Compañía Nacional de Fuerza y Luz, S.A.

(Una institución del Gobierno de Costa Rica)

Carta a la Gerencia – Tecnología de Información

31 de diciembre del 2019

KPMG
27 de abril del 2020
Esta carta a la gerencia contiene 11 páginas
Ref/ kmc, msr

KPMG, S. A.
Edificio KPMG
San Rafael de Escazú
Costa Rica
+506 2201 4100

Confidencial
Sr. Victor Solís
Gerente General
Compañía Nacional de Fuerza y Luz, S.A.
San José, Costa Rica

27 de abril del 2020

Estimado Sr. Victor Solís

Hemos concluido la auditoria de los estados financieros de la Compañía Nacional de Fuerza y Luz, S.A., (en adelante "la Compañía") al 31 de diciembre del 2019 y por el año que termina en esa fecha.

Al planificar y efectuar la auditoría de los estados financieros mencionados hemos considerado la estructura de control interno de la Compañía con el propósito de diseñar los procedimientos de auditoría que son necesarios en las circunstancias, pero no con el propósito de expresar una opinión sobre la efectividad del control interno. Por lo tanto no expresamos una opinión sobre la efectividad del control interno de la Compañía.

Debido a lo anterior pueden existir deficiencias de control inclusive significativas, que no hayan sido detectadas por el auditor durante el transcurso de la auditoría.

Sin embargo, como resultado de nuestro trabajo determinamos algunas deficiencias de control interno que consideramos son asuntos que se deben informar, según lo requieren las normas profesionales. Las Normas Internacionales de Auditoría clasifican las deficiencias de control en dos categorías, las deficiencias de control interno y las deficiencias significativas de control interno.

Una deficiencia de control interno existe cuando un control es diseñado, implementado u operado de tal forma que no previene, detecta o corrige los errores en los estados financieros de una manera oportuna. También existe cuando no existe el control interno necesario para prevenir, detectar o corregir errores en los estados financieros de una manera oportuna.

Una deficiencia significativa de control interno es una deficiencia o combinación de deficiencias de control interno que de acuerdo al juicio profesional del auditor es de suficiente importancia que amerita la atención de aquellas personas encargadas del gobierno de la Compañía. Una deficiencia puede ser significativa no solo por la magnitud del error que ya haya ocurrido, sino también por la probabilidad de que el error ocurra en el futuro y su magnitud potencial.

Para facilitar su lectura, este informe se ha estructurado de la forma siguiente:

Anexo I Hallazgos determinados durante el proceso de auditoría financiera para el período 2019

Anexo II Seguimiento de los hallazgos determinados durante el proceso de auditoría financiera de años anteriores.

Este informe fue discutido en forma de borrador con funcionarios de la Gerencia Financiera de la Compañía.

Este informe es solamente para información y uso del Consejo Directivo, Comité de Auditoría y de la Gerencia de la Compañía y no debe ser usado para propósito adicional alguno. Si la Gerencia tiene alguna observación con respecto al contenido de esta carta tendremos mucho gusto en ampliar cualquier aspecto a su solicitud.

Atentamente

Rodrigo Ramírez.
Socio

Timbre de ¢25 de Ley No. 6663
adherido y cancelado en el original

Cc: Sr. Mauricio Villalobos Campos
Sr. Luis Villegas Carpio

COMPAÑÍA NACIONAL DE FUERZA Y LUZ, S.A.

Índice de contenidos

Anexo I

Hallazgos determinados durante evaluación de controles de tecnología de información 2019

1. Controles Generales de Tecnología de Información (GITC)

Acceso a Programas y Datos (APD)

Situación observada 1

De la revisión realizada a la lista de usuarios activos del sistema SIPROCOM, se encontraron los siguientes usuarios activos y que ya no laboran para CNFL:

Nombre Empleado	**Fecha de salida**
Ramirez Lopez German	2 de diciembre 2018
Hernandez Calderon Jose	18 de noviembre 2019
Fuentes Páz Roberto Fernando	14 de noviembre 2019
Jose Damaso Chavarria	15 de noviembre 2019
Cubillo Rivera Jose Manuel	6 de diciembre 2018
Gomez Mora Marlen	26 de marzo 2017
Padilla Porras Carlos Alberto	1 de febrero 2015
Alvarez Carvajal Henry	1 de febrero 2015
Gomez Mora Marlen	26 de marzo 2017e
Naranjo Aguilar Fernando	23 de enero 2020
Sanchez Villalobos Maria Teresa	17 de febrero 2015
Leon Vargas Alexis Alfonso	9 de octubre 2016
Orozco Azofeifa Esteban	8 de octubre 2016
Sandoval Luna Oscar	8 de octubre 2016
Valerin Sanchez Hector	22 de enero 2020
Coto Rodriguez Laura	16 de enero 2020
Rodriguez Calderon Alvaro	6 de enero 2002
Fernandez Aguero Aniceto	1 de febrero 2015
Porras Zuniga Roger	8 de febrero 2016
Campos Landergren Grettel	9 de octubre 2016
Bolivar Mendez Manuel	8 de octubre 2016
Chacon Brenes Alexander Francisco	20 de enero 2020
Cordero Duran Andrea	9 de octubre 2016
Valverde Delvo Rafael	1 de febrero 2015
Barquero Cordero Mario Alberto	9 de octubre 2016
Vargas Madrigal Veronica Vanessa	9 de octubre 2016
Castro Chacon Laura	14 de julio 2017
Cerdas Herrera Raul	26 de marzo 2016

Situación Observada 2

De la revisión realizada a la lista de usuarios activos del sistema SIPROCOM, se encontraron los siguientes usuarios duplicados:

ID USUARIO	**NOMBRE EMPLEADO**
ACORDOBA	Ana Melissa Cordoba
ANCORDOBA	Ana Melissa Cordoba
MARIASM	Arias Murillo Mario
MARIOARIAS	Arias Murillo Mario
VCHAVARRIA	Chavarria Hidalgo Vivian Alexa
VACHAVARRI	Chavarria Hidalgo Vivian Alexa
DAMARTINEZ	Daniela Maria Martinez
DMMARTINEZ	Daniela Maria Martinez
EPFERNANDE	Evelyn Priscilla Fernandez
EVFERNANDE	Evelyn Priscilla Fernandez
STGOMEZ	Gomez Robleto Steven Alberto
STEVGOMEZ	Gomez Robleto Steven Alberto
KICARRANZA	Kimberly Carranza
KKCARRANZA	Kimberly Carranza
MATREJOS	Mario Alberto Trejos
MTREJOS	Mario Alberto Trejos
PAOVIEDO	Oviedo Cordero Pablo Alexander
POVIEDO	Oviedo Cordero Pablo Alexander
YAZOFEIFA	Yuliana De Los Angel Azofeifa
YDAZOFEIFA	Yuliana De Los Angel Azofeifa

Situación Observada 3

Se determinó que tanto la administración del sistema SIPROCOM como la administración del sistema SACP Contabilidad no han definido formalmente las transacciones consideradas como críticas para cada uno de los sistemas.

Situación Observada 4

El área de Contabilidad ha establecido el documento "Procedimiento Acceso A Sacp-Contabilidad" el cual establece las pautas para asignar el acceso a roles del SACP Contabilidad e indica lo siguiente: el administrador: de SACP Contabilidad "*Recibe vía correo electrónico; para los casos de bloqueo temporal o eliminación de usuario; la solicitud de bloqueo de la jefatura respectiva.*". Sin embargo, se validó que el bloqueo de usuarios se está llevando a cabo por medio de un control automático el cual valida el estado del usuario en la base de datos de Recursos Humanos y en caso de no tener el estado de activo no permite su ingreso al sistema SACP Contabilidad

Situación Observada 5

Se determinó que la administración del sistema SIPROCOM realiza la revisión de usuarios activos e inactivos enviando un correo a cada Unidad para que los mismos validen si los usuarios a su cargo se encuentran aun laborando para CNFL, posteriormente de las respuestas obtenidas se procede a realizar las modificaciones solicitadas por la jefatura. Como resultado de la revisión se solicitó inactivar el usuario "Sanchez Villalobos Maria Teresa"; no obstante, de la revisión efectuada en el sistema se identificó que el usuario se encuentra activo.

Situación Observada 6

De la indagación realizada tanto con la administración del sistema SACP Contabilidad como con la administración del sistema SIPROCOM, se determinó que no cuentan con un documento formal donde se establezca el procedimiento para la revisión de usuarios activos e inactivos y la revisión de segregación de funciones.

Situación Observada 7

Al momento de nuestra evaluación se identificaron 11 usuarios en el sistema SACP Contabilidad los cuales dadas las características de ese sistema no tienen restricción o controles relacionados a la complejidad de sus contraseñas (longitud, caducidad, historial, entre otros). De esos usuarios 3 son administradores del sistema SACP Contabilidad, lo cual, entre otros, les permite revisar y aplicar asientos de diario; de los 3 usuarios indicados anteriormente, 2 de ellos tienen la posibilidad de cambiar sus privilegios en el sistema SACP Contabilidad, particularmente las acciones relacionadas con registro y aplicación de asientos de diario.

Finalmente, las bitácoras en las que se registra la actividad de los usuarios del sistema SACP Contabilidad son revisadas de forma reactiva por personal de CNFL.

Es importante que CNFL evalué los riesgos asociados a las brechas indicadas y evalué el costo/beneficio de implementar controles que mitiguen las situaciones identificadas.

Se detalla a continuación los usuarios descritos:

Usuario	**Nombre**	**Problema**
SILGONRI	Silvia Maria Gonzalez Rivera	Sin restricción de constraseña
REIMARBO	Reiner Antonio Martinez Bonilla	Sin restricción de constraseña
PRISCHVE	Priscila Maria Schumann Venegas	Sin restricción de constraseña, administrador, super usuario
MARSOLRO	Marcial Esteban Solis Rodriguez	Sin restricción de constraseña,
MARCECCA	Maria Ceciliano Cardenas	Sin restricción de constraseña
MARASTAL	Maricel Astua Alvarado	Sin restricción de constraseña, admnistrador

Usuario	Nombre	Problema
LUISOTPA	Luis Guillermo Sotomayor Paredes	Sin restricción de constraseña
LUIFERAR	Luis Eduardo Fernandez Arguedas	Sin restricción de constraseña, administrador, super usuario
KENVILVI	Kenneth Villalobos	Sin restricción de constraseña
FRAQUIAR	FRANKLIN QUIROS ARCE	Sin restricción de constraseña
ADRAGUAL	ADRIANA MARIA AGUILAR ALVAREZ	Sin restricción de constraseña

Operación de Computadoras (CO)

Situación Observada 8

De la indagación realizada se determinó que CNFL no realizó recuperaciones de respaldos para los sistemas bajo nuestro alcance (SACP Contabilidad y SIPROCOM) durante el periodo bajo evaluación.

2. Controles Automáticos (ITACS)

Situación Observada 9

De la revisión de la lista de usuarios con acceso al registro de las transacciones de recaudación por los servicios eléctricos en el sistema SIPROCOM se determinó que el usuario “JARTAVIA, Jose Alberto Artavia Contreras” no está autorizado para tener acceso al rol “BALPAG” el cual se utiliza para realizar cierre de cajas en el proceso de recaudación externa.

ANEXO II

Seguimiento de los hallazgos determinados durante evaluación de controles de tecnología de información de años anteriores

3. Evaluación de Controles Generales de Tecnología de Información (GITC)

Acceso a Programas y Datos (APD)

Situación observada No. 1

La Compañía cuenta con el documento "*Normas para la Seguridad de las Tecnologías de Información*" en donde se especifica que la contraseña deberá ser cambiada mínimo cada 3 meses, sin embargo, a nivel de *Active Directory* se validó que el cambio de contraseña está configurado para realizarse cada 6 meses.
Por otro lado, se validó que, también a nivel de *Active Directory*, no se cuenta con cantidad de intentos fallidos para bloquear la cuenta.

Situación actual: Se mantiene

Situación observada No. 2

A nivel del sistema SACP, cuando un nuevo colaborador solicita acceso, se validó que el sistema le asigna una clave que coincide con el usuario y no una clave dinámica, como si ocurre en el sistema SIPROCOM, por ejemplo. Sumado a ello, el sistema no obliga al cambio de contraseña al primer inicio de sesión y, aunque el Administrador del Sistema hace la recomendación al nuevo usuario que debe realizar el cambio de “password”, no existe certeza de que el mismo realice el cambio hacia a una contraseña más segura.

Situación actual: Se corrige. CNFL estableció que el ingreso al sistema SACP debe ser por medio del dominio (sistema operativo) por lo que a nivel de Active Directory si debe cambiar la clave al primer ingreso.

Situación observada No. 3

Se determinó que el documento *"Normas para el ingreso a zonas de acceso restringido, con tecnologías de información y de comunicación aplicada"* el cual pretende garantizar la protección y seguridad de equipos tales cómo Sala de Cómputo, Sala de Equipo de Comunicación, Sala de Servidores, Nodos, Dato teca, Centro de Control, por mencionar algunos, no ha sido actualizado desde el 2015.

Situación actual: Se corrige. Se realiza revisión del documento "Normas para el ingreso a zonas de acceso restringido, con tecnologías de información y de comunicación aplicada" en junio 2019,

Situación Observada No. 4

Se determinó que la Política de Seguridad de la Información no ha sido revisada ni actualizada desde Marzo del año 2010.

Situación actual: Se corrige. CNFL ha establecido el documento “Política de Seguridad de la Información de la CNFL” la cual fue aprobada en marzo 2019

Situación Observada No. 5

Se determinó que durante el periodo bajo auditoría, la Compañía no ha llevo a cabo una revisión de la segregación de funciones y de usuarios activos e inactivos, que permita identificar conflictos en los roles asignados y/o accesos otorgados.

Situación actual: Se corrige. Tanto la administración de SIPROCOM como la administración de SACP Contabilidad llevó a cabo revisión de la segregación de funciones y de usuarios activos e inactivos durante el periodo bajo evaluación.

Situación Observada No. 6

Se identificó que para el Sistema SACP, no se han establecido reglas de administración de contraseñas, por ejemplo: tamaño, caducidad, complejidad de la contraseña.

Situación actual: Se corrige. CNFL estableció que el ingreso al sistema SACP debe ser por medio del dominio (sistema operativo) por lo que las reglas de administración de contraseñas estarán determinadas por lo establecido en el Active Directory.

<u>Operación de Computadoras (CO)</u>

Situación observada No. 7

Se determinó que CNFL no cuenta con manuales o guías de trabajo para la ejecución de los procesos de Mayorización y Cierre Contable (sistema SACP) los cuales contengan, al menos, las pautas a seguir para la ejecución de ambos procesos así como el procedimiento a seguir en caso de que los mismos fallen durante su ejecución.

Situación actual: Se corrige. Se presenta el Manual de usuario del sistema donde se establece la guía de trabajo para la ejecución de los procesos de Mayorización y Cierre Contable en el sistema SACP Contabilidad.

Situación observada No. 8

CNFL cuenta con el documento *"Plan de Respaldos"* donde se indica que los respaldos realizados de lunes a viernes son de tipo incremental, sin embargo, se validaron las siguientes políticas:

— pro_sv_ora_siprocom_diario_R (servidor pc21dbp08, SIPROCOM)

— pro_vmx_dbp_oracle_diario (servidor sporassa1, SACP)

En las cuales se especifica que los respaldos son diarios (Lunes a Domingo en el caso del servidor pc21dbp08 y Lunes a Sábado para el servidor sporassa1) y que son de tipo "Full Backup", por lo cual, el plan de respaldos referido anteriormente no se encuentra alineado con los procesos que se llevan a cabo en la generación de respaldos; adicionalmente, el plan se encuentra desactualizado desde el 2011.

Situación actual: Se corrige. CNFL ha establecido el documento “Plan de Respaldo” el cual fue aprobado en noviembre 2019.

Situación observada No. 9

Se determinó que el documento *"Trámite para la atención de averías de servicios de internet, infraestructura y sistemas de información"* en el cual se especifica el procedimiento a seguir para la atención de incidentes, se encuentra desactualizado desde el 2015.

Situación actual: Se corrige. CNFL ha establecido una actualización del documento “Trámite para la atención de incidentes de los servicios de TIC” el cual fue aprobado en octubre 2019.