KPMG Cárdenas Dosal, S.C.
Manuel Ávila Camacho 176 P1,
Reforma Social, Miguel Hidalgo,
C.P. 11650, Ciudad de México.
Teléfono: +01 (55) 5246 8300
kpmg.com.mx

Al Comité de Auditoría de
Banco Nacional de Obras y Servicios Públicos,
Sociedad Nacional de Crédito, Institución de Banca de Desarrollo
y a la Comisión Nacional Bancaria y de Valores:

Las observaciones contenidas en este informe por el año terminado el 31 de diciembre de 2018, son resultado de nuestra evaluación de la estructura de control interno de **Banco Nacional de Obras y Servicios Públicos, S.N.C. Institución de Banca de Desarrollo** (la Entidad), se presentan para dar cumplimiento con los aspectos contenidos en las disposiciones que establecen los requisitos que deberán cumplir los auditores externos y los bancos emitidas por la Comisión Nacional Bancaria y de Valores (la Comisión).

- Las observaciones y recomendaciones de mejoras al 31 de diciembre 2018, se resumen a continuación:

1.- Accesos a programas y datos/ Identificación y autenticación para los aplicativos IKOS Tesorería, Yatla, SICOFIN y SIC.

Hallazgo:

Se identificó que las bases de datos para los aplicativos IKOS Tesorería, YATLA, SICOFIN y SIC no se encuentran correctamente configurados de acuerdo a lo establecido en el documento "Directrices de la gestión de cuentas de usuarios" en los apartados:

- 11.4. Del procedimiento de Bloqueo -Desbloqueo y
- 11.8. De la contraseña,

Se identificó que las cuentas no se bloquean a los 3 intentos fallidos, en el caso del administrador se bloquea a los 5 intentos y las cuentas con perfil default se bloquean a los 10 intentos fallidos. Los usuarios default no cuentan con un periodo de cambio de contraseña, este valor se encuentra "UNLIMITED".

Impacto:

El tener un mayor número de intentos para ingresar a la base de datos causa mayor posibilidad de acceso a la base de datos, en caso de tener un acceso exitoso se puede comprometer la integridad, confidencialidad y continuidad de las operaciones del negocio.

Recomendación:

Correctivas: Establecer un plan de trabajo para el cambio de configuración en el número de intentos para ingresar a la Base de Datos, lo anterior, de acuerdo al documento "Directrices de la gestión de cuentas de usuario".

Preventivas: Se recomienda seguir adecuadamente el proceso definido en el documento "Directrices de la gestión de cuentas de usuario".

Respuesta de la Administración:

Se llevará a cabo un plan de trabajo para el cambio de configuración en el número de intentos para ingresar a la Base de Datos; lo anterior, de acuerdo al documento "Directrices de la gestión de Cuentas de Usuario", con fecha de resolución el primer semestre del ejercicio 2019.

(Continúa)

2.- Accesos a programas y datos / Monitoreo de usuarios administradores y finales en actividades transaccionales de los sistemas SIC y SICOFIN.

Hallazgo:

Actualmente Banobras cuenta con una guía del proceso de monitoreo para cuentas de usuarios con privilegios de administrador a nivel aplicativo y base de datos; sin embargo, el alcance está acotado a los sistemas que la empresa tiene definidos como críticos Yatla e IKOS y no incluye SIC y SICOFIN, dicha guía solo monitorea los eventos que pasan a través de una solicitud de cambios, por lo que no fue posible identificar en la política los siguiente:

- Frecuencia de monitoreo
- Quien lo realiza
- Quien lo supervisa
- Que reportes se generan y que actividades se monitorean
- Quien da seguimiento a la resolución de incidentes

Así mismo, no se cuenta con un monitoreo de actividades transaccionales.

Impacto:

El no contar con monitoreo de la actividad de los usuarios, podría dificultar la identificación y rastreo transaccional de movimientos de usuarios pudiendo afectar la confidencialidad e integridad de la información.

Recomendación:

Correctivas: Fortalecer los procedimientos de monitoreo de actividades de los usuarios administradores y finales, donde se establezcan los pasos, frecuencia, responsable, transacciones a monitorear; así como, el seguimiento de incidentes presentados durante el monitoreo.

Preventivas: Las actividades a monitorear se tienen que establecer en conjunto con el negocio (actividades críticas).

Respuesta de la Administración:

Se actualizarán las políticas de la guía del proceso de monitoreo, para incluir los aspectos que se mencionan; asimismo, se analizara la viabilidad de incluir el SIC y SICOFIN, ya que éstos no están catalogados como críticos. Adicionalmente, se evaluarán los recursos necesarios para implementar procedimientos de monitoreo para cuentas de usuarios.

3.- Administración de cambios / Usuarios con ambientes de desarrollo y producción en el sistema IKOS.

Hallazgo:

Se identificó un usuario a nivel sistema operativo en IKOS, con acceso a los servidores de desarrollo y producción, no se identificó en el directorio activo y no existe una responsiva de la existencia de esta cuenta.

(Continúa)

Impacto:

Posible utilización de usuarios para realizar alguna modificación o extracción de información.

Recomendación:

Correctivas: Identificar el usuario y justificar su existencia dentro del servidor con el propósito de tener un control adecuado sobre accesos dentro del sistema operativo de IKOS.

Respuesta de la Administración:

Se elaborará plan de trabajo para eliminar este usuario, probándose primero en desarrollo y de no haber afectaciones se eliminará de producción.

4.- Hallazgo identificado en el transcurso de la auditoría, referente a las contingencias registradas en la cuenta de deudores por reclamación y los montos proporcionados por los abogados externos en la confirmación de saldos.

Hallazgo:

De la revisión efectuada a los montos registrados por la Entidad en la cuenta de orden "Deudores por reclamación – Asuntos laborales", al 31 de diciembre de 2018, se observa que en un 18% de los asuntos y en un 1.7% del saldo de la cuenta referida, existe una diferencia entre los saldos registrados por la Entidad y los montos proporcionados directamente por los abogados externos en la confirmación de saldos, siendo estos abogados externos Diez de Bonilla Kuri y Asociados, Cisneros Abogados, S.C. y Casiopea Asesores, S.C., quienes en 19 asuntos reportaron cifras diferentes a las registradas en la Entidad, cabe mencionar que los Abogados Externos son los que litigan y dan seguimiento a los juicios, por lo que ellos tienen mayor exactitud de los saldos actualizados de los litigios que son registrados en la cuenta de orden.

Impacto:

Al no tener actualizadas las cifras de algunos asuntos en la cuenta de orden "6106, Deudores por Reclamación – Asuntos laborales", se podrían tener pasivos contingentes registrados con montos distintos, afectando la exactitud y la valuación de dicha cuenta de orden.

Recomendación:

Correctivas: Realizar una conciliación entre las cifras que tiene la Entidad, con las cifras proporcionadas por los abogados externos, considerando los saldos que reflejen la situación actual del litigio.

Preventivas: Realizar una conciliación de forma periódica, entre las cifras de la Entidad con las cifras de los abogados externos, dejando documentado este control.

Respuesta de la Administración:

Se solicitará a los Abogados Externos la actualización o en su caso confirmación de los saldos a registrar en la cuenta "6106, Deudores por Reclamación", misma que deberá conciliarse a más tardar el 15 de diciembre de cada año.

(Continúa)

- Las observaciones y recomendaciones de mejoras que son recurrentes y fueron generadas durante ejercicio 2017 y que se encuentran abiertas al 31 de diciembre 2018, se resumen a continuación:

1.- Accesos a programas y datos/ Reglas de configuración de acceso (SOD).

Hallazgo:

Se identificó que el sistema SICOFIN no cuenta con una matriz de segregación de funciones formalmente documentada y aprobada por el negocio.

Impacto:

Que el área de negocio no cuente con una matriz de segregación de funciones del sistema SICOFIN, posibilita la asignación de tareas a un usuario que no necesariamente las requiere, por lo tanto, los usuarios intencionalmente o por error podrían poner en riesgo la integridad de la información financiera.

Recomendación:

Correctivas: El área de negocio deberá gestionar ante el área de Seguridad de la Información y Sistemas el diseño e Implementación de una matriz de segregación de funciones para el sistema SICOFIN, el área de negocio tiene que identificar los conflictos de segregación de funciones que pueden existir por el número de usuarios y/o las necesidades del negocio y documentar e implementar controles compensatorios que mitiguen el riesgo.

Preventivas: Posteriormente se recomienda implementar un procedimiento para la gestión de segregación de funciones.

Respuesta de la Administración:

Actualmente, no es posible implementar el procedimiento de segregación de funciones en el actual sistema SICOFIN esto derivado a que en el aplicativo no es posible implementar cambios, sin embargo, en curso se encuentra el proyecto Implementación del Sistema GRP el cual tiene por objeto a sustitución del actual sistema contable en una plataforma integral (SAP).

2.- Accesos a programas y datos/ Reglas de configuración de acceso (SOD).

Hallazgo:

El sistema SICOFIN no tiene la posibilidad de generar logs de la actividad de los usuarios a nivel aplicación (administradores y finales) por lo tanto no existen actividades de monitoreo.

Impacto:

El no contar con un monitoreo de logs de las cuentas de administración a nivel aplicación, dificulta el rastreo transaccional de movimientos pudiendo afectar la confidencialidad e integridad de la información, así como materializar el riesgo.

Recomendación:

Correctivas: Configurar los logs de la actividad de los usuarios administradores a nivel aplicación (SICOFIN) y en la medida de lo posible adquirir una herramienta robusta para el monitoreo mediante la cual sea posible llevar a cabo un monitoreo en tiempo real de la actividad de los usuarios administradores.

(Continúa)

Respuesta de la Administración:

Actualmente no es posible implementar logs en el sistema SICOFIN; sin embargo, se encuentra en proceso el proyecto de implementación GRP, en donde se tiene dimensionado el Registro de Bitácoras que permita registrar el detalle de cualquier tipo de entrada, salida, configuración y en general movimientos en el catálogo de cuentas. Dicha implementación se encuentra programada conforme el diagrama indicado en el hallazgo 1; sin embargo, como control adicional a nivel de la BD se encuentra implementado Audit Vault, que permite monitorear a nivel base de datos la actividad de los procesos que son ejecutados.

3.- Accesos a programas y datos/ Reglas de configuración de acceso (SOD).

Hallazgo:

Se identificó que el servidor donde reside el aplicativo SICOFIN (Windows server 2003) ya no cuenta con soporte extendido por parte de Microsoft.

Impacto:

Posibles riesgos de seguridad por vulnerabilidades que puedan comprometer la continuidad y disponibilidad de la información, en casos extremos la integridad.

Recomendación:

Correctivas: Actualizar el servidor donde reside el aplicativo SICOFIN y debido a que Banobras no cuenta con el código fuente del sistema SICOFIN se recomienda la implementación de otro sistema contable.

Respuesta de la Administración:

Como se ha comentado, por el momento no es posible realizar la migración derivado a que no hay modificaciones en el código del aplicativo; sin embargo, como una medida compensatoria, en tanto se termina la implementación del Módulo Contable, se consideró en el contrato DAGA/030/2018, que se suscribió para "Fabrica de Software", el "Servicio de Continuidad Operativa", esta continuidad operativa en el aplicativo permite reforzar el soporte del mismo y apoya la extracción de datos de información contable, que a su vez son utilizados en la implementación del Módulo Contable del GRP, con fecha de resolución durante el ejercicio 2019.

4.- Accesos a programas y datos/ Reglas de configuración de acceso (SOD).

Hallazgo:

Se identificaron las siguientes políticas y/o procedimientos que no fueron revisados durante 2017:

- Proceso de administración de incidencias 06/05/2016
- Proceso de administración de problemas 26/04/2016

(Continúa)

Impacto:

Al no tener políticas y/o procedimientos con una revisión y/o actualización periódica pueden existir documentos que se encuentren desactualizados u obsoletos, generando problemas operativos al momento de su consulta.

Recomendación:

Correctivas: Establecer controles mediante los cuales Banobras se asegure que todas las políticas y/o procedimientos se encuentran actualizados en contenido como de las personas que revisan y autorizan.

Respuesta de la Administración:

Me permito informarle, que con fecha 27 de agosto de 2018, se adjudicó el contrato DAGA/051/2018 para la prestación del servicio "Mesa de ayuda y Monitoreo", que comprende entre otros servicios el establecer y actualizar los procesos Administración de Incidentes y Problemas, de acuerdo al plan de trabajo, se encuentra previsto la resolución del hallazgo indicado anteriormente.

KPMG Cárdenas Dosal, S. C.

C.P.C. Jorge Orendain Villacampa
Socio de Auditoría

13 de marzo de 2019