KPMG, S.A.
Edificio KPMG Boulevard Multiplaza
San Rafael de Escazú, Costa Rica.

Telephone: (506) 2201-4100
Telefax: (506) 2201-4299
Internet: www.kpmg.co.cr

To	Edgar Zamora Soto, Jefe de la Unidad Tecnologías de la Información y Comunicación	From	María José Roque IT Audit
Organization	Compañía Nacional de Fuerza y Luz, S.A.	Department	IT Audit
Fax		Telephone	+506 22 01 4100
		Fax	
Copy to	Laura Soto, Gerente Senior de Auditoría Randall Mora Socio Auditoría Angélica Sanchez, Manager IT Audit	Email	mariaroque@kpmg.com
		Ref	MJRR
Date	23 Febrero 2022	page 1 of 17	

Subject **Resultado de la Evaluación Controles Generales de Tecnologías de Información periodo 2021**

Estimado señor Zamora:

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 las oportunidades de mejora que se determinaron de nuestras pruebas efectuadas en conjunto con el personal del área de Tecnología de Información y con base en la documentación aportada por esa área; así como, las identificadas en períodos anteriores.

El propósito único de este documento es validar las oportunidades de mejora identificadas durante nuestra revisión; así como, en períodos anteriores.

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

Contenido	**Anexo**
Resultado Evaluación Controles Generales de Tecnología de Información 2021	I
Seguimiento a las oportunidades de mejora de auditoría del período anterior.	II

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

Resultado Evaluación Controles Generales de Tecnologías de Información 2021

1. Controles Generales de TI (GITC)

1.1 Acceso a Programas y Datos (APD)

Situación Observada 1

- 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 Observada 2

- 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 Observada 3

- 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

Recomendación:
Es importante implementar procesos formalmente documentados y ejecutarlos de forma consistente, que permitan gestionar adecuadamente la segregación de funciones en los diferentes componentes de la infraestructura de Tecnología de CNFL; así como contar con las apropiadas aprobaciones de los accesos otorgados.

1.2 Operaciones Computarizadas (CO)

Situación Observada 4

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.

Recomendación:
Documentar adecuadamente las pruebas de restauraciones de los respaldos a las bases de datos del sistema SIPROCOM, con el fin de validar que los datos sean íntegros y exactos, además de evidenciar la ejecución de dichas pruebas.

1.3 Cambios a Programas (PC)

Situación Observada 5

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.

Recomendación:
Normar el proceso de pases a producción, indicando; entre otros, las personas o puestos autorizados para ejecutar cambios en dicho ambiente. Además, documentar las excepciones surgidas de ejecutar cambios de urgencia y dichas excepciones deben contar con autorización formal para evidenciar quién aprobó la implementación de ese cambio en el ambiente de producción.

Anexo II

Seguimiento a situaciones informadas en el período anterior

2. Controles Generales de TI (GITC)

2.1 Acceso a Programas y Datos (APD)

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.

Derivado de lo anterior, y con relación a los procedimientos de administración de accesos en SACP, se observó lo siguiente:

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

- Seis cuentas de usuarios para las cuales no fue posible validar que los accesos otorgados corresponden con lo observado en la evidencia de solicitud y autorización de sus respectivas jefaturas.

Usuario	Empleado
GISLOPSA	21401: GISELLA LOPEZ SANCHEZ
KATMORPA	17927: KATTIA ALEJANDRA MORA PANIAGUA
ROXSANGA	33709: ROXANA SANCHEZ GARCIA
SONQUEGO	20464: SONIA QUESADA GONZALEZ
JORAGUMA	23170: JORGE ARTURO AGUIRRE MARCHENA
MELALVCA	34051: MELISSA ALVAREZ CASTILLO

- Una cuenta de usuario cuya evidencia suministrada no corresponde a la aprobación de los accesos otorgados.

Usuario	Empleado
HENSALVI	24893: HENRY SALAZAR VINDAS

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 parcialmente:** Se determinó que para el sistema SACP se cuenta con una guía de roles por perfil; en la que se establecen los derechos de acceso asociados a cada cargo definido en su estructura organizativa. No obstante, para el sistema SIPROCOM no se ha formalizado dicha guía; 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).

Recomendación:
Continuar con el proceso de oficialización de la matriz de roles por perfiles para el sistema SIPROCOM.

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

Usuario	Empleado
EXOMS	USUARIO PARA GENERAR AVERIAS OM
MANMONTERO	MONTERO CHACON MANUEL ANTONIO

- 11 cuentas de usuarios que en su solicitud no contienen el detalle de todos los accesos otorgados.

Usuario	Empleado
DATORRES	TORRES WARD DANIELA SOFIA
DCORRALES	CORRALES ALVARADO DAVID GUILLER
JAGOMEZ	GOMEZ RIVAS JOSE ANDRES
JCHAVEZ	CHAVEZ TORRES JOCELYN JANNINE
JJGONZALEZ	GONZALEZ MADRIGAL JAFETH
JMORALES	MORALES CESPEDES JOSE
JOSAGUILAR	AGUILAR GONZALEZ JOSE
NAMENDEZ	MORALES MENDEZ NATALI
OMTORRES	TORRES LEAL OMAR IVAN
VBOLANOS	BOLANOS CERDAS VERONICA MARCEL 1
WGPADILLA	PADILLA ALPIZAR WILLIAN GERARDO

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

- 19 cuentas de usuarios para las cuales no se obtuvo el soporte de autorización de accesos

Usuario	Empleado
ALMARIN	MARIN CAMPOS ALEX RODOLFO
CPORRAS	PORRAS CALVO CARLOS ENRIQUE

Usuario	Empleado
DLEAL	LEAL VALLEJOS LUIS DIEGO
EALVAREZ	ALVAREZ LEPIZ EDUARDO SIMON
EGUZMAN	GUZMAN SANCHEZ ESTEBAN
FRHIDALGO	HIDALGO VIQUEZ FRANKLIN
GEVARGAS	VARGAS CASTILLO GERARDO
GGODINEZ	GODINEZ ARGUEDAS LUIS GUSTAVO
HICHAVES	CHAVES ARROYO HILARY
JECESPEDES	CESPEDES VASQUEZ JENNIFER MARIA
JMUNIZ	MUÑIZ UMAÑA JUAN LUIS
LUDIAZ	DIAZ SANDOVAL LUIS ANGEL
MLUNA	LUNA CHINCHILLA MARIO ALBERTO
PBARAHONA	BARAHONA CONEJO ADELIA PATRICIA
ROGONZALE	GONZALEZ SOLIS ROGER ALONSO
SBRAVO	BRAVO CHAVES SILVANA MARIA
WCHAVES	CHAVES SIBAJA WALTER EDUARDO
WGUILLEN	GUILLEN MORALES WILLIAM
YGUTIERREZ	GUTIERREZ SANCHEZ YORLENY

- Dos cuentas de usuarios que en su solicitud no contienen el detalle de todos los accesos otorgados.

Usuario	Empleado
FARAUZ	ARAUZ STERLING FRANCISCO GERARDO
JOMONGE	MONGE ALVARADO JORGE PAULO

***Situación actual*: Se corrige parcialmente:** 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.

ID trámite	Empleado
112592078	Kimberly Pamela Sanchez Rodriguez
112547184	Daniela Maria Castillo Fonseca

Recomendación:
Debe implementarse un proceso formalmente documentado, que permita gestionar adecuadamente la creación, modificación y eliminación de usuarios en el sistema SIPROCOM. Además, documentar todo datos requerido relacionado con la asignación de roles y evaluar el costo/beneficio de mejorar el procedimiento de asignación de roles/privilegios sustentados en cuentas homologadas/clones.

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.

Usuarios duplicados SIPROCOM:

Usuario	Empleado
CANCHIAB	ANCHIA BRENES CINDY
CANCHIA	ANCHIA BRENES CINDY
ACALVO	ANDRES ESTEBAN CALVO
ANCALVO	ANDRES ESTEBAN CALVO

Usuario	Empleado
AFONSECA	ANGELICA MARIA FONSECA
ANFONSECA	ANGELICA MARIA FONSECA
DANGULO	ANGULO VELASQUEZ DAVID ALBERTO
DAVNGULO	ANGULO VELASQUEZ DAVID ALBERTO
MARIASM	ARIAS MURILLO MARIO
MARIOARIAS	ARIAS MURILLO MARIO
LIARIAS	ARIAS SANCHEZ LIBORIO
LIBARIAS	ARIAS SANCHEZ LIBORIO
AXISMIGRA	AXIS YOVERI
AXISCONF	AXIS YOVERI
AECHAVARRI	CHAVARRIA AZOFEIFA ARMANDO ESTE
ARCHAVARR	CHAVARRIA AZOFEIFA ARMANDO ESTE
VACHAVARRI	CHAVARRIA HIDALGO VIVIAN ALEXA

VCHAVARRIA	CHAVARRIA HIDALGO VIVIAN ALEXA
CHQUESADA	CHRISTOPHER QUESADA
CQUESADA	CHRISTOPHER QUESADA
WTORU\O	COPIA - NO UTILIZAR
WTORUÑO	COPIA - NO UTILIZAR
ADMGEDA	COPIA DEL USUARIO: ADMESAY2
AGESDA	COPIA DEL USUARIO: ADMESAY2
JECORDERO	CORDERO CASCANTE JEREMY JOSE
JJCORDERO	CORDERO CASCANTE JEREMY JOSE
GACOTO	COTO ROJAS GUILLERMO ARTURO
G	COTO ROJAS GUILLERMO ARTURO
GU	COTO ROJAS GUILLERMO ARTURO
RCRAWFORD	CRAWFORD QUESADA ROBII
ROCRAWFORD	CRAWFORD QUESADA ROBII
AGONZAGA	GONZAGA GRANADOS ALLAN JOSE
ALGONZAGA	GONZAGA GRANADOS ALLAN JOSE
GCARPIO	GUSTAVO ALONSO CARPIO
GUCARPIO	GUSTAVO ALONSO CARPIO
HBARQUERO	HELIO BERNARDO BARQUERO
HEBARQUERO	HELIO BERNARDO BARQUERO
DAHERNANDE	HERNANDEZ BENAVIDES DAVID
DHERNANDEZ	HERNANDEZ BENAVIDES DAVID
LUIHERRERA	HERRERA QUESADA LUIS ALFREDO
LAHERRERA	HERRERA QUESADA LUIS ALFREDO
OMHERRERA	HERRERA VARGAS OMAR
OHERRERA	HERRERA VARGAS OMAR

Usuario	**Empleado**
KITREJOS	KIMBERLIN JHOY TREJOS
KJTREJOS	KIMBERLIN JHOY TREJOS
EDLOPEZ	LOPEZ SAENZ EDWIN ESTEBAN
ELOPEZ	LOPEZ SAENZ EDWIN ESTEBAN
JEMARTINEZ	MARTINEZ SERRANO JEFFRY JESUS
JMARTINEZ	MARTINEZ SERRANO JEFFRY JESUS
KEMEZA	MEZA ARIAS KEVIN
KMEZA	MEZA ARIAS KEVIN
ALMONGE	MONGE JIMENEZ ALBERTO RICARDO
AMONGE	MONGE JIMENEZ ALBERTO RICARDO
IAMOYA	MOYA ACHOY ISAAC ANDRES
IMOYA	MOYA ACHOY ISAAC ANDRES
VMURILLO	MURILLO CAMPOS VICTOR MANUEL
VICMURILLO	MURILLO CAMPOS VICTOR MANUEL
AMONTERO	NO USAR

DRAMIREZVA	NO USAR
PRUEBA	NO USAR
PAOVIEDO	OVIEDO CORDERO PABLO ALEXANDER
POVIEDO	OVIEDO CORDERO PABLO ALEXANDER
VRODRIGUEZ	RODRIGUEZ VALVERDE VICTORIA EUG
VIRODRIGUE	RODRIGUEZ VALVERDE VICTORIA EUG
DIEGOROJAS	ROJAS MARIN DIEGO ANDRES
DROJASM	ROJAS MARIN DIEGO ANDRES
ROBADILLA	RONALD (SEG Y VIG) BADILLA
RBADILLA	RONALD (SEG Y VIG) BADILLA
JOSANCHEZ	SANCHEZ LOBO JOSHUA STEVEN
SSANCHEZ	SANCHEZ LOBO JOSHUA STEVEN
SFERNANDEZ	SOFIA VALERIA FERNANDEZ
SOFERNANDE	SOFIA VALERIA FERNANDEZ
MARTREJOS	TREJOS UGALDE MARIO ALBERTO
MATREJOS	TREJOS UGALDE MARIO ALBERTO
LVENEGAS	VENEGAS HERRERA LUIS ALLAN
LAVENEGAS	VENEGAS HERRERA LUIS ALLAN
DIAVILLALO	VILLALOBOS VEGA DIANA ANTONIETA
D	VILLALOBOS VEGA DIANA ANTONIETA
OSVINDAS	VINDAS BONILLA OSVALDO JAVIER
OVINDAS	VINDAS BONILLA OSVALDO JAVIER
YPEÑA	YORLENY MARIA PEÑA MUÑOZ
YPEÑAM	YORLENY MARIA PEÑA MUÑOZ

Usuario	**Empleado**
YAZOFEIFA	YULIANA DE LOS ANGEL AZOFEIFA
YDAZOFEIFA	YULIANA DE LOS ANGEL AZOFEIFA
YUAZOFEIFA	YULIANA DE LOS ANGEL AZOFEIFA
MILZUNIGA	ZUÑIGA GOMEZ MILTON
MILZUÑIGA	ZUÑIGA GOMEZ MILTON

Usuarios Genéricos SIPROCOM:

Usuario	**Empleado**
AXISCNFL	AXISCNFL
AXISREPORT	AXIS REPORTES
EXAXIS3I	USUARIO DE INTERFAZ DE COMUNICAC
EXINTRANET	USUARIO INTRANET
EXPORTAL	USUARIO PORTAL
AXISCONF	AXIS YOVERI
EXSIFRAS	USUARIO SIFRAS
ANALISTAS	COPIA DEL USUARIO: AXISGIN

AXISGIN	USUARIO APLICACION GIN
STMONITOR	ST MONITOR
ESREGU	COPIA DEL USUARIO: NRAMIREZ
ADMSPROCOM	ADMINISTRACION SIPROCOM
CONGEN05	USUARIO CONSULTAS GENERALES 05
EXOMS	USUARIO PARA GENERAR AVERIAS OM
EXST	USUARIO SERVIDOR DE TRANSACCION

Adicionalmente, se identificó que los sistemas SACP y SIPROCOM permiten la posibilidad de multisesiones, en las que un ID de usuario específico puede permanecer conectado a los sistemas simultáneamente y desde terminales diferentes.

***Situación actual*: Se corrige parcialmente:** 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.

Usuarios Genéricos SIPROCOM:

Usuario	Descripción:	Responsable:
ANALISTAS	Usuario que es utilizado por los diferentes funcionarios del Proceso Sistemas de Información Comercial cuando requieren hacer algún “debug” de un objeto de la Base de Datos de SIPROCOM en el ambiente de producción	Gustavo Prado Fallas, Proceso Sistemas de Información Comerciales Sergio Méndez Fernández, Proceso Sistemas de Información Comerciales
AXISGIN	USUARIO APLICACION GIN: utilizado por los funcionarios del Proceso Sistemas de Información Comerciales encargados de las puestas en producción en la base de datos de SIPROCOM	Gustavo Prado Fallas, Proceso Sistemas de Información Comerciales Sergio Méndez Fernández, Proceso Sistemas de Información Comerciales
ADMSPROCOM	Usuario utilizado por el Flujo de los AGD´s, para asignar a cualquiera de los Administradores una solicitud usuaria, para su análisis, posible atención y rechazo.	Andrés Hernández, Administrador del sistema SIPROCOM.
CONGEN05	USUARIO CONSULTAS GENERALES 05	Andrés Hernández, Administrador del sistema SIPROCOM.
EXOMS	Usuario que se encarga de la asignación de ordenes de averías creadas por parte del OMS para que se replique en SIPROCOM. Si no existiera no se crearían órdenes de SIPROCOM provenientes de órdenes creadas en OMS y no se podrían incluir los materiales que son solicitados como parte de los informes que van hacia la ARESEP.	Usuario default automático

Recomendación:
Evaluar el costo/beneficio y riesgo de utilizar usuarios genéricos en los procesos de TI y normar aquellos requeridos, indicando; entre otros, su función y el personal responsable.

Adicionalmente con relación al usuario CONGEN05, documentar formalmente aquellos controles implementados para su administración considerando; entre otros; el proceso a seguir para la activación y desactivación, controles que permitan dar trazabilidad a las actividades realizadas con ese usuario, etc.

Situación Observada 4.

Con relación a la administración y sintaxis de contraseñas de acceso a los sistemas:

- En el Active Directory los parámetros de longitud, caducidad e intentos fallidos sugieren oportunidades de mejora con relación a los parámetros de referencia, con base en las prácticas más comunes en seguridad de la información. En concreto:

  Longitud = 6 caracteres
  Caducidad = 365 días
  Intentos fallidos = 0 intentos

- De igual manera, dado que el acceso al sistema SACP para los usuarios funcionales (no administradores) se encuentra vinculado con las credenciales del dominio, se sugiere la misma conclusión sobre los parámetros de contraseñas configurados para el Active Directory.

- En el sistema SIPROCOM, se determinó que los parámetros de longitud y complejidad sugieren oportunidades de mejora con relación a los parámetros de referencia, con base en las prácticas más comunes en seguridad de la información. En concreto:

  Longitud = 6 caracteres
  Complejidad = Caracteres numéricos y alfabéticos (mayúsculas o minúsculas, no ambos). No considera caracteres especiales.

  ***Situación actual*: Se corrige:** Se identificó lo siguiente:

- En el Active Directory los parámetros de longitud (6 caracteres), caducidad (180 días) y para intentos fallidos hay una Política de bloqueo adicional que aplica a grupos identificados configurada en 3 intentos. Con respecto a la política Domain Policy, está aplica a cuentas genéricas identificadas, que por su funcionalidad no se pueden bloquear.

- Para el sistema SACP, se obtiene la misma conclusión sobre los parámetros de contraseñas configurados para el Active Directory.

- En el sistema SIPROCOM, se determinó que los parámetros de longitud (6 caracteres) y complejidad (solo recibe contraseñas en mayúscula) están definidos en el código fuente del sistema.

Situación Observada 5.

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 mantiene:** Se identificó para la muestra correspondiente a la Sucursal Guadalupe, que las acciones propuestas por la misma no fueron aplicadas por los administradores del sistema, de conformidad con lo establecido en los procedimientos de la Compañía. Se validó que 3 usuarios se mantienen activos.

Recomendación:
Debe implementarse un proceso formalmente documentado, que permita gestionar adecuadamente la revisión y segregación de funciones de los usuarios de los diferentes aplicativos de CNFL y aplicarse de forma consistente.

Situación Observada 6.

Con relación a los usuarios con privilegios especiales en los sistemas:

Los privilegios de amplio acceso sobre los sistemas operativos de los servidores de base de datos y aplicación de SACP y SIPROCOM, así como de sus bases de datos; se encuentran restringidos al personal del Proceso de Dotación y Soporte a Infraestructura y a los usuarios administradores del dominio, de conformidad con sus responsabilidades, sin embargo, se identificó que se utilizan cuentas de usuarios genéricas de uso compartido para llevar a cabo la administración de esta plataforma.

Por otra parte, se identificó una cuenta de usuario “questadmin” no autorizada, con privilegios de amplio acceso en el servidor de aplicación de SACP (PC21VOASSACP). Se determinó que este usuario se utilizó para la administración de la herramienta Foglight, actualmente no operativa en la Compañía.

Además, se identificó una cuenta de usuario “SPLEX_ROLE_BOTH” no autorizada, con privilegios de amplio acceso en la base de datos de SIPROCOM (PROCOM). Se determinó que este usuario se utilizó como parte del proyecto de implementación de la aplicación SharePlex para replicar bases de datos. No obstante, el proyecto resultó cancelado.

De igual manera, se identificó que las cuentas de usuario por defecto SYS y SYSTEM de la base de datos, las cuales conceden privilegios de amplio acceso especiales, permanecen activas y son utilizadas de forma recurrente y compartida por parte del personal del Proceso de Dotación y Soporte a Infraestructura.

Adicionalmente, a pesar de que los sistemas SACP y SIPROCOM, sus bases de datos y sistemas operativos de servidores de bases de datos y aplicación disponen de bitácoras que permiten registrar el acceso y/o

actividades realizadas por los usuarios, se determinó que la Compañía no realiza revisiones formales y periódicas de estas bitácoras, de acuerdo con una frecuencia definida, a fin de efectuar el monitoreo de los usuarios con privilegios de amplio acceso.

***Situación actual*: Se corrige:**

- Se identificó que las cuentas "SPLEX_ROLE_BOTH", "questadmin" ya han sido eliminadas.

- De igual manera, se determinó que se utilizan cuentas de usuarios genéricas de uso compartido para llevar a cabo la administración de esta plataforma y para la asignación de tareas. Con respecto al uso de usuarios genéricos, se identificó que se lleva un control de estos mediante el Sistema de Gestión de Solicitudes de Incidentes (GESI) y también mediante la administración del casillero de averías para el PDSI.

- Adicionalmente, se determinó que el CNFL realiza revisiones periódicas de bitácoras; a nivel de sistemas la realizan los Administradores de sistemas y a nivel de base de datos y sistema operativo se realiza por parte del personal del Proceso de Dotación y Soporte a Infraestructura.

2.2 Cambios a Programas (PC)

Situación Observada 7.

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.

Usuarios SACP:

Usuario
Alfaro Sánchez Linette
González Rivera Silvia

Morales Barquero Fury Farid
Ovares Arce Marjorie
Saborío Cerdas Randal
Sec. Sistemas Administrativos, Calle 21
Solís Rodríguez Marcial
Sotomayor Paredes Luis Guillermo
Villalobos Villalobos Kenneth
Aguilar Álvarez Adriana

Usuarios SIPROCOM:

Usuario	**Empleado**
CNFL\gprado	Gustavo Prado
CNFL\smendez	Sergio Méndez

***Situación actual*: Se mantiene:** 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.

Detalle de los cambios:

- 50 cambios realizados e implementados por el usuario GPRADO:

CODIGO_GIN	CODIGO_GIN	CODIGO_GIN	CODIGO_GIN
GIN-PRO-GPF-2030	GIN-PRO-GPF-2047	GIN-PRO-GPF-2162	GIN-PRO-GPF-2196
GIN-PRO-GPF-2031	GIN-PRO-GPF-2071	GIN-PRO-GPF-2163	GIN-PRO-GPF-2201
GIN-PRO-GPF-2032	GIN-PRO-GPF-2040	GIN-PRO-GPF-2164	GIN-PRO-GPF-2202
GIN-PRO-GPF-2070	GIN-PRO-GPF-2110	GIN-PRO-GPF-2165	GIN-PRO-GPF-2203
GIN-PRO-GPF-2078	GIN-PRO-GPF-2111	GIN-PRO-GPF-2166	GIN-PRO-GPF-2204
GIN-PRO-GPF-2079	GIN-PRO-GPF-2075	GIN-PRO-GPF-2167	
GIN-PRO-GPF-2081	GIN-PRO-GPF-2076	GIN-PRO-GPF-2159	
GIN-PRO-GPF-2146	GIN-PRO-GPF-2077	GIN-PRO-GPF-2160	
GIN-PRO-GPF-2056	GIN-PRO-GPF-2123	GIN-PRO-GPF-2153	
GIN-PRO-GPF-2095	GIN-PRO-GPF-2124	GIN-PRO-GPF-2154	
GIN-PRO-GPF-2096	GIN-PRO-GPF-2072	GIN-PRO-GPF-2155	
GIN-PRO-GPF-2143	GIN-PRO-GPF-2073	GIN-PRO-GPF-2156	
GIN-PRO-GPF-2144	GIN-PRO-GPF-2074	GIN-PRO-GPF-2183	
GIN-PRO-GPF-2145	GIN-PRO-GPF-2135	GIN-PRO-GPF-2157	
GIN-PRO-GPF-2046	GIN-PRO-GPF-2161	GIN-PRO-GPF-2158	

- 13 cambios realizados e implementados por el usuario SMENDEZ:

CODIGO_GIN
GIN-PRO-SME-674
GIN-PRO-SME-675
GIN-PRO-SME-682
GIN-PRO-SME-681
GIN-PRO-SME-676
GIN-PRO-SME-677
GIN-PRO-SME-678
GIN-PRO-SME-683
GIN-PRO-SME-684
GIN-PRO-SME-680
GIN-PRO-SME-688
GIN-PRO-SME-685
GIN-PRO-SME-687

- 24 cambios realizados e implementados por el usuario MAMORALES:

CODIGO_GIN
GIN-PRO-MMR-935
GIN-PRO-MMR-919
GIN-PRO-MMR-920
GIN-PRO-MMR-927
GIN-PRO-MMR-936
GIN-PRO-MMR-930
GIN-PRO-MMR-931
GIN-PRO-MMR-925
GIN-PRO-MMR-962
GIN-PRO-MMR-988
GIN-PRO-MMR-957
GIN-PRO-MMR-958
GIN-PRO-MMR-987
GIN-PRO-MMR-959
GIN-PRO-MMR-960
GIN-PRO-MMR-970
GIN-PRO-MMR-942
GIN-PRO-MMR-945
GIN-PRO-MMR-952
GIN-PRO-MMR-953
GIN-PRO-MMR-955
GIN-PRO-MMR-943
GIN-PRO-MMR-1002
GIN-PRO-MMR-1011

- 3 cambios realizados e implementados por el usuario DARAYA:

CODIGO_GIN
GIN-PRO-DAC-324
GIN-PRO-DAC-325
GIN-PRO-DAC-339

Recomendación:
Restringir los usuarios con acceso a implementar cambios en producción, con el fin de realizar una adecuada segregación de funciones y evitar que una misma persona realice e implemente un cambio en producción.

2.3 Operaciones Computarizadas (CO)

Situación Observada 8.

Con relación a los procedimientos de respaldo y recuperación:

A pesar de que la Compañía realiza pruebas de restauraciones de los respaldos de las bases de datos de los sistemas SACP y SIPROCOM, de acuerdo con una frecuencia formalmente definida, estos procedimientos se realizan solo por el personal del Proceso de Dotación y Soporte a Infraestructura, sin considerar la certificación de las áreas funcionales sobre el funcionamiento de los módulos y las verificaciones de integridad y exactitud de los registros asociados a la preparación de sus estados financieros.

***Situación actual*: Se corrige:** Se identificó que el área de Proceso de Dotación y Soporte a Infraestructura realiza un proceso el cual toma en cuenta las áreas funcionales para realizar las pruebas y verificar la funcionalidad de los módulos; así como, validar la integridad y exactitud de los registros. Dichas pruebas están a cargo de los Administradores de los Sistemas.