Amerafin S.A.

Comentarios y Recomendaciones sobre
el Sistema de Control Interno

31 de diciembre de 2017

KPMG del Ecuador Cía. Ltda.
Av. República de El Salvador, N35-40
y Portugal, Edif. Athos, pisos 2 y 3
Quito - Ecuador

Teléfonos: (593-2) 245 0356
(593-2) 244 4228
(593-2) 244 4225
Febrero 14 de 2018

Señor
Fernando Muñoz, Apoderado Especial
AMERAFIN S. A.
Ciudad

Estimado Sr. Muñoz

Hemos efectuado nuestra auditoría de los estados financieros de Amerafin S. A. al 31 de diciembre de 2017 y hemos emitido nuestro dictamen sin salvedades sobre los mismos con fecha 7 de marzo de 2018. Como parte de nuestra auditoria realizamos un estudio del sistema de control interno contable, dentro del alcance que consideramos necesario evaluar dicho sistema, tal como es requerido por las normas internacionales de auditoría y aseguramiento. Bajo tales normas, el propósito de la evaluación es establecer una base confiable que sirva para determinar la naturaleza, oportunidad y extensión de los procedimientos de auditoría que son necesarios para expresar una opinión sobre los estados financieros y no para expresar una opinión sobre la eficacia del sistema de control interno.

La Administración de la Compañía es responsable de establecer y mantener un sistema de control interno. Para cumplir con esta responsabilidad se requiere que la Administración realice ciertas estimaciones y juicios para evaluar los beneficios anticipados y costos relacionados con los procedimientos de control. Los objetivos de un control interno conllevan a que la Administración obtenga una certeza razonable respecto a la salvaguarda de los activos contra pérdidas resultantes de uso o disposición no autorizada, que las transacciones se efectúen de acuerdo con la autorización de la Administración y que éstas se registren correctamente para permitir la preparación de los estados financieros. El concepto de seguridad razonable reconoce que el costo de un sistema de control interno contable no debe exceder los beneficios que se deriven de él y que la evaluación de estos factores por parte de la Administración requiere la elaboración de estimados y la aplicación de su criterio.

Hay limitaciones inherentes que se deben reconocer cuando se considera la efectividad potencial de cualquier sistema de control interno. En la realización de los procedimientos de control podrán resultar errores por apreciación o malentendido de las instrucciones, falta del debido cuidado y otros factores. Aquellos procedimientos de control cuya efectividad depende de la segregación de funciones pueden ser inoperantes debido a complicidad. Igualmente, los procedimientos de control podrían ser no observados, bien con respecto a los criterios y estimaciones que se requieren en la preparación de los estados financieros, o en la ejecución y registro de transacciones. Además, la proyección de cualquier evaluación del sistema de control interno a períodos subsiguientes está sujeto al riesgo de que los procedimientos puedan resultar inadecuados debido a cambios en las condiciones y de que el grado de cumplimiento de los procedimientos se pueda deteriorar.

... /

Nuestro estudio y evaluación del sistema de control interno contable, el cual fue hecho con el propósito establecido en el primer párrafo de este informe, no necesariamente descubriría todas las debilidades substanciales del sistema; consecuentemente, no expresaremos una opinión sobre la eficacia del sistema de control interno de Amerafin S. A. Sin embargo, este estudio mostró las condiciones que se mencionan en el anexo a esta carta, y que requieren acción correctiva de parte de la Administración de la Compañía, dichas condiciones fueron consideradas para determinar la naturaleza, oportunidad y extensión de los procedimientos que se aplicaron en la auditoría de los estados financieros y este informe no modifica nuestro dictamen sobre los mismos.

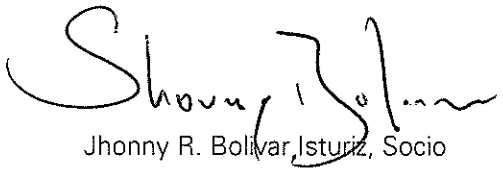
Debe entenderse que los comentarios tratan exclusivamente con principios y técnicas de contabilidad y no deben considerarse contra la integridad o capacidad de alguno de los funcionarios de la Compañía, a quienes deseamos agradecer la colaboración recibida durante el desarrollo de nuestro trabajo.

Es necesario que las recomendaciones aquí descritas sean comunicadas entre los principales funcionarios de la Compañía, de manera que las sugerencias puedan ser tomadas en cuenta por los mismos durante el desarrollo de las labores que se les ha encomendado.

Se entiende que este informe es únicamente para uso o información del Directorio, Gerencia y demás miembros de la Administración de la Compañía.

Muy atentamente,

KPMG del Ecuador Cía. Ltda.



Jhonny R. Bolívar Isturiz, Socio

Adj.: Lo indicado

AMERAFIN S.A.

Índice de Comentarios y Recomendaciones sobre el
Sistema de Control Interno

I.- ASPECTOS GENERALES

Accionista

De la revisión efectuada al listado de accionistas de la Compañía, observamos que la Compañía Inversiones Dogo Dogosa S. A. es accionista en Banco Pichincha C. A. y en Amerafin S. A.

De acuerdo a lo indicado en el Artículo 4 de la Resolución No. 382 del 22 de mayo de 2017 de la Junta de Política y Regulación Monetaria y Financiera, los accionistas directos o indirectos de una entidad financiera no podrán ser accionistas directos o indirectos de las compañías auxiliares de las entidades de los sectores financiero público o privado. Las entidades financieras sí podrán ser accionistas de las referidas compañías.

Es nuestra recomendación regularizar la participación accionaria del referido accionista con el fin de evitar que tanto Banco Pichincha C. A. como la Compañía sean observados por los Organismos de Control.

Comentarios de la Administración:

Inversiones Dogo Dogosa no tiene propiedad con influencia (art. 169 COMF) en Amerafin ni en el Banco, esto será expuesto a la Superintendencia de Bancos en caso de observación.

II.- TECNOLOGIA DE INFORMACION

Los comentarios y sugerencias que presentamos no son el resultado de un estudio detallado del departamento de TI, sino más bien nuestras observaciones surgen de los procedimientos básicos de auditoría aplicados. Nuestra intención al llevar a su conocimiento las situaciones observadas, es ayudarle en su gestión administrativa para la toma de decisiones y de optimizar el uso de los recursos humanos y técnicos.

Módulos de Seguridad Aplicaciones SIO y BPAC System

Se identificó que los módulos de seguridad de las aplicaciones SIO y BPAC System no controlan:

- Complejidad y longitud de contraseña
- Historial de contraseña

Las situaciones identificadas incrementan el riesgo de acceso no autorizado a la información administrada en las aplicaciones.

Recomendamos, se analice la posibilidad de implementar mecanismos de autenticación de usuarios como un single sing on entre el controlador de dominio y las aplicaciones SIO y BPAC System o controles automáticos para el control de contraseñas dentro de los módulos de seguridad como:

Control	Valor Recomendado
Complejidad de Contraseñas	letras, números y caracteres especiales
Historial de Contraseñas	3 últimas utilizadas
Bloqueo de usuarios	Después de 3 intentos
Longitud mínima de contraseña	8 caracteres

Comentarios de la Administración:

En la aplicación SIO: Historial de contraseña: Este tema está en fase de desarrollo y se finalizará hasta junio 2018.

En la aplicación BPACSystem: Complejidad y longitud de contraseña: Este sistema se dará de baja y solo se accederá en forma de consulta con un número reducido de usuarios, tal es así que a partir del segundo semestre del 2015 no se han realizado nuevos desarrollos en este sistema.

Seguridades Base de Datos - Aplicaciones Dynamics y SIO

Identificamos las siguientes deficiencias:

- El usuario "crystal" de la base de datos de la aplicación Dynamics tiene una contraseña igual a su ID de usuario.
- No se cuenta con un proceso de monitoreo de cambios en la base de datos de las dos aplicaciones.
- La cuenta de Administrador del sistema operativo sobre el cual se encuentra instaladas las bases de datos no han sido renombrados.

Las situaciones identificadas incrementan el riesgo de accesos no autorizados a la información contenida en las bases de datos de las aplicaciones SIO y Dynamics.
Recomendamos:

- Revisar la cuenta y contraseña del usuario crystal y analizar la factibilidad de realizar el cambio de contraseña con características de complejidad y longitud mínima de contraseña.

... /

- Establecer un proceso de registro, monitoreo y tratamiento de los cambios a los objetos, información y accesos a la base de datos.
- Renombrar al usuario Administrador a fin de fortalecer su seguridad dentro del sistema operativo. Esta implementación deben ser inicialmente evaluada para verificar que la misma no afecte a la disponibilidad de los servicios que actualmente están implementados.

Comentarios de la Administración:

- Usuario Crystal: es un usuario de lectura, sin embargo se validará con los proveedores el uso de este usuario para proceder a actualizar la contraseña (junio 2018).
- En el sistema BPACSystem existe un control previo a la ejecución del script, solo se puede actualizar con la autorización del jefe de IT.
- En el SIO se implementará el control (julio 2018).
- Se evaluará esta recomendación para no afectar a los procesos actuales, cabe indicar que el servidor se encuentra en la intranet, es decir no está expuesto al internet. (diciembre 2018).

Inexistencia de Monitoreo de Usuarios y Perfiles

Observamos que la Compañía no cuenta con lineamientos para realizar el monitoreo de usuarios y perfiles periódicamente; como consecuencia de esta deficiencia, se identificó la existencia de los usuarios genéricos creados en el controlador de dominio de los cuales se desconoce su uso: pool1, crpool01, pool, Lexmark, helpdesk.

La situación descrita incrementa el riesgo de accesos no autorizados a los recursos de red de la Compañía.

Recomendamos definir lineamientos para el monitoreo de usuarios de aplicaciones, sistemas operativos, bases de datos y recursos de red, el cual se ejecute periódicamente.

Comentarios de la Administración:

Se implementará el monitoreo de usuarios (julio 2018).

Controlador de Dominio

Identificamos las siguientes deficiencias en el controlador de dominio de la Compañía:

- Observamos que la versión del sistema operativo sobre el cual se encuentra instalado el controlador de dominio es Windows Server 2008 R2 el cual contó con soporte por parte del fabricante hasta el año 2013, lo cual incrementa el riesgo de que no se pueda contar con actualizaciones, parches de seguridad y falta de escalabilidad del servicio instalado sobre el servidor.

- No se cuenta con un proceso de monitoreo de eventos que se producen en el controlador de dominio que permita identificar oportunamente cambios y accesos a las configuraciones del controlador de dominio.

Recomendamos:

- Analizar la posibilidad de establecer un plan de actualización del sistema operativo a una versión superior que le permita a la Compañía contar con una infraestructura tecnológica escalable en el tiempo.

.../

- Establecer un proceso de registro y monitoreo de eventos de cambios y accesos a las configuraciones del controlador de dominio.

- Establecer un proceso de registro y monitoreo de eventos de cambios y accesos a las configuraciones del controlador de dominio.

Se establecerá el proceso recomendado (diciembre 2018).

Comentarios de la Administración:

Este es un tema crítico por las aplicaciones instaladas en el servidor y la compatibilidad con las aplicaciones instaladas, se realizará la migración hasta el primer semestre del año 2019 (junio 2019).

III.- SEGUIMIENTO A LA CARTA DE CONTROL INTERNO DEL AÑO ANTERIOR

Durante nuestra auditoría hemos dado seguimiento a los puntos de control interno del año anterior, sobre los cuales observamos que la Administración ha regularizado ciertos puntos, mientras que en otros se encuentra trabajando para su corrección.

- Propiedades de inversión.
- Análisis de las normas contables nuevas y modificadas.
- Administración de usuarios en aplicaciones.
- Parametrización de seguridad de contraseñas en la aplicación BPAC.
- Administración de respaldos del sistema BPAC.
- Actualizaciones del sistema operativo de servidores.
- Procedimiento de seguridad de accesos.
- Manuales, políticas y procedimientos del área de tecnología.