento de Desarrollo continúa investigando posibles opciones para recuperar la integridad de los archivos contenidos en la carpeta ***storage*** y tales como pruebas a través del mismo *GIT* intentando restaurar a una versión anterior a lo realizado por el SiCLi en el servidor. Dichas pruebas tampoco han dado resultados positivos.

A fin de ser exhaustivos en la búsqueda de soluciones, se solicitó asesoría externa de personal técnico altamente especializado en busca de lograr el restablecimiento de la información, a lo cual se decidió acudir a un *Laboratorio Forense de Recuperación de Archivos.* La empresa que realizó la revisión y diagnóstico fue RecoveryMark, ubicada en la calle Rubén Darío no. 97, C.P. 03510 Benito Juárez en la Ciudad de México.

En consecuencia, el día miércoles 9 de agosto de 2023, se acudió a las instalaciones del laboratorio ubicadas en la Ciudad de México, en donde se realizó un diagnóstico y después de correr 5 herramientas forenses, los especialistas solo lograron identificar el tamaño de la carpeta (58Gb), sin embargo, la información continuó siendo ilegible.

Ante las adversidades, el miércoles 9 de agosto de 2023, el personal del Departamento de Desarrollo se dio a la tarea de reconstruir la información generada por el SiCLi, siguiente:

- Pólizas contables
- Libro diario
- Conciliación bancaria
- Estado de posición financiera
- Balanza de comprobación
- Estado de ingresos y egresos
- Auxiliares contables
- Informe y documentación adjunta
- PAT

Lo anterior es posible en virtud de que la base de datos se mantuvo consistente y pudieron tomarse los parámetros para regenerar esos documentos, debido a que la base de datos se aloja en un sitio diferente a la carpeta ***storage***, es decir, se ubica en el manejador de base datos del servidor correspondiente.

d) Consideraciones generales de la configuración de los Sistemas y Servidores

Con la finalidad de tratar de explicar detalladamente algunas de las cuestiones técnicas que contiene el presente informe, se detalla la información siguiente:

- **Carpeta *STORAGE***

El SiCLi está configurado para que toda la información que es subida por las APE´s se almacene en la carpeta denominada ***storage.*** Esto es, los archivos PDF y JPG que las Asociaciones adjuntan al Sistema como evidencia de sus registros contables son relacionadas por el Sistema, almacenándose el nombre en un campo de la base de datos y los archivos físicamente son almacenados en dicha carpeta.

- **Servidores Virtuales**

Es importante informar que los servidores se encuentran virtualizados para eficientar su uso y que el almacenamiento del mismo se encuentra en un arreglo de discos duros que alojan la información de la mayoría de los sistemas del OPLE Veracruz. Al contar con esta configuración se aprovecha de mejor manera el espacio, pero se encuentra almacenado por segmentos en vez de estar de manera conjunta como sería en un servidor físico.

Esta configuración permite que un servidor físico pueda alojar diferentes máquinas virtuales con diferentes sistemas operativos y aplicaciones, otorgando diversos modos de uso para atender las distintas necesidades de los Sistemas, las áreas y los usuarios.

Asimismo, se replica la información en distintos discos (como si fuera un espejo, lo que se modifica en uno se respalda en otro al mismo tiempo), previniendo la perdida de la información con motivo de fallas físicas, ya que en caso un mal funcionamiento, la información se encuentra replicada. Sin embargo, en este evento no fallaron físicamente los discos, si no que el propio sistema al encontrar diversas versiones de programación volvió corruptos los archivos dando como resultado que no pueda accederse a ellos.

- **Gitlab.com (GIT)**

Todos los códigos fuente de los sistemas del OPLE Veracruz se encuentran respaldados en un repositorio en la nube (GIT). Esto proporciona muchas ventajas, una de ellas es que desde cualquier lugar se pueden realizar actualizaciones y/o mantenimientos a los Sistemas.

Es importante mencionar que el repositorio cuenta con todas las medidas de seguridad para garantizar el uso únicamente al personal autorizado, solo es administrado por una cuenta con privilegios administrativos, las demás cuentas son configurables para dar acceso a uno o varios sistemas de los que se encuentran contenidos en él, esto se hace a través del correo electrónico de cada uno de los programadores, de tal manera que solo tienen acceso al sistema del cual son responsables.

Las actualizaciones se trabajan y prueban de manera local con versiones instaladas en servidores locales para corroborar la congruencia de las modificaciones, al subir la actualización al sitio gitlab.com para el control de cambios lleva un registro de todos las actualizaciones, teniendo los datos del responsable de hacerlo, una breve descripción de la modificación y un comparativo donde identifica en específico las líneas de código que sufrieron modificaciones, una vez actualizado el repositorio se hace *Deploy* en el servidor (es decir se aplican los cambios) y solo modifica los archivos identificados con cambios.

- **Extracto del código del SiCLi.**

En las imágenes siguientes se puede apreciar como el repositorio identifica los cambios realizados y en que archivos, de esta manera se verifica que no se afecta ningún otro sitio del sistema:

- En la línea 1306 se puede advertir como se agregan comentarios en el código que dan indicios de que hace esa rutina, sin afectar el funcionamiento del sistema.
- En Línea 1309 se puede observar cómo se *comenta* (agregan dos diagonales) a fin de que el sistema ignore el proceso de envió de un correo electrónico.

- En la Línea 267 se puede observar cómo se *comenta* (agregan dos diagonales) a fin de que el sistema ignore el proceso de envió de un correo electrónico.

app/Http/Controllers/NewApeController.php — View file @ 382766a1

```
...  ...  @@ -264,7 +264,7 @@ class NewApeController extends Controller
264  264          // dd('vali');
265  265          $nombreRequerimiento = Semaforo::find(3);
266  266          $moreUsers = array($ape->email, 'sicli.oplever@gmail.com');
267       -       Mail::to($ape->emailApe->email)->cc($moreUsers)->send(new SemaforoMail($nombreRequerimiento, $user, $fecha,
     $color));
     267  +       //Mail::to($ape->emailApe->email)->cc($moreUsers)->send(new SemaforoMail($nombreRequerimiento, $user, $fecha,
     $color));
268  268
269  269          Alert::success('Datos guardados correctamente', 'Integración del Órgano Interno');
270  270          return redirect()->back();
...  ...
```

- En la Línea 43 se observa cómo se cambia la condición para que habilite la opción de edición.

resources/views/partials/integracion.blade.php — View file @ 382766a1

```
...  ...  @@ -40,7 +40,7 @@
40   40   </div>
41   41   @else
42   42   @foreach($requisitouno as $req)
43       - @if($req->status != 'Validado por APE')
     43   + @if($req->status === 'Validado por APE' && $ape->nombre==='GANEMOS MÉXICO LA CONFIANZA')
44   44   <div class="card">
45   45           <div class="card-body">
46   46                   <div class="row">
...  ...
```

MTRO. JUNIOR ABRAHAM CRUZ ANCONA
TITULAR DELA UNIDAD TÉCNICA DE SERVICIOS DE INFORMÁTICA