UNIVERSIDAD NACIONAL DE INGENIERÍA

Facultad de Electrotecnia y Computación FEC

PRÁCTICAS PROFESIONALES

Para optar al Título de

Ingeniero en Computación

“Auditoría interna de procesos informáticos aplicando el marco de gobierno de tecnologías de la información COBIT 5”

Presentado por:

Br. José César Palacios Grijalva

Tutor:

TkL. Will Johnny Flores Delgadillo

Managua, Nicaragua

Julio 2021

Managua, Nicaragua 17 de junio 2021

UNI-RUSB
Facultad de Electrotecnia y Computación
Decanatura FEC
Ing. Ronald Torres Torres

Estimado Ing. Torres:

A través de la presente, me dirijo a usted para solicitarle su aprobación para presentación y defensa para el día 9 de julio 2021 a las 2:00 PM en la Sala de Profesores del informe final de la práctica profesional **"Auditoría interna de procesos informáticos aplicando el marco de gobierno de tecnologías de la información COBIT 5"**, realizado por el **Br. José César Palacios Grijalva.**

El trabajo final fue revisado por mí, por lo cual emito en carta adjunta aprobación del trabajo realizado.

Sin más que agregar, me despido y agradezco de antemano su apoyo.

TkL. Will Johnny Flores Delgadillo

Managua, Nicaragua 9 de julio 2021

UNI-RUSB
Facultad de Electrotecnia y Computación
Decanatura FEC
Ing. Ronald Torres Torres

Estimado Ing. Torres:

A través de la presente, le informo que el **Br. José César Palacios Grijalva** con número de carnet 2009-29387, ha finalizado el proyecto **"Auditoría interna de procesos informáticos aplicando el marco de gobierno de tecnologías de la información COBIT 5"**, el cual le fue autorizado para concluir sus estudios de Ingeniería en Computación.

He revisado la documentación y se encuentra en condición de ser presentada ante el tribunal examinador que usted designe.

Este trabajo cumple con los requisitos para su presentación y defensa, así mismo su desarrollo cubre los objetivos planteados, tiene coherencia metodológica y detalla conclusiones y recomendaciones de acuerdo a los resultados obtenidos.

Sin más que agregar, me despido y agradezco de antemano su apoyo.

TkL. Will Johnny Flores Delgadillo

AKROSERV

Soluciones que agregan valor a nuestros Clientes.

Managua, Nicaragua 9 de julio 2021

UNI-RUSB
Facultad de Electrotecnia y Computación
Decanatura FEC
Ing. Ronald Torres Torres

Estimado Ing. Torres:

A través de la presente, hago constar que el **Sr. José César Palacios Grijalva** con número de Carnet **2009-29387**, egresado de la carrera Ingeniería en Computación y trabajador activo de AKROSERV, ha finalizado la ejecución del proyecto **"Auditoría interna de procesos informáticos aplicando el marco de gobierno de tecnologías de la información COBIT 5"**.

Hacemos constar que se ha supervisado el trabajo a lo largo del tiempo establecido y en cada fase, obteniendo los resultados deseados cumpliendo así con los objetivos establecidos de manera satisfactoria.

Sin más que agregar, me despido cordialmente de usted.

Atentamente,

Irma Antonia Chamorro Zamora
Gerente de Operaciones
AKROSERV S.A
Tel. +505 89829022
ichamorro@akroserv.com

AKROSERV

Soluciones que agregan valor a nuestros Clientes.

Managua, Nicaragua 9 de julio 2021

UNI-RUSB
Facultad de Electrotecnia y Computación
Decanatura FEC
Ing. Ronald Torres Torres

Estimado Ing. Torres:

El motivo de la presente es para informarle que, debido a la situación sanitaria de la Pandemia COVID-19, la empresa se vio obligada a suspender actividades para salvaguardar la integridad de nuestros colaboradores. Es por esto que el proyecto **"Auditoría interna de procesos informáticos aplicando el marco de gobierno de tecnologías de la información COBIT 5"** que estaba siendo ejecutado por el **Sr. Jose Cesar Palacios Grijalva** sufrió un retraso de 3 meses, lo cual afecto el tiempo establecido en el cronograma.

Nuestra intención es que tenga en cuenta esta situación para que no afecte el proceso de prácticas profesionales para optar al título de ingeniero del **Sr. Palacios** y de esta forma pueda concluir con su proyecto final.

Sin más que agregar, me despido cordialmente de usted.

Atentamente,

Irma Antonia Chamorro Zamora
Gerente de Operaciones
AKROSERV S.A
Tel. +505 89829022
ichamorro@akroserv.com

DEDICATORIA.

Dedico mis prácticas profesionales a Dios, por darme la oportunidad de vida, las fuerzas y los medios necesarios para continuar mi formación como profesional, siendo un apoyo incondicional en cada etapa de mi existencia y una luz para iluminar mi entendimiento.

A mi madre y a mi padre cuyo ejemplo, amor y motivación han sido el eslabón primordial para cumplir mis metas. Su creencia en mi ha sido el impulso para llegar a ser un ingeniero y mejor persona.

Finalmente, a todos mis docentes quienes influyeron con sus lecciones y experiencias en formarme y prepararme para los diferentes retos que nos pone la vida. Y a mis amigos que desde el inicio de mi etapa en la universidad demostraron con sinceridad ser los mejores exponentes de la correcta definición de amistad.

A todos ustedes este esfuerzo es dedicado.

AGRADECIMIENTO.

Agradezco infinitamente a Dios por la oportunidad de vida y ser el motor de fuerzas que me han impulsado a superarme académicamente y como persona al proveerme de todo lo esencial para cumplir mis metas.

Con profundo sentimiento agradezco a mi madre y a mi padre por el amor, ánimo y apoyo que me han brindado desde el primer día, cuyo esfuerzo ha valido tanto para que yo pueda salir adelante. Gracias por hacer posible este triunfo de ser ingeniero.

A mi tutor TkL. Will Johnny Flores Delgadillo, por toda su valiosa colaboración en la realización de este informe de prácticas profesionales, gracias por guiarme en todo el proceso. Agradecimiento perpetuo por transmitir su sabiduría en el desarrollo de mi formación académica.

A mis docentes que sin duda sus conocimientos y experiencias de vida me han ayudado a superarme en las diferentes fases de mi carrera. Sus consejos quedaran atesorados en mi mente y corazón.

Gratitud especial a los colaboradores de AKROSERV S.A., por permitirme llevar en efecto la realización de estas prácticas. Gracias por todo el tiempo que me dieron y la paciencia brindada en la enseñanza de cada una de las actividades desarrolladas.

INDICE

1. INTRODUCCION

COBIT 5 es un marco de trabajo que permite comprender el gobierno y la gestión de las tecnologías de información (TI) de una organización, así como evaluar el estado en que se encuentran las TI en la empresa. COBIT fue creado para ayudar a las organizaciones a obtener el valor óptimo de TI manteniendo un balance entre la realización de beneficios, la utilización de recursos y los niveles de riesgo asumidos. COBIT 5 posibilita que TI sea gobernada y gestionada en forma holística para toda la organización, tomando en consideración el negocio y áreas funcionales de punta a punta, así como los interesados internos y externos.

La empresa AKROSERV está interesada determinar si el estado actual de sus procesos se alinea con lo establecido en el marco de gobierno de TI de COBIT 5, es por esto que se realizará una auditoria interna de procesos informáticos utilizando los siguientes procesos establecidos por la norma:

APO01 – Gestionar el marco de gestion de TI
APO06 – Gestionar el presupuesto y los costos
APO07 – Gestionar los recursos humanos
APO11 – Gestionar la calidad
APO12 – Gestionar el riesgo
APO13 – Gestionar la seguridad
BAI04 – Gestionar la disponibilidad y la capacidad
BAI05 – Gestionar la habilitacion del cambio organizativo
BAI06 – Gestionar los cambios
BAI09 – Gestionar los archivos
BAI10 – Gestionar la configuracion
DSS02 – Gestionar las peticiones y los incidentes de servicio
DSS03 – Gestionar los problemas
DSS05 – Gestionar los servicios de seguridad
MEA01 – Supervisar, evaluar y valorar el rendimiento y conformidad

La auditoria interna consiste en evaluar los procesos de TI de la empresa AKROSERV con respecto a los procesos de COBIT 5 establecidos previamente para de esta forma determinar su estado de madurez actual y tomar medidas para lograr alinearse a la norma y poder brindar un servicio que sea de calidad siguiendo las buenas prácticas internacionales.

2. OBJETIVO GENERAL.

Realizar una auditoría interna al departamento de informática de la empresa AKROSERV utilizando el marco de trabajo COBIT 5 a fin de identificar su estado actual, brindar recomendaciones y oportunidades de mejora que permitan optimizar los proceso y fortalecer el gobierno de TI.

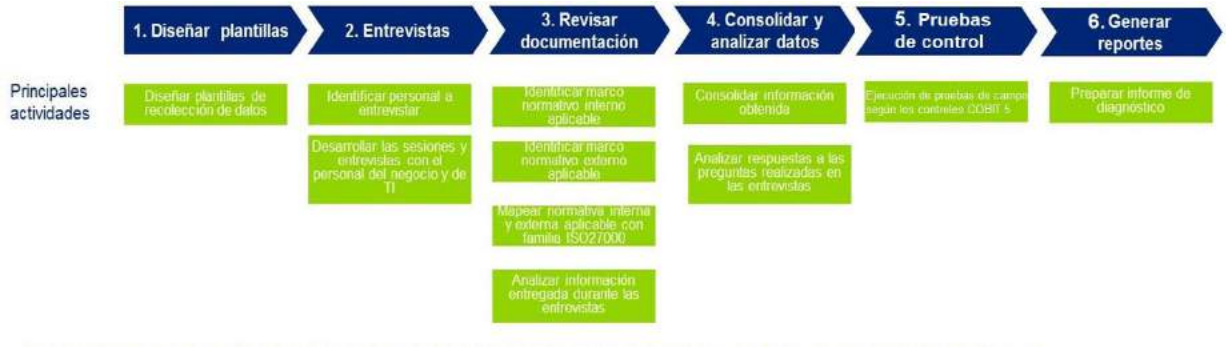
3. OBJETIVOS ESPECIFICOS.

1. Verificar la existencia de políticas claras y buenas prácticas de control que permitan la utilización de los sistemas de modo productivo y seguro, manteniendo la confidencialidad, la integridad y la disponibilidad de la información.

2. Identificar vulnerabilidades existentes en los procesos actuales de TI que impidan una óptima gestión de gobierno.

3. Realizar un informe final de auditoría informática que contenga la evaluación de los elementos auditados, así como las recomendaciones para lograr la mejora y optimización de los procesos de TI en base al marco de trabajo COBIT 5.

4. METODOLOGIA.



Cada una de las actividades anteriormente expuestas se detalla a continuación:

Diseño de plantillas.

El primer paso del análisis de la situación actual fue diseñar las plantillas a utilizar para la recolección y análisis de la información. Para esto se definió una plantilla que abarcara los requerimientos y objetivos de control establecidos en el marco de gobierno COBIT 5.

La plantilla desarrollada está basada en preguntas abiertas que están alineadas a los requerimientos de COBIT 5 y a identificar los niveles de madurez de los requerimientos y controles de este mismo.

Plantilla análisis de requisitos COBIT 5- Situación actual y nivel de madurez de los siguientes requerimientos de la norma:

APO01 – Gestionar el marco de gestion de TI
APO06 – Gestionar el presupuesto y los costos
APO07 – Gestionar los recursos humanos
APO11 – Gestionar la calidad
APO12 – Gestionar el riesgo
APO13 – Gestionar la seguridad
BAI04 – Gestionar la disponibilidad y la capacidad
BAI05 – Gestionar la habilitacion del cambio organizativo
BAI06 – Gestionar los cambios
BAI09 – Gestionar los archivos
BAI10 – Gestionar la configuracion
DSS02 – Gestionar las peticiones y los incidentes de servicio
DSS03 – Gestionar los problemas
DSS05 – Gestionar los servicios de seguridad
MEA01 – Supervisar, evaluar y valorar el rendimiento y conformidad

Entrevistas al personal vinculado.

Una vez que se diseñaron las plantillas de recolección de información, se procedió a

identificar el personal requerido para obtener la información y programar las entrevistas con el mismo.

Para definir el personal a participar en cada una de las sesiones, se debe considerar la relación con cada ítem evaluado.

Adicional a la ejecución de las entrevistas, se consideran las solicitudes de información adicional por medio de correo electrónico, con el objetivo de aclarar puntos relacionados con el análisis.

Revisión de documentación existente.

Como parte del análisis, se revisó la documentación proporcionada por el personal entrevistado. Esta información incluyó, entre otros:

- Políticas
- Directrices
- Procedimientos
- Manuales
- Guías

Consolidación y análisis de datos.

Una vez ejecutadas las entrevistas, se consolida la información en las plantillas respectivas y se procede a analizar la información recopilada.

Pruebas de control.

Se ejecutaron pruebas de campo siguiendo las bases del marco de gobierno establecido en COBIT 5.

Generación de reportes.

Con la información consolidada y analizada, se procede a generar el presente informe con las principales conclusiones y recomendaciones.

5. DIAGNOSTICO DE OBJETIVOS DE CONTROL.

COBIT 5 – Proceso APO01. Gestionar el marco de gestión de TI	
Descripción del proceso	
Aclarar y mantener la gobernabilidad de la misión de la empresa de TI y la visión. Implementar y mantener mecanismos y autoridades para gestionar la información y el uso de TI en la empresa en apoyo de los objetivos de gobierno en línea con otros principios considerados.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
Hallazgos No satisfactorios	
APO01.01 Establecer una estructura organizativa interna y extendida que refleje las necesidades y prioridades de negocio de TI. Poner en marcha las estructuras de gestión necesarias (por ejemplo, comités) que permiten hacer que tenga lugar de la manera más eficaz y eficiente de decisiones de gestión.	**Hallazgos identificados** Está en proceso de actualización el plan estratégico de tecnología conforme se identifica en la entrevista con la Dirección de Informática, por lo tanto, no está bien definida una estructura organizativa interna que se encargue de gestionar de manera eficiente todo lo relacionado a las decisiones de TI. **Conclusiones y recomendaciones** Se recomienda finalizar la revisión y actualización del plan estratégico para garantizar que se establezca de manera adecuada la estructura organizativa interna.
APO01.02 Establecer, acordar y comunicar los roles y responsabilidades del personal de TI, así como otras partes interesadas con responsabilidades de TI de la empresa, que reflejan claramente las necesidades generales de la empresa y los objetivos de TI y de autoridad, las responsabilidades del personal pertinente y la rendición de cuentas.	**Hallazgos identificados** De acuerdo con la revisión efectuada y sesiones obtenidas con las diferentes áreas, se identificó que no existe política de seguridad aplicable a AKROSERV por lo tanto no existe control de los roles y responsabilidades de la seguridad de la información. De igual forma no se observan reportes de desempeño sobre la aplicación de actividades por parte de esos roles. **Conclusiones y recomendaciones** Se recomienda acorde a las buenas prácticas para el gobierno de la seguridad establecidas en el marco de control COBIT 5, crear un área de seguridad de la información con alcance institucional que posea la potestad de ejecutar las acciones de gobierno de seguridad, así como

COBIT 5 – Proceso APO01. Gestionar el marco de gestión de TI	
	evaluar de manera periódica el desempeño de las actividades realizadas por el personal de acuerdo a su rol y autoridad definidos.
APO01.03 Mantener los facilitadores del sistema de gestión y control de entorno para las TI, y asegurarse de que están integrados y alineados con el gobierno de la empresa y la filosofía de gestión y estilo de funcionamiento. Estos habilitadores incluyen la comunicación clara de las expectativas / necesidades. El sistema de gestión debería fomentar entre divisiones cooperación y trabajo en equipo, promover el cumplimiento y la mejora continua, y desviaciones del proceso mango (incluyendo insuficiencia).	**Hallazgos identificados** La empresa cuenta con un conjunto de políticas para el control del área, sin embargo, estas no toman en cuenta temas relevantes como la calidad, seguridad, confidencialidad, controles internos y uso de los activos de TI. De igual forma, estas no son evaluadas ni actualizadas anualmente por lo cual no se ajustan al entorno del negocio. **Conclusiones y recomendaciones** Se recomienda realizar una evaluación de las políticas y actualizarlas de forma que sean adecuadas para las necesidades de la empresa.
APO01.04 Comunicar la conciencia y la comprensión de los objetivos de TI y dirección a las partes interesadas y los usuarios apropiados a lo largo de la empresa.	**Hallazgos identificados** Los objetivos de TI no son comunicados con frecuencia y cuando se hace, no lo hacen de forma clara ni usan suficiente recurso informativo por lo cual estos no están claros para las partes interesadas. **Conclusiones y recomendaciones** Se recomienda comunicar continuamente los objetivos de TI, garantizando que la información sea clara y que cuente con el nivel de detalle adecuado para cada audiencia respectiva de la empresa.
APO01.05 Colocar la capacidad de TI en la estructura organizativa general para reflejar un modelo de empresa correspondiente a la importancia de las TI dentro de la empresa, específicamente su criticidad para la estrategia de la empresa y el nivel de dependencia operativa de TI. La línea de reporte del CIO debe ser proporcional a la importancia de las TI dentro de la empresa.	**Hallazgos identificados** Las ubicaciones en la organización, modelos operativos y de aprovisionamiento no están bien identificadas ni priorizadas. **Conclusiones y recomendaciones** Definir las ubicaciones de las funciones de TI.
APO01.06 Definir y mantener las responsabilidades de propiedad de la información (datos) y los sistemas de información. Asegúrese de que los propietarios de tomar decisiones acerca de la clasificación de la información y sistemas y protegerlos de acuerdo con esta clasificación.	**Hallazgos identificados** Existen políticas para asegurar la clasificación de la información en toda la empresa, sin embargo, estas no cumplen por completo ya que no se cuentas con las herramientas ni técnicas adecuadas para asegurar y tener control efectivo sobre la información y sistemas junto con el propietario. **Conclusiones y recomendaciones** Definir e implementar procedimientos para asegurar la integridad y consistencia de la información almacenada en formato electrónico. Crear y mantener un inventario de la información almacenada que incluya una lista de propietarios, custodios y clasificaciones.
APO01.07 Evaluar, planificar y ejecutar la mejora continua de los procesos y su madurez para asegurarse de que son capaces de entregar los objetivos empresariales, de gobierno, gestión y control. Considere orientación COBIT implementación de procesos,	**Hallazgos identificados** No se realiza evaluación de las políticas ni de los procesos existentes por lo cual estos no están actualizados a la realidad de la empresa. **Conclusiones y recomendaciones**

COBIT 5 – Proceso APO01. Gestionar el marco de gestión de TI	
estándares emergentes, los requisitos de cumplimiento, las oportunidades de automatización, y las votaciones de los usuarios del proceso, el equipo de proceso y otras partes interesadas. Actualizar el proceso y considerar los impactos en facilitadores de proceso.	Identificar los procesos críticos e implementar mejoras que garanticen un rendimiento y cumplimiento optimo, de igual forma remover los procesos y políticas desactualizados o que no aporten ninguna mejora o beneficio a la empresa.
APO01.08 Puesto en marcha procedimientos para mantener el cumplimiento y la medición de los resultados de las políticas y otros facilitadores del marco de control, y hacer cumplir las consecuencias del incumplimiento o cumplimiento defectuoso. Realizar un seguimiento de las tendencias y el rendimiento y considerar estos en el diseño y la mejora del marco de control futuro.	**Hallazgos identificados** No se ha realizado un proceso de revisión ni seguimiento. **Conclusiones y recomendaciones** Se recomienda definir un proceso de revisión y seguimiento, el período al menos una vez al año para revisión de la política, además también se recomienda efectuar actualización cada vez que sucedan grandes incidentes, después de auditorías sin éxito y/o frente a cambios que afectan a la estructura de la organización.

COBIT 5 – Proceso APO06. Gestionar el presupuesto y los costes
Descripción del proceso
Gestionar las actividades financieras relacionadas con las TI en las funciones del negocio y de TI, que abarca el presupuesto, el costo y administración de beneficios, y la priorización de pasar a través del uso de prácticas de presupuestos formales y una feria y sistema equitativo de asignación de costes para la empresa. Consultar a los interesados para identificar y controlar los costes y beneficios totales en el contexto de los planes estratégicos de TI y tácticos, e iniciar acciones correctivas cuando sea necesario.
Madurez
Nivel de madurez general

Situación evidenciada

COBIT 5 – Proceso APO06. Gestionar el presupuesto y los costes	
Hallazgos No satisfactorios	
APO06.01 Establecer y mantener un método para tener en cuenta todos los costes, inversiones y amortizaciones relacionadas con las TI como una parte integral de los sistemas financieros de la empresa y el plan de cuentas para gestionar las inversiones y los costes de TI. Captura y asignar los costes reales, analizar las variaciones entre las previsiones y los costes reales, y el informe utilizando sistemas de medición financieros de la empresa.	**Hallazgos identificados** De acuerdo con la revisión efectuada con la Dirección de Informática, no existe un método claramente establecido al momento de evaluar los costos e inversiones relacionadas con TI. **Conclusiones y recomendaciones** Se recomienda de acuerdo con las buenas prácticas para el gobierno de Ti en el marco de control de COBIT 5, establecer formalmente un método para tomar en cuenta todos los costos e inversiones relacionados con TI para de esta forma evitar cualquier daño financiero a la empresa.
APO06.02 Implementar un proceso de toma de decisiones para priorizar la asignación de recursos y las reglas para las inversiones discrecionales por unidades de negocio individuales. Incluir el uso potencial de los proveedores de servicios externos y considerar la compra, alquiler y desarrollar opciones.	**Hallazgos identificados** No existe un proceso de toma de decisiones. **Conclusiones y recomendaciones** Se recomienda establecer e implementar el proceso para toma de decisiones.
APO06.03 Preparar un presupuesto que refleje las prioridades de inversión que apoyan los objetivos estratégicos basados en la cartera de programas de TI habilitado y servicios de TI.	**Hallazgos identificados** Existe un presupuesto definido en la empresa, pero este no refleja las prioridades de TI de forma adecuada. **Conclusiones y recomendaciones** Se recomienda realizar modificaciones al presupuesto existente para que en el este se reflejen adecuadamente las prioridades de TI.
APO06.04 Establecer y utilizar un modelo de costo basado en la definición del servicio, asegurando que la asignación de costes de los servicios sea identificable, es medible y predecible, para fomentar el uso responsable de los recursos, incluyendo los proporcionados por los proveedores de servicios. Regularmente revisar y comparar la idoneidad del modelo de costo / devolución de cargo para mantener su relevancia y adecuación a la evolución de las actividades de negocio y de TI.	**Hallazgos identificados** No existe un modelo de costos de TI definido, pero si se cuenta con una clasificación de proveedores, aunque no se revisa constantemente. **Conclusiones y recomendaciones** Se recomienda definir un modelo en el cual se establezca como se calcularán y cargaran los costos de TI y que este alineado al presupuesto del área de TI.
APO06.05 Implementar un proceso de gestión de los costes reales se comparan los costos en los presupuestos. Los costos deben ser monitoreados y reportados y, en el caso de desviaciones, identifican de una manera oportuna y su impacto en los procesos y servicios de la empresa evaluados.	**Hallazgos identificados** No existe un proceso de gestión de costos definido. **Conclusiones y recomendaciones** Se recomienda definir un proceso de gestión de costos donde se realice una recopilación de datos relevantes para identificar desviaciones en control presupuestario entre presupuesto y real, así como distribución de costo directo e indirecto.

COBIT 5 – Proceso APO07. Gestionar los recursos humanos

Descripción del proceso

Proporcionar un enfoque estructurado para garantizar una óptima estructuración, colocación, los derechos de decisión y las habilidades de los recursos humanos. Esto incluye la comunicación de los roles y responsabilidades definidos, el aprendizaje y los planes de crecimiento y las expectativas de rendimiento, apoyados con las personas competentes y motivados.

Madurez

Nivel de madurez general

Situación evidenciada

Hallazgos No satisfactorios

APO07.01 Evaluar las necesidades de personal de forma regular o sobre cambios importantes en la empresa u operativos o entornos de TI para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos de la empresa. El personal incluye tanto los recursos internos y externos.	**Hallazgos identificados** No se realiza dicha evaluación, está en proceso de realizarse dicha actividad. Sin embargo, AKROSERV posee un procedimiento de que asegura la asignación de los recursos cuando son necesarios. **Conclusiones y recomendaciones** De acuerdo con lo anterior se requiere un compromiso contundente de todos los involucrados y especialmente de la alta dirección. Es indispensable que los responsables consideren y definan todos los recursos necesarios y que los mismos sean apoyados por la alta dirección.
APO07.02 Identificar al personal clave y reducir al mínimo la dependencia de un solo individuo que realiza una función de trabajo crítico a través de la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y de copia de seguridad personal.	**Hallazgos identificados** Si se ha identificado al personal clave en la empresa, sin embargo, existe mucha dependencia de un solo individuo y no existe documentación ni intercambio de conocimientos. **Conclusiones y recomendaciones** Se recomienda realizar la documentación adecuada sobre los procesos y funciones que están asignadas a la persona que desempeña dicha función critica, para que de este modo se reduzca al mínimo esta dependencia.
APO07.03 Definir y gestionar las habilidades y competencias necesarias del personal. Regularmente verificar que el personal tenga las competencias necesarias para cumplir con sus	**Hallazgos identificados** Se han definido las habilidades; sin embargo, no hay proceso de valoración de competencias necesarias.

COBIT 5 – Proceso APO07. Gestionar los recursos humanos	
funciones sobre la base de su educación, la formación y / o experiencia, y verificar que estas competencias son objeto de mantenimiento, el uso de programas de calificación y certificación en su caso. Proporcionar a los empleados con el aprendizaje y oportunidades para mantener sus conocimientos, habilidades y competencias en un nivel constante requieren para lograr los objetivos de la empresa.	**Conclusiones y recomendaciones** Se recomienda identificar las competencias necesarias por el personal para posteriormente definir una estrategia de capacitación con temática de índole más técnica. Para los casos donde sólo un funcionario pueda asistir, debido al presupuesto limitado, se defina un proceso de transferencia de conocimiento para con los demás funcionarios como parte del plan de entrenamiento.
APO07.04 Realizar evaluaciones de rendimiento puntuales sobre una base regular contra objetivos individuales derivados de los objetivos de la empresa, las normas establecidas, las responsabilidades específicas del trabajo, y las habilidades y el marco de competencias. Los empleados deben recibir entrenamiento sobre el rendimiento y la conducta cuando sea apropiado.	**Hallazgos identificados** No se realizan evaluaciones puntuales a los empleados. **Conclusiones y recomendaciones** Se recomienda la realización de evaluaciones individuales para así poder dar el entrenamiento adecuado sobre rendimiento y conducta a los empleados.
APO07.05 Entender y realizar un seguimiento de la demanda actual y futura de los negocios de TI, recursos humanos con funciones de TI de la empresa. Identificar las deficiencias y aportaciones a planes de abastecimiento, la empresa y el reclutamiento de los procesos de TI Los planes de abastecimiento, y las empresas y los procesos de contratación de TI.	**Hallazgos identificados** Si se realiza seguimiento a la tendencia de las demandas de negocios actuales, pero no se contemplan las futuras. No se han logrado identificar de manera eficaz las deficiencias en los planes que abarcan lo relacionado con TI en la empresa. **Conclusiones y recomendaciones** En este punto se recomienda realizar un seguimiento más amplio que abarque las demandas futuras, de igual forma realizar sesiones de trabajo para identificar y erradicar de forma eficaz las deficiencias en los planes de TI.
APO07.06 Asegurar que los consultores y el personal contratado que apoyan a la empresa con capacidades de TI conozcan y cumplan con las políticas de la organización acordadas en los requisitos contractuales.	**Hallazgos identificados** No se realiza evaluación para asegurar que el personal contratado conoce y cumple con las políticas existentes relacionadas con el área de TI. **Conclusiones y recomendaciones** Se recomienda llevar revisiones y evaluaciones periódicas para asegurar que el personal conozca y cumpla con las políticas. Advertir a los contratistas que la empresa se reserva el derecho de inspeccionar y supervisar todos los recursos de TI.

COBIT 5 – Proceso APO11. Gestionar la calidad
Descripción del proceso

COBIT 5 – Proceso APO11. Gestionar la calidad	
Definir y comunicar los requisitos de calidad en todos los procesos, los procedimientos y los resultados relacionados de la empresa, incluyendo los controles, supervisión continua y el uso de prácticas probadas y estándares en los esfuerzos de mejora de eficiencia y continuas.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
Hallazgos No satisfactorios	
APO11.01 Establecer y mantener un SGC que proporciona un enfoque estándar, formal y continuo a la gestión de calidad de la información, lo que permite procesos de tecnología y negocios que están alineados con los requerimientos del negocio y de gestión de calidad de la empresa.	**Hallazgos identificados** Actualmente no se ha documentado un SGC. Este documento debe ser desarrollado para lograr el cumplimiento del apartado. En su desarrollo se puede utilizar la información contenida en el informe de diagnóstico. **Conclusiones y recomendaciones** Se debe definir un documento formal que defina y establezca un enfoque estándar, formal y continuo y que determine las partes o procesos de la organización que van a ser incluidos para el alineamiento de la empresa con los requerimientos del negocio en cuestión de gestión de la calidad.
APO11.02 Identificar y mantener los requisitos, normas, procedimientos y prácticas para los procesos clave para orientar la empresa en el cumplimiento de la intención de la acordada en la SGC. Esto debería estar en línea con los requisitos del marco de control de TI. Considerar la certificación de los procesos clave, unidades organizativas, productos o servicios.	**Hallazgos identificados** No existen políticas y procedimientos definido puesto que no existe un SGC definido. **Conclusiones y recomendaciones** Se recomienda definir y actualizar las políticas y procedimientos que estén alineados con el marco de control de TI haciendo uso de las mejores prácticas y considerar certificar dichos procesos.
APO11.03 Enfoque de gestión de calidad en los clientes mediante la determinación de sus necesidades y asegurar la alineación con las prácticas de gestión de la calidad.	**Hallazgos identificados** Si bien se determinan de una forma bastante eficiente las necesidades de los clientes, no hay alineación con las prácticas de gestión de calidad puesto que no existen un SGC definido. **Conclusiones y recomendaciones** Se recomienda supervisar y regular periódicamente que el SGC este de acuerdo con lo criterios de aceptación de calidad.

COBIT 5 – Proceso APO11. Gestionar la calidad	
APO11.04 Controlar la calidad de los procesos y servicios de manera continua como se define por las SGC. Definir, planificar y ejecutar las mediciones a la satisfacción del cliente con el monitor de calidad, así como el valor del SGC ofrece. La información recopilada debe ser utilizado por el propietario del proceso para mejorar la calidad.	**Hallazgos identificados** No existen un plan de supervisión de la satisfacción del cliente. **Conclusiones y recomendaciones** Definir un plan para la medición de satisfacción del cliente, así como controlar la calidad de los procesos y servicios de forma continua mediante revisiones permanentes.
APO11.05 Incorporar prácticas de gestión de calidad relevantes en la definición, seguimiento, información y gestión en curso de desarrollo de soluciones y ofertas de servicios.	**Hallazgos identificados** No hay definidas prácticas de gestión de calidad para la gestión de soluciones y servicios ofrecidos. **Conclusiones y recomendaciones** Se recomienda integrar las prácticas de gestión de calidad en los procesos y practicas de desarrollo de soluciones.
APO11.06 Mantener y comunicar periódicamente un plan general de calidad que promueva la mejora continua. Esto debe incluir la necesidad de, y los beneficios de la mejora continua. Recopilar y analizar datos sobre los SGC, y mejorar su eficacia. Corregir las no conformidades para prevenir la recurrencia. Promover una cultura de calidad y mejora continua.	**Hallazgos identificados** No existe un plan general de calidad definido. **Conclusiones y recomendaciones** Se recomienda definir un plan general de calidad el cual debe ser comunicado periódicamente y de forma clara a todos los interesados, así como recopilar datos para la mejora de este.

COBIT 5 – Proceso APO12. Gestionar el riesgo
Descripción del proceso
Continuamente identificar, evaluar y reducir TI relacionada con el riesgo dentro de los niveles de tolerancia al conjunto de la dirección ejecutiva de la empresa.
Madurez
Nivel de madurez general

COBIT 5 – Proceso APO12. Gestionar el riesgo	
	
Situación evidenciada	
Hallazgos No satisfactorios	
APO12.01 Identificar y recopilar datos pertinentes para permitir la identificación efectiva de riesgos relacionados con TI, análisis e informes.	**Hallazgos identificados** No se han recopilado datos para la identificación efectiva de riesgos relacionados con TI. **Conclusiones y recomendaciones** Se recomienda definir un proceso formal para la recopilación de datos. Se puede tomar como referencia el marco COBIT 5.
APO12.02 Desarrollar información útil para decisiones de riesgo de apoyo que tengan en cuenta la importancia del negocio de los factores de riesgo.	**Hallazgos identificados** Se desarrolla información para la toma de decisiones de riesgo, pero esta información es algo deficiente por lo cual no es fiable por completo. **Conclusiones y recomendaciones** Se recomienda realizar una mejor revisión de la información desarrollada para de esta forma hacer una toma de decisión de riesgo acertada.
APO12.03 Mantener un inventario de los atributos conocidos de riesgo (incluyendo la frecuencia esperada, el potencial de impacto y respuestas) y de los recursos relacionados, las capacidades y las actividades de control actuales.	**Hallazgos identificados** No existe dicho inventario. **Conclusiones y recomendaciones** Se recomienda la creación del inventario de atributos de riesgo.
APO12.04 Proporcionar información sobre el estado actual de las exposiciones y oportunidades relacionados con la TI de manera oportuna a todas las partes necesarias para la respuesta apropiada.	**Hallazgos identificados** No se proporciona información sobre el estado actual. **Conclusiones y recomendaciones** Se recomienda recopilar toda la información sobre el estado actual y que esta sea proporcionada a las partes necesarias para que se brinde una respuesta apropiada en caso de que se presente algún cambio inesperado.
APO12.05 Gestionar las oportunidades para reducir el riesgo a un nivel aceptable.	**Hallazgos identificados** No se gestionan las oportunidades por lo cual el nivel de riesgo el alto.

COBIT 5 – Proceso APO12. Gestionar el riesgo	
	Conclusiones y recomendaciones
	Se recomienda realizar una mejor gestión por parte de la Dirección de Informática en este punto para disminuir el nivel de riesgo a aceptable.
APO12.06 Responder de manera oportuna con medidas efectivas para limitar la magnitud de la pérdida de los eventos relacionados con la TI.	**Hallazgos identificados**
	Se responde de manera oportuna a los inconvenientes, pero las medidas no son muy efectivas.
	Conclusiones y recomendaciones
	Se recomienda revisar las medidas que se toman al momento de atender los inconvenientes de TI para que esta respuesta sea lo más eficaz posible y así minimizar cualquier perdida que se pueda producir.

COBIT 5 – Proceso APO13. Gestionar la seguridad	
Descripción del proceso	
Definir, operar y supervisar un sistema de gestión de seguridad de la información.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
Hallazgos No satisfactorios	
APO13.01 Establecer y mantener un SGSI que proporciona un enfoque estándar, formal y continuo a la gestión de la seguridad de la información, permitiendo a los procesos tecnológicos y empresariales seguras que están alineados con los requerimientos del negocio y la gestión de seguridad de la empresa.	**Hallazgos identificados**
	Actualmente se está trabajando en la implementación de un SGSI.
	Conclusiones y recomendaciones
	Se recomienda que se finalice la implementación del SGSI.
APO13.02 Mantener un plan de seguridad de la información que	**Hallazgos identificados**

COBIT 5 – Proceso APO13. Gestionar la seguridad	
describe cómo el riesgo de seguridad de la información se va a gestionar y alineada con la estrategia de la empresa y la arquitectura de la empresa. Asegurar que las recomendaciones para la implementación de mejoras de seguridad se basan en casos de negocio aprobado e implementado como una parte integral del desarrollo de servicios y soluciones, a continuación, funciona como una parte integral de la operación del negocio.	No existe un plan de seguridad de información, pero se tiene contemplada la creación de dicho plan junto a la implementación del SGSI. **Conclusiones y recomendaciones** Se recomienda trabajar en la creación del plan de seguridad de la información basado en casos de negocios aprobados para brindar servicios y soluciones integrales.
APO13.03 Mantener y comunicar regularmente la necesidad y beneficios de información continua mejora de la seguridad. Recopilar y analizar datos sobre el SGSI, y mejorar la eficacia del SGSI. Corregir las no conformidades para prevenir la recurrencia. Promover una cultura de la seguridad y la mejora continua.	**Hallazgos identificados** No se realiza esta actividad ya que aún no existe un SGSI. **Conclusiones y recomendaciones** Se recomienda realizar dicha actividad cuando ya este implementado el SGSI.

COBIT 5 – Proceso BAI04. Gestionar la disponibilidad y la capacidad
Descripción del proceso
Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con la prestación de servicios rentables. Incluir la evaluación de las capacidades actuales, previsión de las necesidades futuras en base a los requerimientos del negocio, análisis de impacto en el negocio, y la evaluación de los riesgos para planificar e implementar acciones para cumplir con los requisitos identificados.
Madurez
Nivel de madurez general

Situación evidenciada
Hallazgos No satisfactorios

COBIT 5 – Proceso BAI04. Gestionar la disponibilidad y la capacidad	
BAI04.01 Evaluar la disponibilidad, el rendimiento y la capacidad de los servicios y recursos para asegurar que la capacidad de coste justificable y el rendimiento están disponibles para las necesidades de negocio de apoyo y entregar los SLA. Crear la disponibilidad, rendimiento y capacidad líneas de base para futuras comparaciones.	**Hallazgos identificados** De acuerdo con la revisión efectuada y sesión obtenida con las diferentes áreas no se ha efectuado una evaluación para la disponibilidad la capacidad y rendimiento de los servicios y recursos. **Conclusiones y recomendaciones** Se recomienda realizar evaluación del rendimiento y la capacidad de los recursos y servicios el cuál sea periódicamente revisado y monitoreado, para que gestione la capacidad y el rendimiento actual, la capacidad y rendimiento futuro, la disponibilidad de recursos de TI.
BAI04.02 Identificar los servicios importantes para la empresa, servicios de mapas y recursos para los procesos de negocio, e identificar las dependencias de negocio. Asegúrese de que el impacto de los recursos no disponibles está totalmente de acuerdo en y aceptado por el cliente. Asegurar que, para las funciones vitales del negocio, los requisitos de disponibilidad SLA pueden ser satisfechas.	**Hallazgos identificados** No se han logrado identificar todos los servicios importantes, así como los servicios y recursos por lo cual no está asegurado que el impacto de los recursos no disponibles este de acuerdo con el cliente. **Conclusiones y recomendaciones** Se recomienda realizar sesiones de trabajo para la identificación adecuada de los servicios y recursos para los procesos de negocio y de esta forma satisfacer los requisitos SLA.
BAI04.03 Planear y priorizar disponibilidad, rendimiento y capacidad de implicaciones, necesidades cambiantes empresariales y requisitos de servicio.	**Hallazgos identificados** De acuerdo con la revisión efectuada con la Dirección de Informática, no se efectúa dicha planeación. **Conclusiones y recomendaciones** Se recomienda realizar un plan en el cual se prioricen los puntos indicados teniendo en cuenta las necesidades cambiantes de los negocios y empresas.
BAI04.04 Monitorear, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad. Identificar las desviaciones de las líneas de base establecidas. Revisar tendencia en informes de análisis de la identificación de cualquier problema y las variaciones significativas, iniciar acciones cuando sea necesario, y garantizar que todas las cuestiones pendientes son objeto de seguimiento.	**Hallazgos identificados** De acuerdo con la revisión realizada, no se realiza ningún monitoreo, ni análisis, ni revisión sobre la disponibilidad, rendimiento y capacidad. **Conclusiones y recomendaciones** Se recomienda establecer un proceso el cual permita realizar un monitoreo, medición, análisis y revisión eficaz de la disponibilidad, rendimiento y capacidad de forma eficaz.
BAI04.05 Direccionar desviaciones mediante investigación y resolución de problemas de disponibilidad, rendimiento y capacidad identificadas.	**Hallazgos identificados** De acuerdo con la revisión efectuada, se determinó que no se realiza investigación adecuada sobre las desviaciones y problemas que se resuelven. **Conclusiones y recomendaciones** Se recomienda elaborar una investigación formal sobre cada desviación encontrada, de igual forma sobre cada problema que se resuelve en la empresa para que estos documentos sirvan para direccionar dichas desviaciones.

COBIT 5 – Proceso BAI05. Gestionar la habilitación del cambio organizativo	
Descripción del proceso	
Maximizar la probabilidad de implementar con éxito el cambio organizacional en toda la empresa sostenible de forma rápida y con menor riesgo, que cubre el ciclo de vida completo de los cambios y todas las partes afectadas en el negocio y TI.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
Hallazgos No satisfactorios	
BAI05.01 Comprender el alcance y el impacto del cambio previsto y de los interesados disposición / voluntad de cambio. Identificar las acciones para motivar a las partes interesadas a aceptar y querer hacer el trabajo de cambio con éxito.	**Hallazgos identificados** No se han identificado las acciones que motiven a las partes interesadas a aceptar cambios en el trabajo. **Conclusiones y recomendaciones** Se recomienda la definición de procedimientos para identificar acciones que motiven a las partes interesadas a aceptar los cambios.
BAI05.02 Establecer un equipo de implementación efectiva mediante el ensamblaje de los miembros apropiados, la creación de confianza, y el establecimiento de objetivos comunes y medidas de efectividad.	**Hallazgos identificados** Si bien existe un equipo de implementación, este no cuenta con los miembros apropiados por lo cual se presenta un cierto déficit en las implementaciones realizadas. **Conclusiones y recomendaciones** Se recomienda evaluar los miembros del equipo de implementación para determinar las medias que deben ser tomadas para su fortalecimiento y así cumplir efectivamente con las implementaciones.
BAI05.03 Comunicar la visión deseada para el cambio en el lenguaje de los afectados por ella. La comunicación debe ser hecha por la alta dirección y la base lógica del, y los beneficios de los cambios, los impactos de no hacer el cambio; y la visión, la hoja de ruta y la	**Hallazgos identificados** No se comunica la visión deseada por parte de la alta dirección de la empresa. **Conclusiones y recomendaciones**

COBIT 5 – Proceso BAI05. Gestionar la habilitación del cambio organizativo	
participación requiere de los diversos grupos de interés.	En este punto se necesita el compromiso formal de la alta dirección para la comunicación de la visión deseada para que de esta forma los interesados tengan conocimiento de todos estos aspectos.
BAI05.04 Capacitar a las personas con funciones de ejecución, asegurando que las responsabilidades se asignan, la capacitación, y la alineación de las estructuras organizativas y procesos de recursos humanos. Identificar y comunicar victorias a corto plazo que se pueden realizar y que son importantes desde una perspectiva de cambio de habilitación.	**Hallazgos identificados** No se capacita a las personas efectivamente en sus funciones. **Conclusiones y recomendaciones** Se recomienda realizar capacitaciones a las personas para que puedan cumplir efectivamente con sus funciones.
BAI05.05 Planificar y ejecutar todos los aspectos técnicos, de explotación y uso de tal manera que todos los que están involucrados en el entorno de estado futuro puedan ejercer su responsabilidad.	**Hallazgos identificados** No se realiza planificación del uso de los aspectos técnicos. **Conclusiones y recomendaciones** Se recomienda realizar un plan de uso y explotación de los aspectos técnicos para que de esta forma los involucrados puedan ejercer sus responsabilidades de manera efectiva.
BAI05.06 Integrar los nuevos enfoques mediante el seguimiento de los cambios implementados, la evaluación de la eficacia del plan de funcionamiento y uso, y el mantenimiento de información continua a través de una comunicación regular. Tomar las medidas correctivas apropiadas, que pueden incluir el cumplimiento de la aplicación.	**Hallazgos identificados** De acuerdo a la revisión efectuada, se determinó que no se efectúa seguimiento cuando se implementa un cambio, de igual forma no se realiza evaluación de eficacia ya que no existe un plan de funcionamiento y uso. **Conclusiones y recomendaciones** Se recomienda realizar el seguimiento adecuado cuando se implementen nuevos cambios e implementar un plan de funcionamiento y uso, con esto se espera mantener una buena comunicación a través de la información continua.
BAI05.07 Sostener los cambios a través de una formación eficaz de nuevo personal, campañas de comunicación en curso, continuo compromiso de la dirección, supervisión adopción y puesta en común de las lecciones aprendidas en toda la empresa.	**Hallazgos identificados** Si bien se da un curso introductorio al nuevo personal, este no se considera eficaz, tampoco se realiza una supervisión continua. **Conclusiones y recomendaciones** Se recomienda realizar modificación al curso de la empresa para que este sea eficaz en la formación del nuevo personal, también se requiere compromiso de la dirección para que se las lecciones aprendidas en toda la empresa sean conocidas por el personal.

COBIT 5 – Proceso BAI06. Gestionar los cambios
Descripción del proceso

COBIT 5 – Proceso BAI06. Gestionar los cambios	
Gestionar todos los cambios de una manera controlada, incluyendo los cambios normales y de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye cambiar las normas y procedimientos, evaluación del impacto, priorización y autorización, los cambios de emergencia, seguimiento, presentación de informes, de cierre y de documentación.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
Hallazgos No satisfactorios	
BAI06.01 Evaluar todas las solicitudes de cambio para determinar el impacto en los procesos de negocios y servicios de TI, y para evaluar si el cambio afectará negativamente al entorno operativo y presentar un riesgo inaceptable. Asegúrese de que los cambios se registran, priorizados, clasifican, evalúan, autorizados, planificadas y programadas.	**Hallazgos identificados** Se realiza una evaluación superficial de los cambios solicitados, dando como resultado que en ocasiones el impacto de dichos cambios sea muy negativo. Si se registran los cambios, pero no se evalúan ni se clasifican ni son aprobados. **Conclusiones y recomendaciones** Se recomienda que la evaluación efectuada sea más detallada para evitar que el impacto de dichos cambios sea negativo, también se recomienda que los cambios sean aprobados, clasificados, priorizados y evaluados antes de ser efectuados.
BAI06.02 Con cuidado, gestionar los cambios de emergencia para minimizar nuevos incidentes y asegúrese de que el cambio está controlado y se lleva a cabo de forma segura. Verificar que los cambios de emergencia son evaluados y autorizados después del cambio apropiadamente.	**Hallazgos identificados** No se gestionan los cambios de emergencia, estos son aplicados en el momento sin ser evaluados ni autorizados. **Conclusiones y recomendaciones** Se recomienda que se implemente un proceso para la gestión de cambios de emergencia, de igual forma que estos sean evaluados y autorizados apropiadamente luego de su aplicación.
BAI06.03 Mantener un sistema de seguimiento y presentación de informes a los cambios de documentos rechazados, comunicar el estado de los cambios aprobados y en proceso, y cambios completos. Asegúrese de que los cambios aprobados se implementan	**Hallazgos identificados** No existe un sistema de seguimiento y presentación de informes sobre los cambios rechazados, aprobados o en proceso. **Conclusiones y recomendaciones**

COBIT 5 – Proceso BAI06. Gestionar los cambios	
como estaba previsto.	Se recomienda la implementación de un sistema de seguimiento y presentación de informes sobre todos los cambios que se rechazan, aprueben o estén en proceso para que de esta forma quede un registro formal y se asegure que todo se implementó como fue previsto.
BAI06.04 Cada vez que se implementan cambios, actualizarán de acuerdo con la documentación de la solución y el usuario y los procedimientos afectados por el cambio.	**Hallazgos identificados** De acuerdo a la sesión efectuada, se determinó que cuando se efectúan cambios, no se actualizan los usuarios ni los procedimientos afectados. **Conclusiones y recomendaciones** Se recomienda que se actualicen cada vez que se efectúen cambios, los usuarios y procedimientos afectados para tener un control adecuado de estos, en casos de revisiones o evaluaciones y para efectos de auditoria.

COBIT 5 – Proceso BAI09. Gestionar los activos	
Descripción del proceso	
Gestionar los activos de TI a través de su ciclo de vida para asegurarse de que su uso proporciona valor a un coste óptimo, que permanecen operativos (apto para el propósito), que se contabilizan como físicamente protegidos, y aquellos activos que son críticos para la capacidad del servicio de soporte son fiables y disponibles. Manejo de licencias de software para asegurarse de que el número óptimo se adquiere, se conserva y se despliega en relación con el uso de negocio requerido, y el software instalado en el cumplimiento de los contratos de licencia.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
Hallazgos No satisfactorios	
BAI09.01 Mantener una puesta al día y registro exacto de todos los activos de TI necesarios para prestar servicios y asegurar la alineación con la gestión de	**Hallazgos identificados** De acuerdo con la revisión efectuada y sesión obtenida con el área de soporte técnico y activos fijos, se corroboro que se mantiene un

COBIT 5 – Proceso BAI09. Gestionar los activos	
la configuración y la gestión financiera.	sistema de activos a nivel contable.
	Conclusiones y recomendaciones
	Se recomienda la implementación de un módulo de activo fijo que lleve un control del ciclo de vida de los activos y no solo a nivel contable.
BAI09.02 Identificar los activos que son críticos en la prestación de servicio y capacidad de dar los pasos necesarios para maximizar su fiabilidad y disponibilidad a las necesidades empresariales de apoyo.	**Hallazgos identificados**
	No se han identificado los activos críticos para la prestación de servicios ya que no se lleva una clasificación detallada de los mismos.
	Conclusiones y recomendaciones
	Se recomienda el desarrollo de una metodología de identificación y clasificación de los activos que permita establecer el mecanismo y/o modelo para la identificación de los activos de la organización como, por ejemplo: - Procesos de negocio o servicios - Datos e información - Aplicaciones de software - Equipos informáticos - Redes de comunicaciones - Equipos auxiliares que soportan los sistemas.
BAI09.03 Administrar los activos a disposición para asegurar se utilizan de forma eficaz y eficiente como sea posible y se contabilizan y protegidos físicamente.	**Hallazgos identificados**
	De acuerdo con la sesión obtenida con el área de soporte y activos fijos cada funcionario firma y obtiene un "Inventario de Activos" que son su responsabilidad sobre su uso y custodia, sin embargo, en esta acta no se detallan las normas y responsabilidades para el uso aceptable de los activos que manejara.
	Conclusiones y recomendaciones
	Se recomienda el desarrollo de una política que detalle las normas y responsabilidades sobre el uso aceptable de los activos de la organización.
BAI09.04 Revisar periódicamente la base de activos en general para identificar formas de optimizar los costes y mantener la alineación con las necesidades del negocio.	**Hallazgos identificados**
	No se revisa la base de datos de activos por lo cual no existe una forma o procedimiento para la optimización de costos
	Conclusiones y recomendaciones
	Se recomienda realizar una revisión cada 6 meses de la base de datos de activos para identificar formas de optimización de costos y de esta forma ayudar a no incurrir en gastos a la empresa.
BAI09.05 Administrar las licencias de software para que el número óptimo de licencias se mantiene a los requerimientos del negocio de soporte y el número de licencias de propiedad es suficiente para cubrir el software instalado en uso.	**Hallazgos identificados**
	Se mantienen las licencias necesarias según el requerimiento del negocio.
	Conclusiones y recomendaciones

COBIT 5 – Proceso BAI10. Gestionar la configuración	
Descripción del proceso	
Definir y mantener las descripciones y las relaciones entre los recursos y capacidades clave requeridas para prestar servicios, incluyendo la recogida de información de configuración, establecer líneas de base, la verificación y la información de configuración de auditoría, y actualizar el depósito de configuración TI.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
Hallazgos No satisfactorios	
BAI10.01 Establecer y mantener un modelo lógico de los servicios, bienes e infraestructuras y la forma de los elementos de registro de configuración (CI) y las relaciones entre ellos. Incluir los elementos de configuración que se consideren necesarios para gestionar servicios de manera eficaz y para proporcionar una única descripción fiable de los activos en un servicio.	**Hallazgos identificados** De acuerdo con la revisión realizada, se identifico que no existe un modelo lógico de los servicios, bienes e infraestructura ni de los registros de configuración. **Conclusiones y recomendaciones** Se recomienda definir y mantener un modelo lógico para la gestión de configuración.
BAI10.02 Establecer y mantener un repositorio de gestión de la configuración y crear líneas de base de configuración controladas.	**Hallazgos identificados** No existe un repositorio completo para la gestión de configuración, el existente es parcial y no se considera fiable. **Conclusiones y recomendaciones** Se recomienda establecer un repositorio completo el cual se pueda considerar fiable y crear las líneas de base para las configuraciones.
BAI10.03 Mantener un repositorio hasta la fecha de los elementos de configuración poblando con los cambios.	**Hallazgos identificados** No existe un repositorio actualizado con los elementos de configuración. **Conclusiones y recomendaciones** Se recomienda la creación de un repositorio a la fecha con todos los elementos de las configuraciones y sus cambios.

COBIT 5 – Proceso BAI10. Gestionar la configuración	
BAI10.04 Definir y producir informes de los cambios de estado de los elementos de configuración.	**Hallazgos identificados**
	De acuerdo con la sesión obtenida, se identificó que no se han definido ni se producen informes con los cambios en los elementos de configuración.
	Conclusiones y recomendaciones
	Se recomienda trabajar en la definición y producción de informes sobre todos los cambios que se efectúan en los elementos de configuración, ya que estos son muy importantes en caso de una incidencia que afecte negativamente los servicios o infraestructura.
BAI10.05 Revisar periódicamente el depósito de configuración y verificar integridad y exactitud contra el objetivo deseado.	**Hallazgos identificados**
	No se realiza esta revisión ya que no existe un depósito ni repositorio de configuración.
	Conclusiones y recomendaciones
	Se recomienda la creación del depósito de configuración y realizar revisiones periódicas del mismo para verificar la integridad de estas.

COBIT 5 – Proceso DSS02. Gestionar las peticiones y los incidentes de servicio	
Descripción del proceso	
Dar una respuesta oportuna y eficaz a las peticiones de los usuarios y resolución de todo tipo de incidentes. Restaurar el servicio normal; registrar y atender las solicitudes de los usuarios; y registrar, investigar, diagnosticar, escalar y resolver incidentes.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
Hallazgos No satisfactorios	
DSS02.01 Definir esquemas y modelos de solicitud de clasificación de	**Hallazgos identificados**

COBIT 5 – Proceso DSS02. Gestionar las peticiones y los incidentes de servicio	
incidentes y de servicios.	De acuerdo con la sesión obtenida, a pesar de que se utiliza un sistema tiquete de solicitud sobre incidentes y servicios, no hay canal formalizado sobre la gestión de estos.
	Conclusiones y recomendaciones
	Se recomienda definir un proceso formal para la gestión de incidentes y de servicios.
DSS02.02 Identificar, registrar y clasificar las solicitudes de servicio e incidentes, y asignar una prioridad de acuerdo a la criticidad de negocios y acuerdos de servicio.	**Hallazgos identificados**
	No se clasifican las solicitudes, No hay definidos tiempos de atención, tiempos de respuesta, no hay definidas prioridades.
	Conclusiones y recomendaciones
	Se recomienda definir un proceso formal para la gestión de incidentes y de servicios.
DSS02.03 Seleccionar los procedimientos de solicitud correspondientes y verificar que las solicitudes de servicio cumplen con los criterios definidos de petición. Obtener la aprobación, si es necesario, y cumplir con las solicitudes.	**Hallazgos identificados**
	No se verifica que las solicitudes cumplan con los criterios necesarios para su atención.
	Conclusiones y recomendaciones
	Se recomienda definir un proceso formal para la gestión de incidentes y de servicios.
DSS02.04 Identificar y guardar registro de incidentes, determinar las posibles causas, y asignar para su resolución.	**Hallazgos identificados**
	Los incidentes solo se registran en el tiquete, estos se asignan a un responsable para su resolución.
	Conclusiones y recomendaciones
	Se recomienda definir un proceso formal para la gestión de incidentes y de servicios.
DSS02.05 Documentar, aplicar y probar las soluciones o alternativas identificadas y realizar acciones de recuperación para restaurar el servicio TI relacionado.	**Hallazgos identificados**
	Las soluciones se aplican, pero no se prueban y solo quedan documentadas en el tiquete.
	Conclusiones y recomendaciones
	Se recomienda definir un proceso formal para la gestión de incidentes y de servicios.
DSS02.06 Comprobar la resolución satisfactoria de incidentes y / o solicitud de cumplimiento, y se cierran.	**Hallazgos identificados**
	No se realiza comprobación de que la solución fue satisfactoria, solamente se cierran.
	Conclusiones y recomendaciones
	Se recomienda definir un proceso formal para la gestión de incidentes y de servicios.
DSS02.07 Regularmente dar seguimiento, análisis y reporte de incidentes y tendencias de Peticiones para proporcionar información para la mejora continua.	**Hallazgos identificados**
	No se da seguimiento ni se generan reportes sobre los incidentes ni se analizan las tendencias sobre estos.
	Conclusiones y recomendaciones

COBIT 5 – Proceso DSS02. Gestionar las peticiones y los incidentes de servicio	
	Se recomienda definir un proceso formal para la gestión de incidentes y de servicios.

COBIT 5 – Proceso DSS03. Gestionar los problemas	
Descripción del proceso	
Identificar y clasificar y problemas de sus causas fundamentales y proporcionar la solución oportuna para evitar incidentes recurrentes. Proporcionar recomendaciones para mejoras.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
Hallazgos No satisfactorios	
DSS03.01 Definir y aplicar criterios y procedimientos para reportar problemas identificados, incluyendo la clasificación problema, categorización y priorización.	**Hallazgos identificados**
	Los problemas son reportados, pero no existen criterios ni procedimientos para su reporte, tampoco cuentan clasificación, priorización ni categorización.
	Conclusiones y recomendaciones
	Se recomienda definir criterios y procedimientos adecuados para el reporte de los problemas, de igual forma que estos sean clasificados, categorizados y priorizados.
DSS03.02 Investigar y diagnosticar problemas utilizando expertos en gestión de temas relevantes para evaluar y analizar las causas de raíz.	**Hallazgos identificados**
	Se determino que se utilizan expertos para la investigación de problemas, sin embargo, los temas no son evaluados ni analizados a profundidad.
	Conclusiones y recomendaciones
	Se recomienda definir un proceso el cual soporte la investigación y análisis de los problemas para identificar sus causas de raíz, así como la generación de informes y reportes de dichos problemas.

COBIT 5 – Proceso DSS03. Gestionar los problemas	
DSS03.03 Tan pronto como se identifican las causas de los problemas, crear registros de errores conocidos y una solución adecuada, e identificar posibles soluciones.	**Hallazgos identificados**
	No existe un registro adecuado de los problemas encontrados
	Conclusiones y recomendaciones
	Se recomienda llevar un registro completo de los problemas encontrados y sobre las soluciones brindadas a los mismos.
DSS03.04 Identificar e iniciar soluciones sostenibles que abordan la causa raíz, aumentando las solicitudes de cambio a través del proceso de gestión de cambios establecido si es necesario para resolver errores. Asegúrese de que el personal afectado es consciente de las medidas adoptadas y los planes desarrollados para prevenir futuros incidentes que se produzcan.	**Hallazgos identificados**
	No se dan soluciones sostenibles a los problemas, El personal afectado no siempre es consciente de las medidas empleadas para la solución de estos.
	Conclusiones y recomendaciones
	Se recomienda revisar de forma continua las soluciones que se dan a los problemas, así como la debida documentación de estas. De igual forma informar a las partes sobre las medidas y planes futuros para resolución de problemas.
DSS03.05 Recoger y analizar datos operativos (especialmente los registros de incidentes y cambios) para identificar las nuevas tendencias que pueden indicar problemas. Registrar los incidentes para permitir la evaluación.	**Hallazgos identificados**
	No se realiza ningún análisis de datos para identificar tendencias sobre los problemas. No se registran los problemas adecuadamente.
	Conclusiones y recomendaciones
	Se recomienda recoger y analizar datos para tener conocimiento sobre las tendencias que indican problemas, de igual forma llevar un registro de los problemas para realizar evaluaciones periódicas.

COBIT 5 – Proceso DSS05. Gestionar los servicios de seguridad
Descripción del proceso
Proteger la información de la empresa para mantener el nivel de riesgo aceptable de acuerdo con la política de seguridad. Establecer y mantener las funciones de seguridad de la información y privilegios de acceso y llevar a cabo la supervisión de seguridad.
Madurez
Nivel de madurez general

COBIT 5 – Proceso DSS05. Gestionar los servicios de seguridad	
	
Situación evidenciada	
Hallazgos No satisfactorios	
DSS05.01 Implementar y mantener medidas de prevención, detección y correctivas (especialmente parches de seguridad y control de virus) a través de la empresa para proteger sistemas de información y la tecnología de software malicioso (por ejemplo, virus, gusanos, software espía, correo no deseado).	**Hallazgos identificados** De acuerdo con la revisión realizada, se determino que la empresa cuenta con un software antivirus, sin embargo, no cuenta con procedimientos definidos ante situaciones de afectaciones por software malicioso o virus. **Conclusiones y recomendaciones** Se recomienda definir procedimientos específicos para situaciones sobre afectación por virus, así como realizar concienciación sobre software malicioso y su prevención.
DSS05.02 Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información sobre todos los métodos de conectividad.	**Hallazgos identificados** No existen procedimientos definidos para la gestión relacionada con medios de conectividad. **Conclusiones y recomendaciones** Se recomienda permitir acceso a la información solo a dispositivos autorizados por la Dirección de TI.
DSS05.03 Asegurar que los puntos finales (por ejemplo, ordenador portátil, de sobremesa, servidores, y otros dispositivos o software móvil y la red) están asegurados a un nivel que es igual o mayor que los requisitos de seguridad definidos de la información procesada, almacenada o transmitida.	**Hallazgos identificados** Los puntos finales cuentan con software antivirus, sin embargo, este no esta bien configurado al igual que el propio sistema operativo. **Conclusiones y recomendaciones** Se recomienda configurar de forma adecuada el sistema operativo y el software antivirus, así como implementar mecanismos de bloqueo en caso de cualquier incidencia.

COBIT 5 – Proceso DSS05. Gestionar los servicios de seguridad	
DSS05.04 Asegurar de que todos los usuarios tengan derechos de acceso a la información, de acuerdo con sus necesidades de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso dentro de los procesos de negocio.	**Hallazgos identificados** De acuerdo con la revisión realizada, se identifico que no existe una asignación definida para el acceso a la información según las necesidades de los usuarios. **Conclusiones y recomendaciones** Se recomienda segregar los usuarios según su función y de esta forma asignar los derechos de acceso a la información adecuados a las necesidades de estos.
DSS05.05 Definir e implementar procedimientos para conceder, limitar y Revocar acceso a los locales, edificios y áreas de acuerdo con las necesidades del negocio, incluidas las emergencias. El acceso a los locales, edificios y áreas debe justificarse, autorizado, registrado y controlado. Esto debería aplicarse a todas las personas que entren en el local, incluido el personal, personal temporal, clientes, proveedores, visitantes o cualquier otro tercero.	**Hallazgos identificados** No existen procedimientos definidos para conceder, limitar y revocar los accesos a los locales, edificios y áreas. **Conclusiones y recomendaciones** Se recomienda definir procedimientos para la concesión, limitación y revocación de accesos.
DSS05.06 Tomar las oportunas precauciones físicas, las prácticas de contabilidad y la gestión de inventarios más activos de TI sensibles, tales como formas especiales, instrumentos negociables, impresoras de propósito especial o tokens de seguridad.	**Hallazgos identificados** No existe definido un procedimiento para la gestión de documentos sensibles y dispositivos de salida. **Conclusiones y recomendaciones** Se recomienda definir un procedimiento para gobernar la recepción, uso, eliminación y destrucción de estos tanto dentro como fuera de la empresa.
DSS05.07 El uso de herramientas de detección de intrusos, monitorear la infraestructura para el acceso no autorizado y garantizar que los eventos están integrados con la supervisión de eventos en general y la gestión de incidencias.	**Hallazgos identificados** De acuerdo con la revisión realizada, se determino que la empresa no hace uso de una herramienta de detección de intrusos ni monitoreo de la infraestructura, por lo cual no hay registro de incidencias. **Conclusiones y recomendaciones** Se recomienda la implementación de una herramienta de monitoreo de incidencias y de detección de intrusos.

COBIT 5 – Proceso MEA01. Supervisar, evaluar y valorar el rendimiento y conformidad
Descripción del proceso
Recoger, validar y evaluar comercial, informático y objetivos del proceso y las métricas. Monitor de procesos que se están realizando en contra acordados en el rendimiento y la conformidad de los objetivos y métricas sin proporcionar detalles que es sistemática y oportuna.

COBIT 5 – Proceso MEA01. Supervisar, evaluar y valorar el rendimiento y conformidad	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
Hallazgos No satisfactorios	
MEA01.01 Comprometerse con las partes interesadas para establecer y mantener un enfoque de monitoreo para definir los objetivos, alcance y método para medir la solución de negocios y la prestación de servicios y la contribución a los objetivos de la empresa. Integrar este enfoque con el sistema de gestión del rendimiento corporativo.	**Hallazgos identificados** No se realizan monitoreos con las partes interesadas para la definición de objetivos, alcances ni método de medición de soluciones de negocio, puesto que no existe un sistema de gestión del rendimiento corporativo. **Conclusiones y recomendaciones** Se recomienda establecer un sistema de gestión del rendimiento corporativo, así como identificar las partes interesadas e involucrarlas para comunicar los objetivos, alcances, etc.
MEA01.02 Trabajar con los interesados para definir, revisar periódicamente, actualizar y aprobar los objetivos de rendimiento y la conformidad del sistema de medición del desempeño.	**Hallazgos identificados** No se realizan revisiones ni se actualizan los objetivos puesto que no hay un sistema de medición del desempeño establecido. **Conclusiones y recomendaciones** Se recomienda establecer un sistema de medición del desempeño en el cual trabajen los interesados, también que se revisen y se actualicen los objetivos de rendimiento.
MEA01.03 Recopilar datos precisos y procesarlos alineado con los requerimientos de la empresa.	**Hallazgos identificados** De acuerdo con la revisión realizada, se determinó que no se recopilan datos por lo cual no existe un proceso de análisis de estos. **Conclusiones y recomendaciones** Se recomienda definir un proceso de recopilación y análisis de datos puntuales que este alineado a los requerimientos de la empresa.
MEA01.04 Periódicamente revisar e informar sobre el rendimiento respecto a los objetivos, utilizando un método que proporciona una vista de todos entorno sucinto de desempeño de TI y encaja dentro del sistema de vigilancia de la empresa.	**Hallazgos identificados** No se realiza revisión ni se informa sobre el rendimiento de desempeño de los objetivos. **Conclusiones y recomendaciones**

COBIT 5 – Proceso MEA01. Supervisar, evaluar y valorar el rendimiento y conformidad	
	Se recomienda definir un proceso de revisión de rendimiento de desempeño de los objetivos, de igual forma diseñar informes que sean concisos, fáciles de entender y alineados a las necesidades de la empresa.
MEA01.05 Ayudar a los interesados en la identificación, la iniciación y seguimiento de las acciones correctivas a las anomalías de dirección.	**Hallazgos identificados**
	No se realiza un seguimiento adecuado de las acciones correctivas, estas solo se aplican.
	Conclusiones y recomendaciones
	Se recomienda dar apoyo a las partes interesadas en todo el proceso de implementación de las acciones correctivas.

6. PRUEBAS DE CONTROL.

Las oportunidades de mejora descritas en las páginas siguientes están clasificadas de acuerdo con la metodología de AKROSERV, definida con base en el riesgo que representan para los recursos tecnológicos (datos, aplicaciones, plataforma tecnológica, instalaciones físicas y personal). Adicionalmente, se presenta el mapa de riesgo el cual resume la relación entre el impacto para la organización y la probabilidad de ocurrencia de eventos que comprometan la efectividad, eficiencia, confidencialidad, integridad, disponibilidad y cumplimiento de los controles implementados.

Los niveles de clasificación se describen a continuación:

7. CATEGORIAS DE RIESGO.

Alto (A)

Representa una deficiencia significativa en los controles relacionados con tecnología e información. Deberá ser atendido lo antes posible.

Medio (M)

Representa una deficiencia en los controles relacionados con tecnología e información. Deberá ser atendido durante los siguientes 30-180 días.

Bajo (B)

Representa una desviación en los controles relacionados con tecnología e información. Deberá ser atendido de acuerdo con la disponibilidad de tiempo de los recursos asignados por la Empresa.

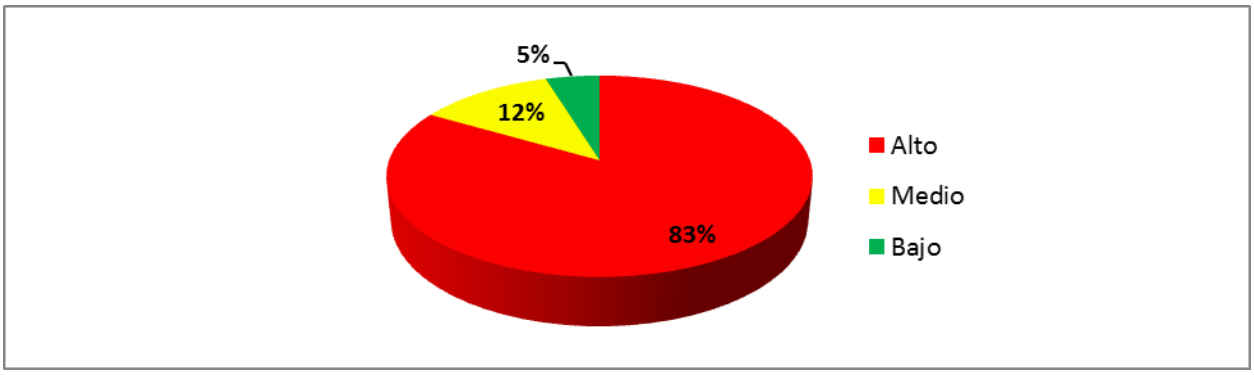
8. CONCLUSIONES DE LA REVISIÓN DE LOS CONTROLES.

Adjunto se detallan a manera de resumen general, las oportunidades de mejora identificadas con una clasificación de nivel de riesgo segregado en tres categorías alto (A), medio (M) y bajo (B), esto para que constituya una herramienta para la priorización de los esfuerzos.

Núm.	Oportunidades de Mejora	Nivel de Riesgo		
		Alto	Medio	Bajo
5.1	Debilidades en el proceso de respaldo de la Información.	✔		
5.2	Debilidades en el proceso de Restauración de información.	✔		
5.3	Debilidades en el proceso de cambios en la Infraestructura Tecnológica.	✔		
5.4	Debilidades en el proceso de respuesta a incidentes.	✔		
5.5	Debilidades en el proceso de Monitoreo de la Infraestructura Tecnológica.	✔		
5.6	Red inalámbrica insegura.	✔		
5.7	Debilidades en la configuración de parámetros de contraseñas.	✔		
5.8	Debilidades en la configuración de cuentas de usuarios y contraseñas.	✔		
5.9	Debilidades en configuración de Cuentas Invitado y Administrador.	✔		
5.10	Debilidades en el Nivel de Actualización de los Servidores Windows Server 2008 R2.	✔		
5.11	Debilidades en los Privilegios Sysadmin.	✔		
5.12	Debilidades en cuentas contraseñas null.	✔		
5.13	Debilidades en la Autenticación del Sistema.	✔		
5.14	Debilidades en la identificación de Responsables de Eventos o sucesos.	✔		
5.15	Cuentas Activas de Exfuncionarios.	✔		
5.16	Debilidades en el uso de cuentas genéricas.	✔		
5.17	Bitácoras de seguridad no confiables.	✔		
5.18	Debilidades en el proceso de asignación de privilegios administrativos	✔		
5.19	Registros contables que no reflejan el usuario que lo realizó.	✔		
5.20	Debilidades en el proceso de cambios al sistema.	✔		
5.21	Debilidades en el Plan de Pruebas del Sistema.	✔		

Núm.	Oportunidades de Mejora	Nivel de Riesgo		
		Alto	Medio	Bajo
5.22	Debilidades en el Uso de Software.	✔		
5.23	Debilidades en el Ambiente de Prueba.	✔		
5.24	Plan de Tecnología.	✔		
5.25	Plan de Continuidad de Negocio.	✔		
5.26	Plan Estratégico de Tecnología de Información.	✔		
5.27	Medidas de protección de equipos de Centro de Datos.	✔		
5.28	Centro de Datos alterno.	✔		
5.29	Ausencia de centralización de Contratos.	✔		
5.30	Dependencia del Proveedor de Internet.	✔		
5.31	Estandarización de Servidor Windows Server 2012.	✔		
5.32	Plan de Seguridad TI.	✔		
5.33	Ausencia de Análisis de Vulnerabilidades periódicas.	✔		
5.34	Ausencia de uso estandarizado de las versiones de las licencias del Sistema ASPELCOI- ASPEL BANCO.	✔		
5.35	Ausencia de Metodología utilizada para análisis de requerimientos, diseño, programación, pruebas e implementación en el ambiente de producción.	✔		
5.36	Ausencia de políticas que garanticen la seguridad de la Información.		✔	
5.37	Actualización de Políticas y Procedimientos de TI.		✔	
5.38	Aprobación de Políticas.		✔	
5.39	Matriz de Riesgo de TI.		✔	
5.40	No existe una interfaz automática entre ASPEL COI – ASPEL BANCO y los demás sistemas desarrollados en casa.		✔	
5.41	Ausencia de Organigrama de TI.			✔
5.42	Ausencia del Diagrama de Red LAN y WAN.			✔

9. ESTADÍSTICAS DE LA EJECUCIÓN DEL PROGRAMA DE TRABAJO.



Como resultado de la evaluación, se identificaron un total de 42 oportunidades de mejora, las cuales se describen en esta sección y son clasificadas en tres categorías de riesgo de la siguiente forma:

35 riesgo Alto
5 riesgo Medio
2 riesgo Bajo

10. DESCRIPCIÓN DE LAS OPORTUNIDADES DE MEJORA DEL PROGRAMA DE TRABAJO.

Hallazgo Nº 5.1	Debilidades en el proceso de respaldo de la Información		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se denota que el proceso de respaldo fue realizado de manera manual y los respaldos para cada base de datos se efectúa de manual, por lo que, se procedió a revisar la configuración establecida para las notificaciones del respaldo exitoso o fallido, y se identificó que no existe tal alerta de aviso, tampoco cuenta con bitácora de registro de respaldos, ni almacenamiento externo que pueda ser almacenado en una CINTOTECA.

Impacto
La ausencia de herramientas automatizada que contribuyan a la eficiencia del proceso de respaldo, los lineamientos adecuados para la realización de respaldos, la ausencia de notificaciones que indiquen falla en el respaldo, la falta de control en bitácoras que registren los respaldos realizados de manera exitosa y la ausencia de equipo contingente para replicar los respaldos en otro disco externo que tenga la protección y ubicación adecuada en el Centro de Datos, incrementa el riesgo de que no se cuente con la información de los sistemas de manera oportuna en caso de un evento inesperado y que los procesos no puedan ser activados de manera oportuna para su correcto funcionamiento.

Recomendación
Se recomienda a la Empresa analizar la posibilidad de contar con una herramienta de respaldo automatizada, así mismo la definición de lineamientos de respaldo acorde a las sanas prácticas de seguridad, además, proceder a configurar el acuse de respaldos tanto fallidos como exitosos, contar con una bitácora donde se lleve el control de cada respaldo, y de igual manera la implementación de un disco externo donde se repliquen los respaldos realizados de manera exitosa, y que esté ubicado en el fuera del Centro de Datos, según lo orientan las sanas prácticas. COBIT:(Ds4 Asegurar el Servicio Continuo).

Hallazgo Nº 5.2	Debilidades en el proceso de Restauración de información		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se denota que no existen establecidos lineamientos para realizar el proceso de restauración de la Información periódicos, así mismo no se cuenta con una herramienta automática que permita la ejecución de esta acción de acuerdo a las sanas prácticas, por lo tanto no se realizan pruebas de restauración de las copias de respaldos de los sistemas críticos, y durante la fecha de revisión se verificó que los procesos ejecutados de manera intuitiva se llevan a cabo de manera manual, sin embargo no se cuenta con controles de registro de restauraciones en bitácoras y no se han configurado las notificaciones correspondientes para que le informen al responsable que la restauración fue exitosa o fallida.

Impacto
La ausencia de una herramienta automatizada de restauración que permita obtener notificaciones que indiquen falla o éxito en la restauración, incrementa el riesgo de que no se cuente con la información de los sistemas de manera oportuna en caso de un evento inesperado. Y la falta de una bitácora de control de restauración incrementa el riesgo de que no se lleve un consecutivo de la realización de restauraciones realizadas. En donde se puede garantizar la integridad y disponibilidad de la información almacenada en los medios de respaldos de la Empresa.

Recomendación
Se recomienda a la Empresa realizar un análisis para contar con una herramienta automatizada que les permita configurar los acuses de restauraciones tanto fallidos como exitosos. Además, contar con una bitácora donde se lleve el control de cada restauración realizada, de acuerdo con las sanas prácticas. COBIT:(Ds4 Asegurar el Servicio Continuo).

Hallazgo Nº 5.3	Debilidades en el proceso de cambios en la Infraestructura Tecnológica		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
De la revisión, se denota que no existen controles relacionados para realizar los cambios en la Infraestructura de la Empresa. En reunión con la Gerencia de TI, explicó que cuando se realizan cambios programados o no programados en los equipos y componentes de TI, no son registrados en una bitácora por el encargado de realizar el cambio. De igual manera, no se han definido procedimientos de cambios de equipos o reemplazo de piezas.

Impacto
La ausencia de políticas que definan los lineamientos adecuados para el control de cambios en los equipos de Tecnología maximiza la probabilidad de interrupciones, alteraciones no autorizadas y errores, incrementando el riesgo de que no se cuente con la información de los sistemas de manera oportuna en caso de un evento inesperado.

Recomendación
Se recomienda a la Empresa la definición de una metodología de Control de cambios que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual, y tomar en consideración: 1. Identificación de cambios tanto internos como por parte de proveedores. 2. Procedimientos de categorización, priorización y emergencia de solicitudes de cambios. 3. Evaluación del impacto que provocaran los cambios. 4. Autorización de cambios. 5. Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc. 6. Distribución de software, estableciendo medidas de control específicas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna. Acorde a lo que indican las sanas prácticas. COBIT:(AI6 Administración de los cambios).

Hallazgo Nº 5.4	Debilidades en el proceso de respuesta a incidentes		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
En la Empresa no existe un documento formal donde se defina la manera llevar a cabo dicha gestión de incidentes, que incluya: ▪ Alcance de la política. ▪ Procedimiento de gestión de incidentes. ▪ Responsables de resolver el incidente de acuerdo con el área que corresponde. ▪ Registro de incidente en la base de conocimiento. Tampoco cuentan con una herramienta de gestión de incidentes que lleve el control de los registros de problemas que ocurren en la Empresa, la manera de resolverlo, indicadores de solución de incidentes, usuarios que solicitan mayormente apoyo por parte del Dpto. desempeño por parte del personal de TI asignado a cada incidente.

Impacto
La ausencia de un Sistema de Incidentes disminuye la capacidad de respuesta en tiempo y forma por parte del equipo de la Gerencia de TI, además, incrementa la Insatisfacción del usuario por no ser atendida su solicitud a tiempo. Finalmente, no sé asigna la solicitud del usuario a la persona adecuada y experta en el área.

Recomendación
Se recomienda a la Empresa se lleve a cabo la Implementación de un Sistema de Gestión de Incidentes y la definición de políticas para llevar a cabo esta actividad, y agilizar el tiempo de respuesta a las solicitudes de los usuarios. De acuerdo con lo sugerida en las sanas prácticas. (COBIT DS3: Gestionar incidentes).

Hallazgo Nº 5.5	Debilidades en el proceso de Monitoreo de la Infraestructura Tecnológica		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se denota la existencia de controles de monitoreo del Enlace a Internet de la Empresa, mediante el Software SOLARWINDS facilitada por el proveedor con quien se contrató el Servicio, sin embargo, no existen establecidos lineamientos para realizar el proceso de Monitoreo de la Infraestructura de TI, así mismo no se cuenta con una herramienta automática que permita la revisión constante y permanente de los equipos de tecnología de la Empresa, la cual alerte en caso de una falla en alguno de los equipos.

Impacto
La ausencia de una Herramienta de Monitoreo de la Infraestructura Tecnológica incrementa el riesgo de no contar con la información disponible en tiempo y forma, ya que no se podrá obtener notificación precisa y efectiva del estado de los equipos donde se aloja la información, para poder realizar revisiones puntuales preventivas y correctivas.

Recomendación
Se recomienda a la Empresa contar con una Herramienta de monitoreo de la Infraestructura Tecnológica que permita la revisión constante de los servidores, y demás equipos de seguridad y comunicaciones. COBIT:(Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.6	Red inalámbrica insegura		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se denota que la Empresa ha diseñado controles relacionados con la seguridad del acceso a la red inalámbrica, sin embargo, no existe un documento formal al respecto donde se defina la manera de implementar: **Alcance de la política** - Estándar de seguridad inalámbrico. - Cifrado implementado. - Protocolo y Servidor de autenticación. - Permisos de acceso a la red inalámbrica. Para evaluar los controles del Esquema de seguridad inalámbrica implementada por la Empresa, en reunión con la Gerencia de TI, se solicitó la configuración establecida en los equipos inalámbricos de AKROSERV, determinando que la seguridad establecida en los protocolos es inadecuada según las sanas prácticas, estas debieron modificarse al instalar el equipo en la Red de la Empresa, para evitar dejar las políticas que trae por defecto el equipo.

Impacto
La ausencia de políticas y procedimientos documentados, aprobados y divulgados respecto a la seguridad inalámbrica podría originar que las actividades relacionadas con la seguridad de los recursos informáticos, no se desarrolle de manera eficiente, se omitan procedimientos específicos o se violenten en forma deliberada, aspectos relacionados con la seguridad de la información de la Empresa y del equipo computacional.

Recomendación
Documentar, aprobar y comunicar a todos los usuarios las políticas y procedimientos de seguridad de la información relacionados con: - Seguridad inalámbrica Además, debe existir un procedimiento para hacer del conocimiento de los usuarios, las políticas y procedimientos de seguridad de la información. (COBIT: AI4 Desarrollo y mantenimiento de procedimientos.).

Hallazgo Nº 5.7	Debilidades en la configuración de parámetros de contraseñas		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo

Se identificó la existencia de controles relacionados con la configuración de contraseñas en el ambiente de TI, con el propósito de restringir el acceso a usuarios no autorizados a la información y las aplicaciones mediante el uso de contraseñas seguras en todos los ambientes tecnológicos con los que cuenta. Se identificó la existencia de una política de seguridad, donde se indica lo siguiente relacionado con las políticas de contraseñas en los sistemas operativos:

El formato o nomenclatura de las contraseñas, debe cumplir lo siguiente:

1er Carácter: Letra Mayúscula

2do al 6to Carácter: Letras Minúsculas

7mo al 10mo Carácter: Numérico, o Símbolos

Sin embargo, durante la revisión de las políticas implementadas en el Directorio Activo (Active Directory) de la Empresa, se identificó que no están debidamente configuradas.

Impacto

Configuración y cambios malintencionados en las transacciones que se pueden registrar por parte de usuarios no autorizados a generarlas. Se compromete la información de la Empresa, en lo que respecta a acceso inadecuado y divulgación de información sensitiva, además atentar validez y confiabilidad de la información.

Recomendación

Establecer políticas de parametrización de contraseñas en el Directorio Activo (Active Directory) y los sistemas de aplicación, de acuerdo con lo sugerida a las sanas prácticas informáticas:

Política	Valor
Vencimiento	30- 90 días
Históricos	6 o más
Complejidad	Activada
Bloqueo	3-6 intentos.

Hallazgo Nº 5.8	O.M Debilidades en la configuración de cuentas de usuarios y contraseñas(A)		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo

La Empresa ha diseñado controles relacionados con la creación de cuentas de usuarios y modificaciones de usuarios en el servidor de dominio de la Empresa.

Durante la revisión se observó lo siguiente:

Las solicitudes de ingreso son enviadas vía correo electrónico por las jefaturas de cada área.

Existe una política de seguridad, donde se indica lo siguiente:

La cuenta debe ser construida de la siguiente manera:

1erLetra del PrimerNombre.1erApellido: Ej. **fsaavedra**

Cuentas de correo electrónico:

La cuenta debe ser construida de la siguiente manera, 1era letra nombre apellido@dominio

fsaavedra@akroserv.com

Se realizó una revisión de las cuentas de usuario con el fin de verificar que los identificadores de las cuentas cumplen con el estándar definido por el departamento.

Los resultados obtenidos de dicha revisión son los siguientes:

Existen **14 cuentas** de usuario con un identificador que no cumple con lo establecido en las políticas y procedimientos del departamento de las cuales **13 están activas**. Las cuentas tienen poco detalle en su descripción.

Se realizó una revisión de las cuentas de usuario con el fin de verificar que las políticas establecidas en la configuración de la contraseña.

Los resultados obtenidos en dicha revisión son los siguientes:

Se observó la existencia de **15 cuentas de usuario activos**, **cuya contraseña no expira**. No existe un documento debidamente autorizado que justifique esta configuración.

Impacto

La utilización de usuarios que no cumplen con el estándar establecido de creación de usuarios podría dificultar las labores de administración e identificación de responsables ante el eventual uso no autorizado de estos usuarios por parte de personas malintencionadas que obtengan las contraseñas de forma deliberada.

Recomendación

Eliminar los usuarios que no cumplen con el estándar de la plataforma tecnológica y crearlos cumpliendo la nomenclatura definida, en el eventual caso de requerir el uso estricto de este tipo de usuarios, se debe mantener una lista formal en donde se autoricen su uso y se indique cual será el responsable de estas cuentas. (COBIT: Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.9	Debilidades en configuración de Cuentas Invitado y Administrador		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
1. Se puede observar que la cuenta de usuario Administrador no se encuentra renombrada de acuerdo con las sanas prácticas de seguridad. 2. 2. Se observó que la cuenta Invitado, creada por el instalador del gestor de la red Windows Server 2012 R2 se encuentra activada, incumpliendo con las sanas prácticas de seguridad.

Impacto
La utilización de usuario Invitado y Administrador que no cumplen con el estándar establecido, podría dificultar las labores de administración e identificación de responsables ante el eventual uso no autorizado de estos usuarios por parte de personas malintencionadas que obtengan las contraseñas de forma deliberada.

Recomendación
Desactivar la cuenta Invitado y renombrar el usuario Administrador para garantizar la seguridad de accesos a los equipos y sistemas de la Empresa. (COBIT: Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.10	Debilidades en el Nivel de Actualización de los Servidores Windows Server 2008 R2		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
Los servidores son Sistema Operativo Windows Server 2008 R2 se encuentran desactualizados, tienen instalado el service pack 1, y la última versión liberada por el proveedor es el service pack 2.

Impacto
Los service packs o paquetes de servicio son actualizaciones generadas por los proveedores de los sistemas operativos y bases de datos para corregir vulnerabilidades importantes detectadas por ellos mismos. El hecho es que dichas actualizaciones no estén aplicadas en los sistemas operativos y bases de datos incrementa el riesgo de eventuales errores en los sistemas y exposición a vulnerabilidades que pueden ser aprovechadas por el software malicioso, usuarios malintencionados para dañar o alterar la información.

Recomendación
Se recomienda a la Empresa la posibilidad de instalar los últimos paquetes de servicios distribuidos por los fabricantes. Se debe establecer un control debidamente documentado de las actualizaciones que los proveedores como Microsoft, liberan al mercado en donde se evidencie la valoración que justifique la necesidad, ventajas y riesgos de implementar una actualización. La administración debe estar informada de los análisis que al respecto se realicen. COBIT: Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.11	Debilidades en los Privilegios Sysadmin		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se denota que la Empresa no ha diseñado controles relacionados con la seguridad del Sistema ASPEL y su base de datos PARADOX, acorde a las sanas prácticas de seguridad de los perfiles de usuario administrador.

No existen políticas establecidas para definir la seguridad de los componentes del Sistema, ya que no se logra tener control sobre el aplicativo y realizar implementación de controles de seguridad a las bases de datos.

Impacto

El uso de cuentas con rol *Sysadmin* que no correspondan al usuario *"sa"* en la base de datos del sistema, incrementa el riesgo del ingreso de usuarios no autorizados que puedan afectar la integridad, disponibilidad y confidencialidad de la información de la Empresa.

Recomendación

Se recomienda la eliminación de cuentas con rol Sysadmin en la base de datos del sistema que no estén debidamente justificadas, para evitar accesos no autorizados a la misma.

Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

1. Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso.

2. Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario.

3. Administración de llaves criptográficas definiendo, implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de estas.

4. Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de estos.

Acorde a lo que indican las sanas prácticas. COBIT:(Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.12	Debilidades en cuentas contraseñas null		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se denota que no se cuenta con configuración de contraseñas en el Sistema, ya que quien instala la base de datos es el proveedor del sistema. Por lo tanto, no se tiene control total del aplicativo para realizar cambios a los sistemas, y de igual manera no se permite el acceso a implementar seguridad en las bases de datos.

Impacto
El uso de cuentas cuya contraseña no es requerido en la base de datos del sistema, incrementa el riesgo del ingreso de usuarios no autorizados que puedan afectar la integridad, disponibilidad y confidencialidad de la información de la Empresa.

Recomendación
Se recomienda la eliminación de cuentas cuya contraseña no es requerido en la base de datos del sistema, para evitar accesos no autorizados a la misma. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración: **1.** Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso. Acorde a lo que indican las sanas prácticas. COBIT:(Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.13	Debilidades en la Autenticación del Sistema		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se denota que no existen parámetros establecidos por la Empresa en el servidor del Sistema acorde a las sanas prácticas de seguridad, mediante la revisión de propiedades de autenticación establecidas en la base de datos del Sistema, ya que no se tienen permisos como Empresa para ingresar a la base.

Impacto
Las debilidades en la Autenticación del Sistema impiden salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida.

Recomendación
Se recomienda la implementación de controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración: • Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso. • Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario. Acorde a lo que indican las sanas prácticas. COBIT:(Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.14	Debilidades en la identificación de Responsables de Eventos o sucesos		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
Se solicitó la revisión de los permisos basado en los roles de cada usuario según perfil para las operaciones en el Sistema. En reunión con la Gerencia TI, se solicitó la lista de usuarios que ingresan al Sistema ASPEL. Se observan los permisos de operaciones que se les brindan a los usuarios en dependencia del perfil en el Sistema ASPEL. Existe un usuario el cual tiene permisos en el sistema para eliminar registros. Sin embargo, observamos que no es posible llevar a cabo la acción de eliminar por debilidades en la seguridad del ASPEL, razón por la cual acude al responsable de sistemas en TI para que proceda a eliminar según solicitud. Por tanto, no es posible garantizar la veracidad de las operaciones que cada usuario tiene asignado en su perfil.

Impacto
La deficiencia en la configuración de parámetros de seguridad relacionados a la identificación adecuada de responsables de eventos o sucesos incrementa el riesgo de que la información de los sistemas críticos pueda ser fácilmente obtenida por usuarios, que podrían atentar contra la validez de esta.

Recomendación
Implementar controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados, mediante la definición de perfiles de usuarios, donde se detalle los permisos que corresponden a sus responsabilidades, y a los sistemas que pueden ingresar. Acorde a lo que indican las sanas prácticas. COBIT:(Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.15	Cuentas Activas de Exfuncionarios		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
Se realizó una revisión de las cuentas de usuario con el fin de verificar que no existen transacciones que puedan ser realizadas por usuarios que ya han sido dados de baja en RRHH y notificados a TI. Los resultados obtenidos de dicha revisión son los siguientes: Existen 12 cuentas de usuario que están dados de baja en RRHH y aparecen Activos en el Active Directory.

Impacto
La existencia de exfuncionarios activos en las aplicaciones podría dificultar las labores de administración e identificación de responsables ante el eventual uso no autorizado de estos usuarios por parte de personas malintencionadas que hagan uso de los permisos y privilegios otorgados mientras laboraban para la Empresa.

Recomendación
Llevar un estricto control y seguimiento a las bajas de usuarios, y de esta manera garantizar la seguridad de la información, restringiendo completamente todos los permisos del usuario que ha sido dado de baja. (COBIT: Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.16	Debilidades en el uso de cuentas genéricas		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
Durante la revisión se identificó que no se cuentan con lineamientos establecidos para el uso de cuentas genéricas, cuya descripción nos indique la naturaleza de estas. Además, no existe un documento debidamente autorizado que justifique la existencia y el responsable de cada cuenta. Se identificaron **10 cuentas** de usuarios genéricos. De las cuales **9** están activas.

Impacto
El uso de usuarios genéricos podría dificultar las labores de administración e identificación de responsables ante el eventual uso no autorizado de estos usuarios por parte de personas malintencionadas que obtengan las contraseñas de forma deliberada.

Recomendación
Evaluar la posibilidad de eliminar los usuarios genéricos de la plataforma tecnológica, en el eventual caso de requerir el uso estricto de este tipo de usuarios, se debe mantener una lista formal en donde se autoricen su uso y se indique quién será el responsable de estas cuentas. (COBIT: Ds5 Garantizar la seguridad de sistemas)

Hallazgo Nº 5.17	Bitácoras de seguridad no confiables		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se observó que existen debilidades en los Servidores del Sistema ya que no se están cumpliendo con las sanas prácticas de seguridad. La ruta es: Start > Programs > Administrative Tools > User Manager for Domains > Policies Menu >Audit Policy.

Impacto
La deficiencia en la configuración de parámetros de seguridad relacionados a la configuración de las políticas de auditoría incrementa el riesgo de que la información de los sistemas críticos pueda ser fácilmente obtenida por usuarios, que podrían atentar contra la validez de la misma.

Recomendación
Definir políticas de seguridad que permitan establecer los parámetros de sanas prácticas en el Servidor de Windows. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios no autorizados. (COBIT: Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.18	Debilidades en el proceso de asignación de privilegios administrativos.		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, la Empresa no tiene establecidos controles para otorgar los privilegios de súper usuario, siendo otorgado únicamente a la persona encargada según su perfil de puesto y autorizado.

Impacto
La deficiencia en la asignación de privilegios incrementa el riesgo de que la información de los sistemas críticos pueda ser fácilmente obtenida por usuarios, que podrían atentar contra la validez de esta.

Recomendación
Definir y establecer una política para la asignación de privilegios administrativos. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios no autorizados. (COBIT: Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.19	Registros contables que no reflejan el usuario que lo realizó		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión de los asientos contables, se denota que el Sistema ASPEL no permite identificar a los usuarios que realizan registros de asientos contables en el Sistema. Se me indicó que el sistema no cuenta con este tipo de control.

Impacto
Cuando las transacciones contables no indican el usuario que las realiza, se incrementa el riesgo que, ante el eventual caso de transacciones no autorizadas, se dificulte el proceso de identificación oportuna y eficiente de responsables, lo cual podría comprometer la integridad de la información.

Recomendación
Definir y establecer un control para poder identificar a los usuarios que registran y aprueben asientos contables dentro del sistema Financiero Contable. (COBIT: Ds5 Garantizar la seguridad de sistemas).

Hallazgo Nº 5.20	Debilidades en el proceso de cambios al sistema		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se denota que la Empresa no tiene establecidos controles para realizar los cambios en el sistema. En reunión con la Gerencia TI, explicó que no se pueden realizar cambios al Sistema debido a que no cuentan con el código fuente del aplicativo.

Impacto
La ausencia de procesos de cambios al sistema incrementa la probabilidad de interrupciones, alteraciones no autorizadas y errores.

Recomendación
Se recomienda a la Empresa contar con procedimientos de cambios debidamente documentados y aprobados, que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a los sistemas de Información, tomando en consideración: 1. Identificación de cambios tanto internos como por parte de proveedores 2. Procedimientos de categorización, priorización y emergencia de solicitudes de cambios. 3. Evaluación del impacto que provocaran los cambios. 4. Autorización de cambios 5. Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc. De acuerdo con las sanas prácticas. COBIT:(AI6 Administración de los cambios).

Hallazgo Nº 5.21	Debilidades en el Plan de Pruebas del Sistema		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se denota que la Empresa no tiene establecido controles para realizar pruebas con las modificaciones solicitadas por el usuario final. En reunión con la Gerencia de TI, nos explicó que no cuentan con un plan de pruebas dado que no se pueden hacer cambios al Aplicativo porque no tienen el código fuente.

Impacto
La ausencia de plan de pruebas de los sistemas críticos incrementa el riesgo de que no se cumplan con los requerimientos solicitados por los usuarios, ya que no se lleva una planificación de actividades para realizar el requerimiento en base a pruebas.

Recomendación
Se recomienda el debido cumplimiento de un plan de pruebas de requerimientos de usuarios, para garantizar que lo solicitado por el usuario esté acorde a lo entregado. (COBIT: AI2. Adquisición y mantenimiento del software aplicativo).

Hallazgo Nº 5.22	Debilidades en el uso de Software		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se denota la existencia de controles relacionados con el Uso de software no licenciado por parte de los usuarios finales. El área de TI ha definido una política de seguridad, donde se indica lo siguiente relacionado con los programas sin autorización de instalación: ***5.5.2 De Software. - RESPONSABILIDAD DE IT"*** a) Instalar el Software autorizado por la Gerencia IT. b) No instalar Software pirata en los equipos informáticos. c) Los Software gratuitos deben ser autorizados por la Gerencia IT para su instalación. d) Soporte técnico debe garantizar las seguridad y resguardo del Software proporcionado por la Gerencia IT para las instalaciones en los equipos informáticos. e) No deben instalarse estos Software en equipos externos o que no pertenezcan a los activos de AKROSERV. Sin embargo, en las políticas de grupo del Active Directory están desactivadas las propiedades de bloqueo de instalación de programas.

Impacto
La ausencia de políticas que definan los lineamientos del uso e instalación apropiados de Software, ponen en riesgo la seguridad de la información y a su vez la imagen corporativa de la Empresa, ya que pueden generar un conflicto con los proveedores del software por derechos reservados.

Recomendación
Se recomienda a la Empresa la configuración de políticas y definición de lineamientos de Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo. (COBIT: AI2. Adquisición y mantenimiento del software aplicativo).

Hallazgo Nº 5.23	Debilidades en el Ambiente de Prueba		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A través de la revisión, se identificó que la Empresa no tiene un ambiente de pruebas establecido para realizar pruebas, previo a realizar el pase o traslados al ambiente de producción, en reunión con la Gerencia de TI, nos explicó que aún no han implementado esta seguridad que les permita proteger las operaciones de la Empresa por falta de recursos.

Impacto
La ausencia de un ambiente de pruebas independiente limita la capacidad de brindar una respuesta oportuna a los usuarios ante un requerimiento, además pone en riesgo los procesos de negocio ya puede quedar fuera de línea el ambiente de producción por saturar el rendimiento del Servidor.

Recomendación
Se recomienda a la Empresa la implementación de un servidor de pruebas, para garantizar la seguridad del sistema en caso de modificaciones al mismo, según las sanas prácticas. (COBIT: AI2. Adquisición y mantenimiento del software aplicativo).

Hallazgo Nº 5.24	Plan de Tecnología		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A la fecha de revisión el área de TI de AKROSERV tiene definidas responsabilidades a cada personal del Dpto. TI de acuerdo con su experiencia, sin embargo, no cuenta con un plan de Tecnología al periodo auditado, para poder asignar las actividades y darle seguimiento al cumplimiento de metas y objetivos. Se apoyan en una tabla de objetivos para llevar el control de lo que debe realizarse bajo supervisión de otras áreas.

Impacto
No se cuenta con un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar los logros futuros, ya que la realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo que brinden un alto nivel estratégico en el área de TI.

Recomendación
Se recomienda a AKROSERV, definir un Plan de Tecnología que involucre las áreas claves de las operaciones tecnológicas, considerando la definición de objetivos de negocio y necesidades de TI, y desarrollando e implementando planes a largo y corto plazo que satisfagan la misión y las metas generales de la Empresa. Además, se deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes. (COBIT: PO1 Definición de un plan Estratégico).

Hallazgo Nº 5.25	Plan de Continuidad de Negocio		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A la fecha de revisión, se determinó que AKROSERV no cuenta con un plan de continuidad del negocio probado y funcional, que esté alineado con los requerimientos del negocio.

Impacto
La ausencia de un Plan de Continuidad del Negocio incrementa el riesgo de no poder garantizar la disponibilidad de los ciclos del negocio, sus funciones y procesos en caso de un incidente, ya que no cuentan con estrategias de Disponibilidad del Servicio.

Recomendación
Se recomienda a la Empresa desarrollar un plan de continuidad de Negocio para garantizar la Alta disponibilidad del servicio brindado por la Empresa, de acuerdo con lo sugerida en las sanas prácticas. (COBIT: Ds4 Asegurar el Servicio Continuo), Este plan debe incluir lo siguiente: A. Análisis del impacto en un evento desfavorable para el negocio. B. Análisis y evaluación de riesgo determinado para cada proceso crítico. C. Estrategia de continuidad ante una contingencia. D. Manejo de crisis durante el período en que se presenta la contingencia. E. Respuesta de emergencia, desarrollo y documentación del plan. F. Pruebas del plan ante una contingencia y su mantenimiento.

Hallazgo Nº 5.26	Plan Estratégico		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
Durante la revisión, se identificó que no existe una estrategia documentada de Tecnología a corto y largo plazo que apoye la estrategia general del negocio e integre las necesidades de todas las áreas de la Empresa.

Impacto
La ausencia de una adecuada estrategia de tecnologías de información a mediano y largo plazo podría implicar a futuro las siguientes situaciones: •Costo creciente y poco controlado de la tecnología informática. •Problemas o inconsistencia en la ejecución del presupuesto anual. •La inversión real total podría ser más alta y menos productiva que una inversión planeada a mediano y largo plazo. •Falta de atención a problemas específicos que podrían generar una subutilización de los recursos informáticos y una sub-productividad del usuario, entre otros. •Desarrollo tecnológico inconsistente con las metas y objetivos corporativos.

Recomendación
Formalizar la estrategia de tecnologías de información a mediano y largo plazo en función de los objetivos y metas de la Empresa. •Identificar recursos adecuados e incluir presupuestos detallados para el área de Tecnología de Información que estén acordes con los objetivos de la Empresa. •La estrategia debe ser dinámica, incluyendo mecanismos para supervisión y actualización anual. •Incluir dentro de la estrategia el plan anual de Sistemas que incluya: cronogramas de las actividades a desarrollar durante el año y recursos requeridos por cada uno de los proyectos en curso. (COBIT: PO1 Definición de un plan Estratégico).

Hallazgo Nº 5.27	Medidas de protección de equipos de Centro de Datos		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A la fecha de revisión se determinó que en el actual cuarto de comunicaciones de AKROSERV se encuentran equipos tecnológicos ubicados en sus respectivos Rack de comunicaciones, hay extinguidores en caso de incendios y alarmas que alerten cualquier eventualidad que ocurra dentro del sitio, pero no se cuenta con una buena climatización. Sin embargo, se identificó que los equipos tecnológicos no cuentan con el debido etiquetado para su debida administración, además el cuarto de comunicaciones no está cerrado en su totalidad ya que las puertas de acceso son convencionales y comparte aire acondicionado con el área de TI, exponiendo los equipos tecnológicos a filtro de polvo y humedad.

Impacto
El mantenimiento insuficiente en el Centro de Datos provoca un ambiente físico inconveniente para proteger los equipos y al personal de TI contra peligros naturales (fuego, polvo, calor excesivo) o fallas humanas que implica un riesgo para la Continuidad del Negocio.

Recomendación
Se recomienda a la Empresa la implementación de los siguientes aspectos sugeridas por las sanas prácticas: (COBIT: Ds12 Administración de las instalaciones, Ds4 Asegurar la continuidad del Negocio, AI3 Adquisición y mantenimiento de la infraestructura tecnológica) 1. Etiquetado tanto en el cableado, como en los Equipos Tecnológicos, que incluya: Rotulación de cables de red, Rack de Equipos, Slot, Equipo de conexión, Número de puerto. 2. Ubicar todos los equipos tecnológicos en Rack, (Ej.: Servidor de Aplicaciones) 3. Garantizar mejoras al espacio físico del centro de Datos, cerrar completamente el espacio entre las puertas de acceso y el techo ya que hay riesgo de filtración de polvo y filtración de humedad.

Hallazgo Nº 5.28	Centro de Datos Contingente		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A la fecha de revisión la Empresa cuenta con un Cuarto de Comunicaciones ubicado en Managua, sin embargo, no se cuenta con un Centro de Datos Contingente en caso de ocurrir un desastre en las instalaciones de la Empresa.

Impacto
La ausencia de un Centro de Datos Contingente pone en riesgo a la Empresa ya que es una limitante para mantener el servicio disponible de acuerdo con los requerimientos caso de interrupciones.

Recomendación
Se recomienda a la Empresa contar con un Centro de Datos Contingente que les permita continuar sus procesos de negocios de manera efectiva en caso de un evento desfavorable. (COBIT: Ds4 Asegurar la continuidad del Negocio).

Hallazgo Nº 5.29	Ausencia de centralización de Contratos		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A la fecha de revisión se denota que la Empresa tiene 9 contratos distintos de contratación para la solución Symantec Antivirus, Controlador de dominio y para el proveedor de Internet, lo que genera un incremento en los costos de Servicios brindados por el proveedor.

Impacto
La descentralización de contratos de servicios incrementa los gastos de la Empresa, ya que no se utiliza la negociación de precios que desea contratar los servicios.

Recomendación
Se recomienda a la Empresa la centralización de contratos con los proveedores, ya que esto permitirá la una reducción significativa en los costos, y así mismo definir de manera conglomerada acuerdos de servicios con terceras partes a través de contratos entre la Empresa y el proveedor este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado. Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.

Hallazgo Nº 5.30	Dependencia del Proveedor de Internet		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A la fecha de revisión se denota que la Empresa actualmente no tiene proveedor contingente. Si cuentan con enlace de doble fibra con el mismo proveedor, lo cual no es garantía de redundancia en el servicio de manera efectiva.

Impacto
La ausencia de un proveedor de Internet contingente incrementa el riesgo de no contar con la información disponible, por problemas de comunicación entre los usuarios y los servidores crítico, de igual manera puede representar pérdidas significativas al brindarle servicios a los diferentes clientes de AKROSERV.

Recomendación
Se recomienda a la Empresa la contratación de un proveedor de Internet contingente, que les garantice la continuidad del Servicio de Internet, y así mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones. (COBIT: Ds4 Asegurar el Servicio Continuo).

Hallazgo Nº 5.31	Estandarización de Servidor Windows Server 2012		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A la fecha de revisión se denota que la Empresa ha adquirido el Sistema Operativo para Servidores Windows 2012 R2, el cual es la última versión liberada por la empresa Microsoft. Sin embargo, de los 5 servidores físicos con los que cuenta la Empresa, únicamente 1 tiene instalada la versión 2012 Server R2, los demás trabajan con la versión Server 2003 y 2008.

Impacto
La adquisición de tecnología que no será aprovechada genera pérdidas significativas a la Empresa, ya que no hay justificación de costos y beneficios de las actividades realizadas por TI, ya que si solicitan un software o hardware que no se necesita se está perdiendo la inversión brindada al recurso.

Recomendación
Se recomienda a la Empresa la implementación estandarizada del Sistema Operativo Windows Server 2012 R2 en todos los servidores físicos y virtuales. De esta manera, se está usando el recurso para el cual se pidió financiamiento y cuya funcionalidad traerá ventajas y efectividad a las operaciones del área de TI y por ende a la Empresa. Ésta sana práctica tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros. (COBIT:PO5 Manejo de la inversión).

Hallazgo Nº 5.32	Plan de Seguridad TI		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A la fecha de revisión, se determinó que AKROSERV implementa ciertas medidas de seguridad en sus aplicaciones y accesos. Sin embargo, no cuentan con Plan de Seguridad Informático definido que les brinde los lineamientos para garantizar la autenticidad, confidencialidad e integridad de la información.

Impacto
La ausencia de un Plan de Seguridad TI para resguardar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI implican un riesgo para la Empresa ya que no cuentan con estrategias de seguridad que protejan todos los activos, así como la información en los sistemas.

Recomendación
Se recomienda a la Empresa la elaboración de las políticas de Seguridad TI, para garantizar la protección de la información sugerida en las sanas prácticas. (COBIT: DS5.2. Plan de Seguridad TI) e ISO/IEC 27002.
En particular la Política de Seguridad al menos debe tener los siguientes aspectos:
A. La relación con la política general del negocio.
B. La coordinación con los otros procesos TI.
C. Los protocolos de acceso a la información.
D. Los procedimientos de análisis de riesgos.
E. Los programas de capacitación
F. El nivel de monitorización de la seguridad.
G. Qué informes deben ser emitidos periódicamente.
H. El alcance del Plan de Seguridad.
I. La estructura y responsables del proceso de Gestión de la Seguridad.
J. Los procesos y procedimientos implementados.
K. Los recursos necesarios para el negocio: software, hardware y personal.

Hallazgo Nº 5.33	Ausencia de Análisis de Vulnerabilidades periódicas		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
A la fecha de revisión se denota que la Empresa no realiza análisis periódicos de vulnerabilidades a los sistemas y Equipos de la Infraestructura tecnológica, que permitan identificar y resolver los riesgos de seguridad propios de cada área de Tecnología.

Impacto
La Empresa puede alcanzar un nivel de protección óptimo en un momento determinado y ser totalmente sensible poco después, tras cambios en la configuración de un servidor o luego de instalar nuevos dispositivos de red. Al mismo tiempo, continuamente aparecen nuevos fallos de seguridad en software existentes, que previamente se creían seguros.

Recomendación
Se recomienda a la Empresa la realización de Análisis de Vulnerabilidades periódicas los cuales mitigan, en gran medida, el riesgo asociado a un entorno en constante cambio, tal como lo representan los sistemas informáticos de cualquier compañía.

Hallazgo Nº 5.34	Ausencia de uso estandarizado de las versiones de las licencias del Sistema ASPELCOI- ASPEL BANCO		
Nivel de Riesgo	Alto	Medio	Bajo
	✔		

Descripción del Hallazgo
Durante la revisión, se denota que en los distintos servidores del Sistema de Información hay versiones instaladas de Aspel COI- Aspel Banco diferentes, ya sean v.3.0, 5.7 y 6.1.

Impacto
La ausencia de uso conjunto de versión única del Sistema de Información Aspel COI- Aspel Banco, incrementa el riesgo de exposición a perdida de la información, ya que al tener instaladas versiones inferiores, no se cuenta con el soporte necesario para resolver problemas propios de cada versión, así mismo disminuye la eficiencia operativa ya que las diferentes versiones tienen características propias e independiente a cada sistema, las cuales no están relacionadas, y generan que se realicen las actividades contables de maneras aisladas.

Recomendación
Se recomienda estandarizar e implementar en todos los servidores la última versión adquirida de ASPEL COI-ASPEL BANCO, ya que la administración de versiones es fundamental al realizar cambios en los entornos de tecnología de la información (TI). Después de que uno o más cambios se hayan desarrollado, probado y empaquetado en versiones para su implementación, se debe asumir la responsabilidad de introducir estos cambios y administrar su lanzamiento de manera conjunta. Así se minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores. (COBIT: AI6 Administración de los cambios)

Hallazgo Nº 5.35	**Ausencia de Metodología utilizada para análisis de requerimientos, diseño, programación, pruebas e implementación en el ambiente de producción.**		
Nivel de Riesgo	**Alto**	**Medio**	**Bajo**
	✔		

Descripción del Hallazgo
Durante la revisión se denota que no existe una metodología definida que permita la adecuada implementación de los desarrollos realizados al software, ya sea in-house o del Aspel COI- Aspel Banco, para mitigar los riesgos de ejecución de los programas.

Impacto
La ausencia de Metodologías impide la verificación y confirmación de que la solución sea adecuada para el propósito deseado por el área de TI. Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas.

Recomendación
Se recomienda a la Empresa la debida elaboración de metodología de los sistemas de información, para poder contar con el adecuado proceso de implementación considerando: •Capacitación del personal de acuerdo con el plan de entrenamiento definido y los materiales relacionados. •Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo. •Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio. •Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente. •Revisiones post implementación con el objeto de reportar si el sistema proporciono los beneficios esperados de la manera más económica.

Hallazgo Nº 5.36	Ausencia de políticas que garanticen la seguridad de la Información		
Nivel de Riesgo	Alto	Medio	Bajo
		✔	

Descripción del Hallazgo
A la fecha de revisión se denota que la Empresa no cuenta con políticas suficientes para llevar a cabo las directrices de seguridad de las aplicaciones en las diferentes especialidades, que le permitan al departamento garantizar la seguridad de la información.

Impacto
La ausencia de políticas limita el aseguramiento del uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas. Y pone en riesgo la confidencialidad, disponibilidad y seguridad de la información.

Recomendación
Se recomienda a AKROSERV la elaboración de políticas conteniendo todos los aspectos sugeridos por las sanas prácticas, para asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas con que cuentan, y brindar el nivel de seguridad apropiado a la información de la Empresa (COBIT: AI4 Desarrollo y mantenimiento de procedimientos). Elaborar políticas que vayan orientadas a aspectos relacionados con: 1. Restauración de Base de Datos local. 2. Administración e Implementación de Sistemas. 3. Política del Sistema de Incidencia. 4. Cuentas genéricas. 5. Cambios en los sistemas de Información

Hallazgo Nº 5.37	Actualización de Políticas y Procedimientos de TI		
Nivel de Riesgo	Alto	Medio	Bajo
		✔	

Descripción del Hallazgo
A la fecha de revisión el área de TI de AKROSERV cuenta con 1 Política y 7 Procedimientos que establecen lineamientos para velar por la seguridad de la información y activos tecnológicos de la Empresa, sin embargo, se recomienda la actualización de cada uno de estos documentos al menos 1 vez al año.

Impacto
La desactualización de Políticas y Procedimientos es un riesgo para la Empresa ya que no cuenta con lineamientos claros y vigentes en el proceso de toma de decisiones, generando que se afecten las operaciones financieras y resto del ciclo del negocio. Debido a que no se podrá garantizar el uso apropiado de las aplicaciones y de las soluciones tecnológicas.

Recomendación
Se recomienda a AKROSERV la actualización de Manuales y políticas que se elaboran, para garantizar el cumplimiento de los lineamientos establecidos por la Empresa sugerida en las sanas prácticas. (COBIT: AI4 Desarrollo y mantenimiento de procedimientos).

Hallazgo Nº 5.38	Aprobación de Políticas		
Nivel de Riesgo	Alto	Medio	Bajo
		✔	

Descripción del Hallazgo
A la fecha de revisión el área de TI de AKROSERV cuenta con 1 políticas elaboradas y 7 procedimientos. Sin embargo, estas políticas no están debidamente aprobadas y autorizadas por el comité correspondiente.

Impacto
La ausencia de aprobación de Políticas, diseñadas para proveer aseguramiento razonable de que se lograrán los objetivos del negocio y se prevendrán, detectarán y corregirán los eventos no deseables, son un riesgo para la Empresa de no contar con un lineamiento que les permita la mejora de sus procesos y actividades.

Recomendación
Se recomienda a la Empresa la aprobación de todas las políticas que se elaboran, para garantizar el cumplimiento de los lineamientos establecidos por la Empresa sugerida en las sanas prácticas. (COBIT: AI4 Desarrollo y mantenimiento de procedimientos).

Hallazgo Nº 5.39	Matriz de Riesgos de TI		
Nivel de Riesgo	Alto	Medio	Bajo
		✔	

Descripción del Hallazgo
A la fecha de revisión se denota que la Empresa no cuenta con una Matriz de Riesgo de TI que permita llevar un control de los Riesgos que se identifican en el área y la manera en que estos son tratados para mitigarlos.

Impacto
La ausencia de matriz disminuye la capacidad de TI para el logro de los objetivos y responder a las amenazas hacia la provisión de servicios de TI. Ya que no cuenta con la información necesaria para la identificación de riesgos de TI y el análisis de impacto, que le permita tomar medidas para mitigar los riesgos.

Recomendación
Se recomienda a la Empresa la definición de una Matriz de Riesgos de TI, que permita lo sugerida por las sanas prácticas. (COBIT:PO9 Evaluación de riesgos) 1. Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI (por ej.: tecnológicos, de seguridad, etc.) de manera de que se pueda determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable. 2. Definición de alcances, límites de los riesgos y la metodología para las evaluaciones de los riesgos. 3. Asegurar la definición de controles y medidas de seguridad que mitiguen los riesgos en forma continua.

Hallazgo Nº 5.40	**No existe una interfaz automática entre ASPEL COI – ASPEL BANCO y los demás sistemas desarrollados en casa**		
Nivel de Riesgo	**Alto**	**Medio**	**Bajo**
		✔	

Descripción del Hallazgo
Durante la revisión se denota que no se cuenta con una interfaz que relacione el sistema Aspel COI- Aspel Banco, con los desarrollos in-house realizados por el Dpto. TI

Impacto
La ausencia de interfaz con el Sistema principal de la Empresa incrementa los tiempos de operatividad por parte de los usuarios, ya que se duplica el trabajo al tener que acceder a aplicaciones independientes, cuya relación automatizada no existe, incrementando también la posibilidad de errores por partes de los operarios.

Recomendación
Se recomienda el desarrollo de una interfaz que permita la interrelación entre el Sistema ASPEL COI-ASPEL Banco y los sistemas desarrollados en casa, para de esta manera, la interfaz permita al usuario acceder al sistema y a su información de manera congruente con sus necesidades, y con esto maximizar el tiempo de entrada de datos y minimizar los errores. Proporcionando funciones automatizadas que soporten efectivamente al negocio. (COBIT: AI2 Adquisición y mantenimiento del software aplicativo).

Hallazgo Nº 5.41	Ausencia de Organigrama de TI		
Nivel de Riesgo	Alto	Medio	Bajo
			✔

Descripción del Hallazgo
A la fecha de revisión, se determinó que AKROSERV no cuenta con un Organigrama del área de Tecnología que permita el entendimiento de líneas de subordinación e ilustran la división de responsabilidades y el grado de segregación de funciones, el mismo fue elaborado durante la Auditoria.

Impacto
La ausencia del Organigrama de TI impide desarrollar una estructura organizativa qué atienda el cumplimiento de la misión y objetivos. La estructura organizativa, formalizada en un organigrama, constituye el marco formal de autoridad y responsabilidad en el cual las actividades que se desarrollan en cumplimiento de los objetivos del organismo son planeadas, efectuadas y controladas.

Recomendación
Se recomienda a la Empresa desarrollar un Organigrama que permita identificar las líneas de subordinación según responsabilidades de cada usuario, para poder evaluar que la subordinación esté basada en conceptos correctos del negocio y no afecten la segregación de funciones, de acuerdo con las sanas prácticas (Normas de Control Interno COSO: Organigrama).

Hallazgo Nº 5.42	Ausencia del Diagrama de Red LAN y WAN		
Nivel de Riesgo	Alto	Medio	Bajo
			✔

Descripción del Hallazgo
Durante la revisión se denota que no contaban con un diagrama de Red LAN y WAN de la Empresa. El mismo fue elaborado durante la Auditoria.

Impacto
La ausencia de un Diagrama de Red limita la administración de los equipos de la Infraestructura, por la falta de orden e interrelación entre los diferentes componentes de la topología, así mismo el control de cambios o ingreso de equipos no será eficiente porque no existe un orden de conexión claro y preciso documentado para servir de guía al encargado de las telecomunicaciones o proveedor de servicios. Administración de cambios en la configuración asegurando que los registros de configuración reflejen el estatus real de todos los elementos de la configuración.

Recomendación
Se recomienda a la Empresa la elaboración del Diagrama de Red LAN y WAN que permita garantizar mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones, de acuerdo con las sanas prácticas (COBIT: Ds4 Asegurar el Servicio Continuo), (COBIT: Ds9 Administración de la configuración).

11. RECOMENDACIONES DE IMPLEMETACION BCP POR CONSIDERAR.

- Generar un diagnóstico del estado de madurez de las definiciones de continuidad, relacionadas con:
  - Requerimientos regulatorios de la industria, el gobierno, etc.
  - Actividades actuales de continuidad en las funciones de negocio.
  - Tipo de planes de atención de emergencia y salvaguarda del personal.
  - Planes de recuperación de desastres para la plataforma tecnológica.
- Acotar el alcance de la implementación del BCP
  - Definir qué objetivos estratégicos de negocio desea cubrir en forma prioritaria en una primera fase.
  - Identificar los procesos o áreas de negocio asociados a esos objetivos.
  - Establecer el proyecto semilla de implementación del BCP.
- Defina la implementación del plan considerando:
  - El patrocinador del proyecto general.
  - Desarrollo del plan del proyecto y su presupuesto.
  - La estructura y la administración del proyecto.
  - Los roles y responsabilidades de los involucrados en el plan.

12. ESTRATEGIA DE IMPLEMENTACION BCP.

- Realizar un trabajo continuo de la implementación del modelo:
  - Establecer monitoreo continuo sobre el cumplimiento de las actividades administrativas definidas en el plan.
  - Extender el proyecto semilla a las áreas no incorporados inicialmente.
  - Establecer indicadores de gestión para medir el cumplimiento.
  - Evaluar periódicamente el nivel de madurez de implementación.

- Factores clave de éxito
  - Gestionar el apoyo y liderazgo de la alta gerencia.
  - Definir un líder de proyecto, idealmente un líder de procesos.
  - Identificar el personal idóneo que debe participar en cada fase.
  - Realizar actividades de sensibilización.
  - Realizar actividades de transferencia de conocimiento al personal.
  - Utilizar enfoque de procesos y no de tecnología.

13. CRONOGRAMA DE ACTIVIDADES.

CRONOGRAMA		
Auditoría interna de procesos informáticos aplicando el marco de gobierno de tecnologías de la información COBIT 5		
Plan de Trabajo AKROSERV	**Mes**	**Día**
Inicio		
Reunión con gerencia AKROSERV	Mes 1	Dia 1
Planificación		
Documentación del plan de proyecto	Mes 1	Dia 10
Creación de la matriz de diagnóstico COBIT 5	Mes 1	Dia 13
Definición de los requerimientos de documentación	Mes 1	Dia 20
Definición del equipo de trabajo AKROSERV	Mes 1	Dia 24
Reunión de inicio con el equipo de trabajo	Mes 1	Dia 25
Envío de los requerimientos de documentación	Mes 1	Dia 26
Revisión de Plan de proyecto por AKROSERV	Mes 1	Dia 27
Ajustes de Plan de Proyecto por consultor	Mes 2	Dia 2
Entrega de Plan de Proyecto	Mes 2	Dia 3
Listado de documentos para verificar el cumplimiento	Mes 2	Dia 4
Matriz de diagnóstico COBIT 5	Mes 2	Dia 5
Ejecución		
Diagnóstico de objetivos de control.		
APO01. Gestionar el marco de gestión de TI		
Entrevistas con el personal responsable	Mes 2	Dia 10
Evaluación de la documentación	Mes 2	Dia 11
Análisis de los criterios de evaluación	Mes 2	Dia 15
Análisis de brechas de cumplimiento	Mes 2	Dia 16
Documentación de observaciones y conclusiones	Mes 2	Dia 18
APO06. Gestionar el presupuesto y los costes		
Entrevistas con el personal responsable	Mes 2	Dia 23
Evaluación de la documentación	Mes 2	Dia 24
Análisis de los criterios de evaluación	Mes 2	Dia 26
Análisis de brechas de cumplimiento	Mes 2	Dia 29
Documentación de observaciones y conclusiones	Mes 2	Dia 31
APO07. Gestionar los recursos humanos		
Entrevistas con el personal responsable	Mes 3	Dia 5
Evaluación de la documentación	Mes 3	Dia 6
Análisis de los criterios de evaluación	Mes 3	Dia 8
Análisis de brechas de cumplimiento	Mes 3	Dia 9
Documentación de observaciones y conclusiones	Mes 3	Dia 13
APO11. Gestionar la calidad		

Entrevistas con el personal responsable	Mes 3	Dia 16
Evaluación de la documentación	Mes 3	Dia 19
Análisis de los criterios de evaluación	Mes 3	Dia 21
Análisis de brechas de cumplimiento	Mes 3	Dia 22
Documentación de observaciones y conclusiones	Mes 3	Dia 26
APO12. Gestionar el riesgo		
Entrevistas con el personal responsable	Mes 3	Dia 29
Evaluación de la documentación	Mes 3	Dia 30
Análisis de los criterios de evaluación	Mes 4	Dia 3
Análisis de brechas de cumplimiento	Mes 4	Dia 4
Documentación de observaciones y conclusiones	Mes 4	Dia 6
APO13. Gestionar la seguridad		
Entrevistas con el personal responsable	Mes 4	Dia 11
Evaluación de la documentación	Mes 4	Dia 12
Análisis de los criterios de evaluación	Mes 4	Dia 16
Análisis de brechas de cumplimiento	Mes 4	Dia 17
Documentación de observaciones y conclusiones	Mes 4	Dia 19
BAI04. Gestionar la disponibilidad y la capacidad		
Entrevistas con el personal responsable	Mes 4	Dia 24
Evaluación de la documentación	Mes 4	Dia 25
Análisis de los criterios de evaluación	Mes 4	Dia 27
Análisis de brechas de cumplimiento	Mes 4	Dia 30
Documentación de observaciones y conclusiones	Mes 5	Dia 2
BAI05. Gestionar la habilitación del cambio organizativo		
Entrevistas con el personal responsable	Mes 5	Dia 7
Evaluación de la documentación	Mes 5	Dia 8
Análisis de los criterios de evaluación	Mes 5	Dia 10
Análisis de brechas de cumplimiento	Mes 5	Dia 11
Documentación de observaciones y conclusiones	Mes 5	Dia 15
BAI06. Gestionar los cambios		
Entrevistas con el personal responsable	Mes 5	Dia 18
Evaluación de la documentación	Mes 5	Dia 21
Análisis de los criterios de evaluación	Mes 5	Dia 23
Análisis de brechas de cumplimiento	Mes 5	Dia 24
Documentación de observaciones y conclusiones	Mes 5	Dia 28
BAI09. Gestionar los activos		
Entrevistas con el personal responsable	Mes 5	Dia 31
Evaluación de la documentación	Mes 6	Dia 1
Análisis de los criterios de evaluación	Mes 6	Dia 5
Análisis de brechas de cumplimiento	Mes 6	Dia 6
Documentación de observaciones y conclusiones	Mes 6	Dia 8

BAI10. Gestionar la configuración		
Entrevistas con el personal responsable	Mes 6	Dia 13
Evaluación de la documentación	Mes 6	Dia 14
Análisis de los criterios de evaluación	Mes 6	Dia 18
Análisis de brechas de cumplimiento	Mes 6	Dia 19
Documentación de observaciones y conclusiones	Mes 6	Dia 21
DSS02. Gestionar las peticiones y los incidentes de servicio		
Entrevistas con el personal responsable	Mes 6	Dia 26
Evaluación de la documentación	Mes 6	Dia 27
Análisis de los criterios de evaluación	Mes 6	Dia 29
Análisis de brechas de cumplimiento	Mes 7	Dia 2
Documentación de observaciones y conclusiones	Mes 7	Dia 4
DSS03. Gestionar los problemas		
Entrevistas con el personal responsable	Mes 7	Dia 9
Evaluación de la documentación	Mes 7	Dia 10
Análisis de los criterios de evaluación	Mes 7	Dia 12
Análisis de brechas de cumplimiento	Mes 7	Dia 13
Documentación de observaciones y conclusiones	Mes 7	Dia 17
DSS05. Gestionar los servicios de seguridad		
Entrevistas con el personal responsable	Mes 7	Dia 20
Evaluación de la documentación	Mes 7	Dia 23
Análisis de los criterios de evaluación	Mes 7	Dia 25
Análisis de brechas de cumplimiento	Mes 7	Dia 26
Documentación de observaciones y conclusiones	Mes 7	Dia 30
MEA01. Supervisar, evaluar y valorar el rendimiento y conformidad		
Entrevistas con el personal responsable	Mes 8	Dia 2
Evaluación de la documentación	Mes 8	Dia 3
Análisis de los criterios de evaluación	Mes 8	Dia 7
Análisis de brechas de cumplimiento	Mes 8	Dia 8
Documentación de observaciones y conclusiones	Mes 8	Dia 10
Pruebas de control operativo		
FASE I - Centro de Datos y operaciones de Red		
Respaldos	Mes 8	Dia 15
Restauración	Mes 8	Dia 17
Cambios a la Infraestructura	Mes 8	Dia 20
Respuesta a Incidentes	Mes 8	Dia 22
Monitoreo de la Infraestructura	Mes 8	Dia 23
Red Inalámbrica	Mes 8	Dia 27
Respuesta a Incidentes	Mes 8	Dia 28
FASE II - Seguridad de la Información		

Parámetros de contraseñas	Mes 8	Dia 30
Contraseñas sin vencimiento	Mes 8	Dia 31
Cuentas Guest y Administrador	Mes 9	Dia 4
Nivel de Actualización	Mes 9	Dia 5
Privilegios sysadmin	Mes 9	Dia 7
Cuentas contraseñas null	Mes 9	Dia 10
Autenticación del Servidor del Sistema y BD	Mes 9	Dia 12
Responsables de Eventos o sucesos	Mes 9	Dia 13
Exfuncionarios	Mes 9	Dia 30
Usuarios genéricos	Mes 9	Dia 31
Bitácoras de seguridad	Mes 9	Dia 4
Segregación de funciones	Mes 9	Dia 5
Privilegios administrativos	Mes 9	Dia 7
Registro contable no refleja el usuario que lo realizó	Mes 9	Dia 10
FASE III - Control de Cambios en los Sistemas y Controles de Aplicación		
Cambios generados en el sistema	Mes 9	Dia 17
Plan de Pruebas	Mes 9	Dia 18
Uso de Software no licenciado	Mes 9	Dia 20
Ambiente de pruebas.	Mes 9	Dia 21
Cierre		
Presentación de informe a la directiva	Mes 9	Dia 25
Evaluación de oportunidades de mejora con TI	Mes 9	Dia 26
Ajustes finales de informe	Mes 9	Dia 28
Cierre del proyecto	Mes 9	Dia 30

14. ANALISIS DE COSTOS.

El salario del auditor se va a establecer mensualmente y el horario de trabajo va a ser de lunes a viernes, 8 horas diarias sin incluir la hora almuerzo.

Recurso Humano

# Personas	Cargo	Total Meses	pago/mensual $	Total $
1	consultor	10	1,000.00	10,000.00

Pago total $: 10,000.00

Adquisición de Software:

Cantidad	Nombre del Programa	Precio $
1	Microsoft Project Pro 2019	1,280.00
1	Microsoft Office Pro 2019	550.00

Total: $1,830.00

Adquisición de Hardware

Cantidad	Descripción	Precio Unitario $	Total $
1	computadora de Escritorio	450.00	450.00
1	Mesa de computador	200.00	200.00
1	batería / estabilizador	45.00	45.00

Total $: 695.00

Costo total: US$12,525.00

15. IMPACTO TECNICO-ECONOMICO Y SOCIAL.

El COBIT 5 se adapta mejor a los clientes que usan marcos múltiples, como ITIL, ISO/IEC 2000 y CMI, con ciertos silos dentro de TI que utilizan su propio marco o estándar. También se adapta bien a las organizaciones que deben seguir las directrices reglamentarias específicas del gobierno y las autoridades locales.

El marco COBIT 5 ayuda a AKROSERV a alinear los marcos existentes en la organización y comprender cómo cada marco se ajustará a la estrategia general. También ayuda a la empresa a monitorear el desempeño de estos otros marcos, especialmente en términos de cumplimiento de seguridad, seguridad de la información y gestión de riesgos.

También brinda a la alta dirección más información sobre cómo la tecnología se puede alinear con los objetivos de la organización. El marco brinda a los CIO y otros ejecutivos de TI una forma de demostrar el ROI en un proyecto de TI y cómo esto ayudará a alcanzar los objetivos comerciales clave.

El impacto social se ve reflejado en la mejora de vida que tienen tanto los trabajadores de la empresa, así como sus allegados, esto debido a que al mejorar los servicios brindados por la empresa se obtiene una excelente reputación ante los ojos de los clientes los cuales son vitales para el crecimiento económico y profesional de la empresa y por ende de la sociedad al generar mejores ingresos.

16. CONCLUCIONES.

Mediante la realización de esta auditoría interna al departamento de informática de la empresa AKROSERV basada en el marco de trabajo COBIT 5, se identificó su estado actual, se brindaron recomendaciones y oportunidades de mejora que permitan optimizar los proceso y fortalecer el gobierno de TI.

Para los objetivos específicos tenemos que:

- Se verificó la existencia de políticas claras y buenas prácticas de control que permitan la utilización de los sistemas de modo productivo y seguro, manteniendo la confidencialidad, la integridad y la disponibilidad de la información.

- Se identificaron las vulnerabilidades existentes en los procesos actuales de TI que impiden una óptima gestión de gobierno.

- Se realizó un informe final de auditoría informática que contiene la evaluación de los elementos auditados, así como las recomendaciones para lograr la mejora y optimización de los procesos de TI en base al marco de trabajo COBIT 5.

17. BIBLIOGRAFIA.

- COBIT 5 A Business Framework for the Governance and Management of Enterprise IT, https://www.isaca.org/bookstore/cobit-5/wcb5

- COBIT 5 Framework for the Governance of Enterprise IT, https://www.itgovernance.co.uk/cobit

- COBIT 5 IT Governance Framework, https://apmg-international.com/cobit5#zone-1