Crowe Horwath CR, S.A.

Compañía Nacional de Fuerza y Luz, S.A

Sistema de tecnología de información

Al 31 de diciembre de 2024

Compañía Nacional de Fuerza y Luz, S.A

Índice

Página

I. Resumen ejecutivo 3
II. Objetivo 4
III. Alcance 4
IV. Procedimientos 4
V. Valoración basada en riesgo 4
VI. Criterios de evaluación 5
VII. Determinación del cumplimiento y nivel de exposición al riesgo 6
VIII. Conclusiones generales del año 2024 7
IX. Mapa de calor de los riesgos evidenciados 8
X. Actividades evaluadas 9
A. Gestión de Tecnologías de Información 9
B. Gestión de la seguridad de la información 12
C. Gestión de riesgos de tecnologías de información 12
D. Gestión de sistemas de información 12
E. Gestión de la continuidad de negocio y TI 13
F. Seguimiento del periodo anterior 13

Crowe Horwath CR, S.A.
2442 Avenida 2
Apdo. 7108-1000
San José, Costa Rica
Tel + (506) 2221 4657
Fax + (506) 2233 8072
www.crowe.cr

27 enero de 2025

Señores
Compañía Nacional de Fuerza y Luz, S.A
Atención: Ing. Rayner García Villalobos
Presidente
Ing. Luis Fernando Andrés Jácome,
Gerente General

ASUNTO: CARTA SOBRE CONTROLES DE TECNOLOGIA DE INFORMACION

Al revisar la gestión de Tecnología de Información de Compañía Nacional de Fuerza y Luz, S.A., como parte de la auditoría de los estados financieros al 31 de diciembre de 2024, observamos asuntos relacionados con las buenas prácticas de control de TI, sobre los cuales preparamos las conclusiones incluidas en el documento adjunto. Este informe se estructura como resultado del cumplimiento de las NIA 315 y 330; no es ni debe interpretarse como una evaluación al área de Tecnología de Información de forma específica.

Al planear y ejecutar la revisión evaluamos la estructura de control interno existente y aplicamos pruebas selectivas de cumplimiento, con el fin de determinar el alcance de los procedimientos de auditoría para expresar opinión sobre los estados financieros al 31 de diciembre de 2024, y no para opinar sobre la estructura de control interno o los sistemas de información en su conjunto. Este informe no es ni debe interpretarse como una auditoría de los sistemas de información.

Es necesario señalar que nuestra evaluación es limitada para efectos de una revisión de controles generales, por lo que una revisión más detallada de controles de aplicación podría revelar más oportunidades de mejora de las que incluye este informe.

Los temas tratados no se refieren a empleados en particular y tienen por objeto plantear medidas para fortalecer el sistema de tecnología de información.

Nuestra responsabilidad sobre este informe sobre sistema de tecnología de información al 31 diciembre de 2024 se extiende hasta el día 27 de enero de 2025. La fecha de la carta de gerencia indica al usuario, que el auditor ha considerado el efecto de los hechos y de las transacciones de los que ha tenido conocimiento y que han ocurrido hasta dicha fecha; en consecuencia, no se amplía por la referencia de la fecha en que se firme digitalmente.

Atentamente,

FABIAN ZAMORA AZOFEIFA (FIRMA)

Firmado digitalmente por FABIAN ZAMORA AZOFEIFA (FIRMA)
Fecha: 2025.02.24 18:58:06 -06'00'

Fabian Zamora Azofeifa
Socio

Nombre del CPA: FABIAN ZAMORA AZOFEIFA
Carné: 2186
Cédula: 302870450
Nombre del Cliente: Compañía Nacional de Fuerza y Luz S.A.
Identificación del cliente: 3101000046
Dirigido a: Compañía Nacional de Fuerza y Luz S.A.
Fecha: 16-02-2025 12:00:59 PM
Tipo de trabajo: Sistema de tecnología de información

Timbre de ¢25 de la Ley 6663 adherido y cancelado en el original.

FABIAN ZAMORA AZOFEIFA
Contador Público Autorizado No. 2186
COSTA RICA

COSTA RICA TIMBRE
25 COLONES 25

Código de Timbre: CPA-25-435262

c.c. Comité de Auditoría

Crowe Horwath CR, S.A.

Radiográfica Costarricense, S.A

Sistema de tecnología de información

I. Resumen ejecutivo

Como parte del trabajo de la auditoría de los estados financieros del periodo 2024 se llevó a cabo la evaluación de controles para el área de Tecnología de Información (TI), de Compañía Nacional de Fuerza y Luz, S.A (CNFL) la cual se basó en el cumplimiento de la Norma Internacional de Auditoría 315 "Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y su entorno", la Norma Internacional de Auditoría 330 "Procedimientos del auditor en respuesta a los riesgos evaluados" y marco normativo para TI y no es ni debe interpretarse como una auditoría de los sistemas de información, ni de la Jefatura de Tecnologías de Información de .

Los riesgos y recomendaciones informadas en la Carta de Gerencia Financiera con corte al 30 de junio de 2024 son vinculantes y deben ser revisados de forma integral con los resultados indicados en este informe; entre algunas:

- En proceso la digitalización de los libros legales.

- Registros contables de obras en proceso a partir del 2018 en proceso de ser capitalizables.

Las Normas vigentes y de acatamiento fueron emitidas por la Dirección de Gobernanza Digital del MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones), conforme oficio No. MICITT–DGD-OF-215-2021.

Es nuestro criterio que la identificación y gestión de los riesgos de ciberseguridad es fundamental para garantizar la confiabilidad y seguridad de la información presentada en los informes. Esto no solo protege los activos de la organización, sino que también asegura la transparencia y confianza en los procesos de toma de decisiones.

Aunque no se puede eliminar completamente el riesgo inherente de ciberseguridad, se pueden reducir sus impactos mediante una gestión efectiva de riesgos, controles robustos y un monitoreo constante. Esto es esencial para proteger los activos digitales y garantizar la continuidad del negocio. El riesgo inherente en ciberseguridad se refiere a las amenazas y vulnerabilidades propias de los entornos tecnológicos que podrían comprometer la confidencialidad, integridad y disponibilidad de la información, sin considerar las medidas de mitigación o controles existentes.

En la evaluación del área de TI se identificaron 2 observaciones del periodo 2024, que de acuerdo con la naturaleza del riesgo representa riesgo elevado.

En la sección de conclusiones de este informe se comunican los resultados.

II. Objetivo

Evaluar el cumplimiento de requerimientos de seguridad y control en Tecnología de Información (TI) en la Compañía de acuerdo con las Normas Internacionales de Auditoría 315 y 330, el marco normativo interno y las buenas prácticas de control para gobierno y control de TI.

III. Alcance

El alcance incluyó aspectos relacionados con la gestión de control y sistemas de información de la Compañía respecto a la elaboración de procedimientos y aplicación de controles que fortalezcan la seguridad, integridad, funcionalidad y precisión de los procesos de gestión del área de TI, gestión de la seguridad de la información, gestión de riesgos de TI, gestión de los sistemas de información, gestión de la continuidad y seguimiento de recomendaciones anteriores.

IV. Procedimientos

A partir del alcance se elaboraron y utilizaron instrumentos para recopilar la información referente al alcance indicado; entre estos, entrevistas, cuestionarios, revisión documental, levantamiento de minutas, selección de muestras y verificación de la funcionalidad de los sistemas.

Entre los temas evaluados en cada área se indican los hallazgos evidenciados.

V. Valoración basada en riesgo

Para determinar el nivel de riesgo al que se expone la entidad derivada del incumplimiento de aspectos normativos y/o deficiencias detectadas en el control interno, se procede a aplicar un análisis de impacto y frecuencia, que da como resultado la ubicación de este en un mapa de calor de 5x5 cuadrantes.

El riesgo puede evaluarse en términos de una combinación de frecuencia y magnitud y de acuerdo con dicha relación se concibe un nivel de exposición al riesgo y la posible medida a tomar en caso de mitigación.

VI. Criterios de evaluación

De acuerdo con la evaluación de control interno del área de TI y con base en el riesgo que representan para los recursos de TI (aplicaciones, información, infraestructura y personas), se presenta el mapa de riesgos que resume la relación entre el impacto para la organización y la posibilidad de materialización del riesgo que garanticen la alineación con los criterios de información (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad).

Los niveles de cumplimiento se describen a continuación:

Cumple	La entidad muestra desempeño adecuado respecto al factor evaluado.
Cumplimiento parcial alto	La entidad muestra algunas deficiencias, pero en general el desempeño respecto al factor evaluado es satisfactorio.
Cumplimiento parcial bajo	La entidad muestra débil desempeño respecto al factor evaluado.
No cumple	La entidad muestra desempeño crítico respecto al factor evaluado, por lo que no es aceptable clasificarlo en ninguno de los tres niveles anteriores.

Las categorías de riesgos se describen a continuación[1]:

Nivel de riesgo	Descripción
Inaceptable	Se estima que este nivel de riesgo es mucho más allá de su riesgo tolerable; cualquier riesgo que se encuentre en esta clasificación puede desencadenar una respuesta inmediata al riesgo.
Elevado	Riesgo elevado, por encima del riesgo tolerable; la entidad puede, como política interna, mitigar el riesgo u otra respuesta adecuada definida dentro de un tiempo límite.
Normal	Nivel aceptable de riesgo, por lo general sin realizar una acción en especial excepto para el mantenimiento de los actuales controles u otras respuestas.
Oportunidad	Nivel de riesgo muy bajo, en el cual las oportunidades de ahorro de costos pueden ser disminuir el grado de control o determinar en cuáles oportunidades pueden asumirse mayores riesgos.

El formato de este informe fue estructurado para proporcionar dos referencias específicas; Cumplimiento y Nivel de riesgo.

En la práctica el "apetito de riesgo" puede ser definido en términos de una combinación de frecuencia y magnitud de un riesgo descritos en bandas de significancia del riesgo. Hemos establecido niveles de riesgo en las bandas descritas anteriormente basándonos en la frecuencia y magnitud de los riesgos.

[1] Datos tomados del Manual CRISC (*Certified in Risk and Information Systems Control*), emitido por el ISACA.

La frecuencia y magnitud de los riesgos no necesariamente están directamente relacionados con niveles de cumplimiento de la normativa, debido a que, aunque haya incumplimiento, el impacto que puede ocasionar y la frecuencia de veces que puede ocurrir pueden tener efecto poco significativo en el proceso de administración integral de riesgos y en las operaciones.

VII. Determinación del cumplimiento y nivel de exposición al riesgo

Para obtener el nivel de exposición al riesgo nos hemos basado en la aplicación de una matriz de 25 cuadrantes (5 verticales y 5 horizontales), en la cual el riesgo de los factores es determinado por su ocurrencia e impacto.

Para cada acción evaluada que presenta incumplimiento hemos determinado el nivel de impacto y ocurrencia y obtuvimos el nivel de exposición al riesgo basados en la matriz indicada anteriormente.

La frecuencia (cuadrantes horizontales) se basa en la verificación de las siguientes categorías:

Muy baja	La probabilidad de ocurrencia es insignificante, puede ocurrir solo en circunstancias excepcionales.
Baja	Tiene poca probabilidad de ocurrencia; no se espera que ocurra en cierto periodo de tiempo.
Frecuente	El evento ocurrirá más de una ocasión en un determinado lapso.
Alta	Se espera que suceda en muchas ocasiones en un periodo de tiempo dado, en circunstancias definidas.
Muy alta	Se materializa de forma continua y ocurrirá bajo muchas circunstancias.

El impacto (cuadrantes verticales) se basa en las siguientes categorías:

Insignificante	El costo no afecta la entidad. No es necesario tomar medidas al respecto.
Mínimo	La materialización podría traer un costo para la entidad, sin embargo, no es de importancia para los resultados de la entidad. Debe valorarse los motivos de la materialización del riesgo.
Moderado	Su materialización conlleva un costo para la entidad que puede incluir pérdidas. Deben establecerse medidas de prevención para posibles eventos.
Serio	Representa un costo elevado. Las medidas que deben tomarse son correctivas y preventivas.
Crítico	El costo asumido no es tolerable y es necesario tomar medidas correctivas inmediatas.

A continuación, presentamos la matriz de 5 x 5 cuadrantes

Impacto	Frecuencia				
	Muy baja	**Baja**	**Frecuente**	**Alta**	**Muy alt**
Crítico	5	10	15	20	25
Serio	4	8	12	16	20
Moderado	3	6	9	12	15
Mínimo	2	4	6	8	10
Insignificante	1	2	3	4	5

Calificaciones:

Basado en los resultados de los análisis por acción se determina el nivel de exposición al riesgo de acuerdo con los siguientes rangos:

De 1 a 2:	El nivel de riesgo es de oportunidad.
De 3 a 9:	El nivel de riesgo es normal.
De 10 a 12:	El nivel de riesgo es elevado.
De 15 a 25:	El nivel de riesgo es inaceptable.

VIII. Conclusiones generales del año 2024

En cumplimiento con la NIA 260, “Comunicaciones de asuntos de auditoría con los encargados del gobierno corporativo”, el auditor tiene la responsabilidad de comunicar en una auditoría de estados financieros los hechos observados relacionados con los riesgos de TI y negocio que gestiona actualmente la administración y que son significativos y relevantes en relación con la responsabilidad de supervisión del proceso de información financiera.

Hay observaciones que han sido comunicadas sobre riesgos inherentes, financieros y de mercado en la Carta de Gerencia de la auditoría financiera que deben ser revisados de forma integral con este informe.

El riesgo inherente de ciberseguridad representa una exposición significativa y natural a las amenazas que enfrentan las organizaciones debido a la creciente dependencia de la tecnología y la conectividad digital. Este riesgo, definido por la naturaleza misma de los sistemas tecnológicos, existe independientemente de los controles implementados y afecta directamente la confidencialidad, integridad y disponibilidad de los datos y sistemas, motivo por el cual es inevitable pero gestionable. Requiere un enfoque proactivo y estratégico para proteger los activos tecnológicos y garantizar la resiliencia organizacional frente a las amenazas emergentes.

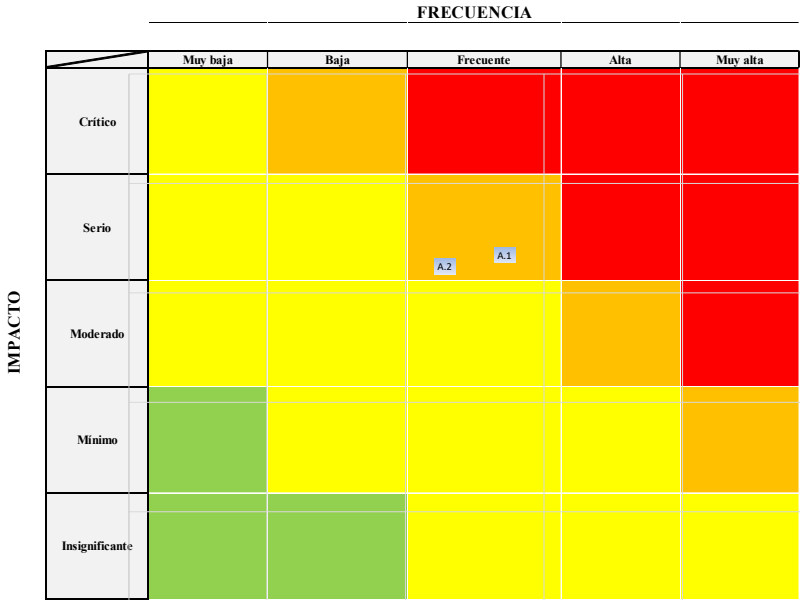
Como auditores, nuestra función es asegurar que este riesgo sea comprendido, cuantificado y abordado con medidas efectivas que reduzcan su impacto en las operaciones y objetivos estratégicos de la organización.

Observaciones del periodo 2024

Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
A.1	Plan Estratégico de Tecnología de Información	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
A.2	Actas del Comité de Tecnología de Información	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

IX. Mapa de calor de los riesgos evidenciados

De acuerdo con nuestra revisión y a la metodología de calificación del nivel de exposición al riesgo, presentamos a continuación la matriz de 25 cuadrantes donde se resume de manera gráfica, las observaciones que incluimos en nuestro informe y su nivel de riesgo.



Mapa de riesgos identificado para las observaciones de los sistemas de información de Compañía Nacional de Fuerza y Luz, S.A.

Como resultado de la revisión se comunican 2 observaciones que de acuerdo con la naturaleza del riesgo representan riesgo elevado.

X. Actividades evaluadas

A. Gestión de Tecnologías de Información

En la revisión de estas actividades se verificó lo siguiente:

1. Plan estratégico institucional.
2. Plan estratégico de TI.
3. Plan operativo de TI.
4. Organigrama institucional y de TI.
5. Informes de labores de TI del periodo auditado.
6. Reglamento del Comité de TI.
7. Actas del Comité de TI.
8. Matriz o informe sobre las recomendaciones en proceso o pendientes de atender internas, externas y regulatorias.
9. Informes de la auditoría interna de TI o entes reguladores.
10. Lista de los proveedores de servicio de TI actuales.
11. Contratos de TI de los proveedores de servicios.
12. Evaluaciones de los SLA´s con los proveedores actuales de servicios de TI.
13. Lista con el marco normativo (procedimientos, metodologías, entre otros) para los procesos y servicios de TI.
14. Plan de capacitación a los colaboradores del área de TI del periodo y su grado de ejecución.

Se comunican las siguientes oportunidades de mejora:

A.1 Plan Estratégico de Tecnología de Información

Elevado
✔

Se identificó un Plan Empresarial de Tecnología de Información del periodo 2020-2023, el cual incluía el planeamiento estratégico de la Dirección de Tecnologías de Información, manifestado a través de objetivos y estrategias institucionales, y alineado con el Planeamiento Estratégico Institucional.

En el 2024 no se evidencia un PETI aprobado ni en desarrollo, se nos informa que se está elaborando el Plan para el periodo 2024-2027.

El PETI es el documento de gestión que orienta el desarrollo de las tecnologías en cualquier entidad, a fin de que en la ejecución de un portafolio de proyectos informáticos estratégicos soporte a la organización en su meta de realizar la visión/misión que se propone, es una hoja de ruta ordenada y estructurada para proyectar en un tiempo determinado una arquitectura de TI deseada para soportar los objetivos estratégicos de la organización.

La carencia del PETI y la no alineación con el plan institucional puede presentar las siguientes desventajas:

1. No traducir las estrategias de la organización en programas e iniciativas que TI puede implementar.
2. No permitir que todos los proyectos tecnológicos estén enlazados con los planes y presupuestos de la organización.
3. No establecer las competencias sistemáticas o aquellos atributos de TI que son competencias distintivas de la organización y contribuyen a la generación de nuevas estrategias del negocio.
4. Los procesos de TI no atienden las necesidades de forma eficiente y eficaz como un elemento habilitador de la estrategia del negocio.
5. Impactar los productos y servicios nuevos.
6. No tener una herramienta de análisis para estructurar la ruta estratégica de manera concurrente y cohesiva de la empresa por medio de sus indicadores.

Recomendaciones

Actualizar y desarrollar un plan estratégico de TI, para establecer una visión a mediano plazo, que permita alinear las iniciativas de TI con la visión estratégica institucional por medio de fases como: análisis situacional, modelo del negocio, modelo de TI y modelo de planeación.

Confeccionar los planes anuales necesarios para identificar las oportunidades y limitaciones de TI para medir el desempeño, identificar la capacidad y los requerimientos de recursos para ejecutar el plan estratégico de TI.

Revisar y alinear los objetivos, metas y priorización de proyectos de TI con el negocio en lo referente a estrategia y operaciones, fomentando la toma de decisiones estratégicas y la obtención de los beneficios provenientes de las inversiones habilitadas con TI.

Desarrollar un marco normativo que guíe en la ejecución y el monitoreo del Plan Estratégico de TI, con el fin de cumplir y que sea consistente en la institución y con las partes interesadas durante todo el proceso de aprobación.

Comentario de la administración

En la CNFL actualmente se encuentra publicado el *"Plan empresarial de tecnologías de información y comunicación 2020-2023 v0.1";* sin embargo, se encuentra desactualizado, ya que corresponde a la "Estrategia Empresarial 2020-2023".

Por esta razón, la Dirección Transformación y Gestión Tecnológica, junto con la participación de varias dependencias, está elaborando la nueva versión del *"Plan empresarial de tecnologías (PETEC)"*, en alineamiento con la *"Estrategia Empresarial 2023-2027"* vigente.

El PETEC establecerá la dirección y los objetivos relacionados con el uso de las tecnologías en alineamiento con la estrategia empresarial, considerando la convergencia entre tecnologías de información, comunicación, operación y ciberseguridad. Este documento también se alineará con el "*Marco de gobierno y gestión de tecnologías*", el cual se encuentra en proceso de revisión y actualización.

Como parte de este proceso se ha realizado una identificación de las necesidades de tecnologías de información, comunicación, operación y ciberseguridad, y se está trabajando en el borrador del PETEC.

Es importante destacar que la *"Estrategia Empresarial 2023-2027"* incluye el objetivo estratégico *"OE.07 Adecuar la infraestructura actual y futura para apoyar la transformación digital y ciberseguridad al 2027"* con indicadores estratégicos referentes a la gestión de tecnologías, lo cual garantiza que la estrategia tecnológica se alinea con la estrategia empresarial. Para alcanzar estos indicadores se ha definido un portafolio de iniciativas de modernización digital, una cartera de soluciones digitales y un portafolio de iniciativas de ciberseguridad.

A.2 Actas del Comité de Tecnología de Información

Elevado
✔

No se evidenció actas o minutas del Comité de Tecnología de información del periodo 2024. Se identificó un “Reglamento del Comité Asesor de Tecnologías de Información y Comunicación” con fecha 17/06/2020, en donde se indica que sesionaran ordinariamente una vez cada 3 meses.

La práctica de documentar los asuntos analizados y comunicados que se discuten en esas reuniones se aplica con la finalidad de medir el grado de avance de los proyectos, el plan estratégico institucional y TI, validar el rumbo de las estrategias institucionales.

El proceso de COBIT 2019 (Incluido en la matriz de implementación de buenas prácticas de TI del MICITT) “APO01 — Gestionar el marco de gestión de I&T” en la práctica “APO01.04 Definir e implementar las estructuras organizativas.” indica lo siguiente:

“Establecer un comité de dirección de I&T (o equivalente) compuesto por directores ejecutivos, de negocio y de I&T para hacer un seguimiento del estado de los proyectos, resolver los conflictos de recursos y monitorizar los niveles y mejoras del servicio. Comprobar de forma regular la adecuación y eficacia de las estructuras organizativas.”

Recomendación

Analizar las funciones que tiene el Comité Asesor, para cumplir con la periodicidad de las sesiones establecidas en el Reglamento, al no realizar una sesión, podría correrse el riesgo de no tratar temas importantes como seguimiento del Plan Estratégico de TI, priorización de los proyectos de TI, la asignación de recursos y la atención de los requerimientos propios de la institución.

B. Gestión de la seguridad de la información

En la revisión de estas actividades se verificó lo siguiente:

1. Plan y estrategia de seguridad de la información.
2. Políticas y procedimientos para la administración de la seguridad.
3. Evaluaciones de seguridad de la red, infraestructura, sitio web internos.
4. Informes sobre las pruebas de vulnerabilidad y pent test.
5. Plan de acción de las recomendaciones en proceso y pendientes de atender sobre las evaluaciones de vulnerabilidad.
6. Informe de revisión de roles y perfiles de usuario.
7. Lista de atención de incidentes, el estado y su seguimiento.
8. Plan de trabajo de la seguridad informática y seguridad de la información

De acuerdo con el resultado de las pruebas realizadas no evidenciamos situaciones que nos hagan creer que no se cumple con los requerimientos de la gestión de seguridad de la información al 31 de diciembre de 2024.

C. Gestión de riesgos de tecnologías de información

En la revisión de estas actividades se verificó lo siguiente:

1. Metodología de riegos de TI.
2. Evaluaciones de riesgos de TI a los procesos o servicios.
3. Plan de acción para mitigar los riesgos.
4. Mapa o lista de riesgos de TI.
5. Informes de riesgos comunicados a los Órganos de Dirección.

De acuerdo con el resultado de las pruebas realizadas no evidenciamos situaciones que nos hagan creer que no se cumple con los requerimientos de la gestión de riegos de tecnología de información al 31 de diciembre de 2024.

D. Gestión de sistemas de información

En la revisión de estas actividades se verificó lo siguiente:

1. Diagrama de la integración de los sistemas de información.
2. Lista detallada de los sistemas, aplicativos y equipos obsoletos en caso de existir.
3. Inventario de los activos (software, hardware, aplicaciones) gestionados por TI.

4. Lista de los requerimientos o necesidades para la atención de los sistemas de información (desarrollo de sistemas) del periodo.
5. Lista de cambios realizados a los sistemas y aplicativos del periodo.
6. Evidencia de la activación de las bitácoras de los sistemas principales o Core.
7. Manuales técnicos y de usuarios de los sistemas.

De acuerdo con el resultado de las pruebas realizadas no evidenciamos situaciones que nos hagan creer que no se cumple con los requerimientos de la gestión de sistemas de información al 31 de diciembre de 2024.

E. Gestión de la continuidad de negocio

En la revisión de estas actividades se verificó lo siguiente:

1. Análisis de Impacto de Negocio (BIA).
2. Plan de continuidad de negocio.
3. Plan de recuperación (DRP).
4. Plan de pruebas del plan de continuidad y planes de acción de los resultados de las pruebas.
5. Evidencia de capacitación a los usuarios sobre la continuidad de operaciones.
6. Bitácora o reporte de eventos si ha sido requerido activar el plan de continuidad o recuperación.
7. Evidencia de la validación de respaldos.
8. Descripción de los sitios de procesamiento.

De acuerdo con el resultado de las pruebas realizadas no evidenciamos situaciones que nos hagan creer que no se cumple con los requerimientos de la gestión de la continuidad de negocio al 31 de diciembre de 2024.

F. Seguimiento del periodo anterior

No se identifican observaciones de seguimiento del periodo anterior de acuerdo con la Carta de Gerencia emitida por otro auditor al 31 de diciembre de 2023.