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

To	Mario Venegas, Jefe de Unidad de Tecnologías de Información y comunicación.	**From**	Abigail Urbina, Asistente Auditoría
Organization	Compañía Nacional de Fuerza y Luz S.A.	**Department**	IT Audit
Telephone	+ 506 2284-8022	**Telephone**	+506 2201 4299 +506 2201 4216
Fax	+ 506 2257-2398	**Fax**	+506 2201 4141 +506 2201 4131
Copy to	Ledy Herrera, Supervisora Auditoría Angélica Sánchez, Manager IT Audit	**Email**	abigailurbina@kpmg.com
		Ref.	AUG
Date	28 de abril de 2023	**Page 1 of**	**6**

Subject **Resultado de la Evaluación de Controles de Tecnología de Información 2022.**

Estimado señor Venegas:

En relación con nuestra Evaluación de Controles de Tecnología de Información para la **Compañía Nacional de Fuerza y Luz S.A,** de ahora en adelante llamado CNFL, le detallo a continuación el seguimiento de las oportunidades de mejora identificadas en periodos anteriores.

En caso de que se tenga alguna observación, favor tramitarla lo más pronto posible y si es de su aceptación, le solicito me lo indique para posteriormente enviar el documento a nuestro equipo de Auditoría de KPMG para que haga el envío formal del mismo.

Le agradezco sus atenciones y quedo a su disposición para aclarar cualquier aspecto relacionado con la presente o cualquier otro que considere conveniente.

Gracias.

Anexo I

1. Controles Generales de Tecnología de Información

1.1. Acceso a Programas y Datos

Situación Observada 1.

Con relación a los procedimientos de administración de accesos en general:

A pesar de que la Compañía dispone de procedimientos para la administración de accesos a los sistemas SACP y SIPROCOM, en los cuales se considera la autorización de los accesos por parte de las jefaturas involucradas, se identificó que no dispone de una matriz de roles por perfiles, en la que se establezcan los derechos de acceso asociados a cada cargo definido en su estructura organizativa; por lo que en caso de no recibir el detalle de los accesos autorizados, estos se otorgan, utilizando como base a usuarios con cargos homólogos (asignación de roles por referencia y/o clones) o, con base en la experiencia de los administradores de los sistemas o, en el caso de SACP, con base en un documento de referencia que, pese a no ser de carácter formal, tradicionalmente ha servido de apoyo en la ejecución de esta actividad.
No obstante, la Compañía dispone de procedimientos formales de monitoreo y/o revisiones periódicas de acceso, considerando usuarios activos, inactivos y segregación de funciones, los cuales permiten detectar y corregir desviaciones en los accesos otorgados a usuarios, actuando como elemento mitigante del riesgo asociado. Estos procedimientos fueron contemplados dentro del alcance de auditoría y, en el caso específico de SACP, se concluyeron como satisfactorios.

Situación Actual:

Se corrige.

La entidad desarrolló una matriz de roles por perfiles definidos en el sistema SIPROCOM, la cual permite identificar los derechos de acceso asociados a cada cargo.

Situación Observada 2.

Con relación a los procedimientos de administración de accesos en SIPROCOM:

Para una muestra de 15 cuentas de usuarios creadas en el sistema SIPROCOM durante el período auditado, se identificó:

- Dos cuentas de usuarios para las cuales no se obtuvo el soporte de autorización de accesos
- Once cuentas de usuarios que en su solicitud no contienen el detalle de todos los accesos otorgados.

Adicionalmente, para una muestra de 25 cuentas de usuarios modificadas en el sistema SIPROCOM durante el período auditado, se identificó:

- Diecinueve cuentas de usuarios para las cuales no se obtuvo el soporte de autorización de accesos
- Dos cuentas de usuarios que en su solicitud no contienen el detalle de todos los accesos otorgados.

Con relación a los procedimientos de administración de accesos en SIPROCOM, las solicitudes de creación/modificación que se obtuvieron en nuestras muestras están aprobadas por las jefaturas correspondientes; sin embargo, la creación/modificación de usuarios se realiza basados en cargos homólogos/clones.

Además, para una muestra de 10 cuentas de usuarios creadas en el sistema SIPROCOM durante el período auditado, se identificó dos cuentas de usuarios para las cuales no se indica el detalle de accesos/roles a asignar.

Situación Actual:

Se corrige.

De la muestra seleccionada se determinó que todas las cuentas de usuario contaban con el soporte de autorización y el detalle de los accesos otorgados.

Situación Observada 3.

Con relación a los mecanismos de identificación y autenticación:

Se identificaron 87 cuentas de usuarios duplicadas en el sistema SIPROCOM, correspondientes a 42 empleados de la Compañía. De igual manera, se determinó que existen 15 cuentas de usuarios genéricas en el sistema SIPROCOM, cuyo estatus permanece activo, de las cuales cuatro contaron con acceso durante el período auditado.

Se identificó que no hay cuentas duplicadas activas en el sistema SIPROCOM. No obstante, se determinó que existen 5 cuentas de usuarios genéricas en el sistema, cuyo estatus permanece activo, dichas cuentas contaron con acceso durante el período auditado.
Según indica la Administración de SIPROCOM, las cuentas genéricas activas no se pueden desactivar ya que tendrían implicaciones importantes en la operatividad y funcionalidad del Sistema; sin embargo, se identificó que el usuario genérico CONGEN05, se encuentra en estado activo y su última conexión fue 11/05/2021. Según comentarios de la Administración dicho usuario estará inactivo y se activará únicamente cuando se requiera realizar consultas o servicios al sistema.

Situación Actual:

Se corrige.

Se determinó que el usuario CONGEN05 fue eliminado del sistema. SIPROCOM para el periodo 2022.

Situación Observada 4.

Con relación a los procedimientos de monitoreo y/o revisión de accesos en el sistema SIPROCOM:

Se identificó que la Compañía realizó las actividades de revisión de usuarios activos, inactivos y segregación de funciones en el sistema SIPROCOM, enviando la información pertinente a las distintas Sucursales, las cuales realizaron sus observaciones sobre las acciones a ser implementadas.

No obstante, para una muestra de dos Sucursales en las cuales se efectuó este procedimiento, se identificó que para la Sucursal Guadalupe las acciones propuestas por la Sucursal no fueron aplicadas por los administradores del sistema, de conformidad con lo establecido en los procedimientos de la Compañía.

Adicionalmente, los administradores del sistema no mantienen documentación formal sobre los cambios aplicados en los accesos al sistema, derivados de las acciones propuestas por las Sucursales.

Situación Actual:

Se corrige. Para el periodo 2022 la administración del sistema realizó la revisión de usuarios activos, inactivos y segregación de funciones del sistema SIPROCOM junto con los encargados de las sucursales.

Situación Observada 5

Al momento de nuestra evaluación el usuario "soptecjose" en estado “Activo” tiene acceso privilegiado a nivel del sistema operativo del servidor de base de datos SACP (sporassa1); sin embargo, al validar esos privilegios con el personal del Proceso de Dotación y Soporte a Infraestructura, se determinó que tales accesos no deben estar asignados a ese usuario.

Situación Actual:

Se corrige.

Se determinó que el usuario “soptecjose” fue deshabilitado del servidor de base de datos SACP, en el periodo 2022.

Situación Observada 6

De la revisión efectuada a nivel del sistema operativo del servidor “uno” de aplicación SIPROCOM (pc21app01), se identificaron cuatro usuarios activos del grupo Administradores, los cuales no debían tener acceso, dichos usuarios corresponden a:

- admCMA
- admCODISA
- admINRA
- Operador

Situación Actual:

Se corrige.

Se determinó que los usuarios identificados en el grupo Administradores del servidor “uno”, fueron eliminados del sistema en el periodo 2022.

Situación Observada 7

De la revisión efectuada a nivel del sistema operativo del servidor dos de aplicación SIPROCOM (pc21app02), se identificaron cinco usuarios activos del grupo Administradores, los cuales no debían tener acceso, dichos usuarios corresponden a:

- admCMA
- admCODISA
- admINRA
- Operador
- dalmeida

Situación Actual:

Se corrige.

Se verificó que los usuarios identificados en el grupo Administradores del servidor dos de aplicación SIPROCOM, fueron eliminados del sistema en el periodo 2022.

1.2.Cambios a Programas (PC)

Situación Observada 8.

Con relación al proceso de migración al ambiente de producción:

Se identificó que la Compañía dispone de servidores separados de desarrollo/pruebas y producción para la gestión de cambios en SACP y SIPROCOM. Adicionalmente, dispone de políticas y/o procedimientos formalmente establecidos para el desarrollo y actualización de fuentes en el sistema, incluyendo el alcance y las responsabilidades de los distintos funcionarios involucrados en el proceso. Además, cuenta con las herramientas SubVersion y Tortoise para el control de versiones y la gestión de las fuentes desarrolladas.

Sin embargo, según lo establecido en el documento "Gestión de mantenimiento de los sistemas de información", se identificó que la responsabilidad de formalizar los cambios ejecutados en el ambiente de producción recae en el analista que atendió el mantenimiento (desarrollador), es decir, no está contemplada la segregación de funciones entre desarrolladores y personal con acceso para pases a producción, por lo que existe el riesgo de que se realicen cambios en producción que no se encuentren autorizados y/o probados por parte de los funcionarios responsables y/o no cumplan en todos los casos con el protocolo de gestión de cambios establecido por la Compañía.

Adicionalmente, a través de las verificaciones efectuadas directamente sobre los ambientes de desarrollo/pruebas y producción de SACP y SIPROCOM, se determinó que 10 usuarios de SACP y dos usuarios de SIPROCOM, involucrados en el proceso de desarrollo de fuentes, disponen de acceso para efectuar pases a producción.

Para el sistema SIPROCOM, se identificó cambios en producción que fueron realizados e implementados por el mismo usuario, lo que evidenció que para esos casos no se realizó una correcta segregación de funciones entre desarrolladores y personal con acceso para implementar pases a producción.

Situación Actual:

Se corrige. Se determinó que los usuarios con acceso a los ambientes de desarrollo/pruebas y producción de los sistemas SACP y SIPROCOM se encuentran segregados.

Situación Observada 9.

Se identificó que los usuarios “MAMORALES” y “DARAYA” tienen acceso al usuario genérico AXISGIN, el cuál es utilizado para implementar pases al ambiente producción; sin embargo, no hay autorizaciones formales que respalden esa asignación y el acceso de esos usuarios a dicho ambiente.

Situación Actual:

Se corrige.

Se determinó que los usuarios “MAMORALES” y “DARAYA” son autorizados por la Administración para utilizar el usuario AXISGIN.

Operaciones Computarizadas (CO)

Situación Observada 10.

Se determinó que el Área de TI realiza pruebas de restauraciones de los respaldos a las bases de datos de los sistemas; sin embargo, para el sistema SIPROCOM, se identificó que no hay documentación o evidencia que respalde la ejecución de las pruebas realizadas.

Situación Actual:

Se corrige.

Se determinó que para el periodo 2022 el área de TI documentó el resultado de las pruebas de restauraciones de los respaldos a la base de datos del Sistema SIPROCOM.