INFORME DE AUDITORIA

NOMBRE DEL PROCESO, ÁREA O TEMA A AUDITAR: Auditoría Integral de Gestión al Proceso de Infraestructura Tecnológica

INFORME PRELIMINAR: 16/06/2021 **INFORME DEFINITIVO**: 25/06/2021

1. INTRODUCCIÓN

La Oficina de Control Interno, en ejercicio de las facultades legales otorgadas por la Ley 87 de 1993, modificada por la Ley 1474 de 2011, el Decreto 2145 de 1999 y sus modificaciones, los Decretos 648 y 1499 de 2017, el Decreto 338 de 2019 "Por el cual se modifica el Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, en lo relacionado con el Sistema de Control Interno y se crea la Red Anticorrupción", el Decreto 403 de 2020 CGR, "Fortalecimiento del Control Fiscal" y las Circulares Normativas establecidas por la Entidad, el estatuto de Auditoría Interna y la guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el DAFP en su versión No 5, , tiene como función realizar la evaluación independiente y objetiva al Sistema de Control Interno, a los procesos, procedimientos, actividades y actuaciones de la administración, con el fin de determinar la efectividad del Control Interno, el cumplimiento de la gestión institucional y los objetivos de la Entidad, produciendo recomendaciones para asesorar al Representante Legal en busca del mejoramiento continuo y permanente del Sistema de Control Interno.

En cumplimiento al Plan Anual de Auditorías aprobado en el mes de enero de 2020 y sus modificaciones, por el Comité Asesor de Junta Directiva de Auditoría, la Oficina de Control Interno con el apoyo de la firma externa Bellicorp SAS realizó Auditoría Integral de Gestión al Proceso de Infraestructura Tecnológica, de conformidad al Plan de Auditoría y Carta de Representación dado a conocer con anterioridad al líder del proceso, cuyo propósito principal de la auditoría integral de gestión, fue verificar la existencia y efectividad de los controles, la correcta administración de los riesgos y efectuar las recomendaciones necesarias en pro del mejoramiento continuo y permanente del Proceso, lo cual redundará en el cumplimiento de la Misión y los Objetivos Institucionales.

2. OBJETIVO DE LA AUDITORÍA

Evaluar la efectividad de los controles existentes, el manejo de los riesgos e indicadores, la pertinencia y oportunidad de los procedimientos establecidos en los Manuales, las Circulares Normativas aplicables al proceso de Gestión Tecnológica, como también, la gestión del proceso y el diseño y operatividad de los controles seleccionados en cada uno de los componentes que integran la Infraestructura Tecnológica de la entidad, como se relacionan a continuación:

2.1. Planeación y Administración de Tecnología de Información (TI):

- Plan Estratégico de Tecnología de Información – PETI
- Indicadores de desempeño de la gestión de TI

- Gestión de riesgos de TI
- Organización de la Dirección de tecnología
- Plan de capacitación de TI
- Gestión de Proyectos de Tecnología de Información
- Cumplimiento normativo de TI
- Gestión financiera del proceso de TI
- Procedimiento de Selección y Gestión de Proveedores

2.2. Centro de Datos y Operaciones de Red:

- Controles de acceso físico y ambiental del centro de computo
- Plan de Mantenimiento a equipos tecnológicos
- Gestión de la capacidad y desempeño de TI
- Procedimientos de Mesa de ayuda y gestión de incidentes
- Gestión de ANS – Acuerdos de Niveles de Servicio
- Procedimientos de gestión de procesos automáticos, Jobs o batch
- Procedimientos de copias de respaldo de la información restauración
- Procedimiento de Control de licenciamiento de software
- Plan de continuidad de negocio – BCP y recuperación de desastres – DRP
- Proyecto Migración protocolo IPV4 a IPV6

2.3. Desarrollo de Software y Control de Cambios:

- Metodología del ciclo de vida de desarrollo de software
- Procedimiento de Gestión de Cambios
- Control de acceso para los ambientes de Desarrollo, Pruebas y Producción
- Versionamiento de Software
- Derechos de autor ante la Dirección Nacional de Derechos de Autor – DNDA de las aplicaciones
- Identificación de costos de la fábrica de software
- Controles para Integridad, confiabilidad y confidencialidad de la información en las aplicaciones

2.4. Seguridad de la Información y Ciberseguridad:

- Gestión de riesgos de seguridad de la información y ciberseguridad
- Indicadores de desempeño de seguridad de la información y ciberseguridad
- Gestión de vulnerabilidades técnicas
- Políticas de seguridad de la información y ciberseguridad
- Procedimientos de gestión de seguridad de la información
- Roles y Responsabilidades de la función de seguridad de la información
- Gestión de activos de seguridad de la información
- Procedimiento de gestión de incidentes de seguridad de la información y ciberseguridad

- Procedimiento para la Revisión y verificación de perfiles de usuarios en las aplicaciones.
- Procedimiento de verificación de Seguridad en bases de datos.
- Plantillas de aseguramiento (Hardening) de servidores

3. ALCANCE

La Oficina de Control Interno con el apoyo técnico de la firma externa Bellicorp SAS realizó Auditoría Integral de Gestión al Proceso de Infraestructura Tecnológica, evaluando la aplicabilidad de los procesos y procedimientos establecidos en los manuales y las circulares internas, políticas y normatividad legal vigente, donde se evaluó el periodo comprendido entre el 1 de enero de 2020 al 30 de abril de 2021.

Esta auditoría se llevó acabo en cumplimiento a las normas y técnicas de auditoría generalmente aceptadas, con fundamento en normas internacionales de auditoría basadas en riesgos, la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5, Estatuto de Auditoria Interna, séptima dimensión y tercera línea de defensa del Modelo Integrado de Planeación y Gestión – MIPG, la auditoría se realizó del 14 de diciembre de 2020 al 16 de junio de 2021.

4. DESARROLLO DE LA AUDITORÍA

4.1. EVALUACIÓN DE AUDITORÍAS ANTERIORES

4.1.1. Auditorías Anteriores: Revisadas las acciones previstas en el Plan de Mejoramiento producto de la Auditoria realizada en el año 2017 al proceso de Infraestructura Tecnológica que se encuentran detalladas en el Anexo 1, donde se verificó su implementación y efectividad para soportar el cierre de las mismas, se evidenció lo siguiente:

Hallazgo 5.1.1 Ausencia de DRP (Plan de Recuperación de Desastre): Se verificó la implementación de la política descrita en el numeral 5.16 - Control DRP, contenida en la Circular Normativa N°093 y la cual tiene alcance con la implementación del BCP (Continuidad del Negocio) y DRP (Plan de Recuperación de Desastre).

Apoyados en la métrica de cumplimiento, se verificó que se estableció el contrato de prestación de servicios N° 030-2019 con COLUMBUS Networks Colombia Ltda., para la prestación de los servicios de infraestructura virtual e implementar un esquema de recuperación de desastres – DRP; **por lo que equipo auditor considera el cierre del hallazgo.**

Hallazgo 5.1.2 Inconsistencia en la externalización de copias de respaldo: No se evidenciaron soportes de la capacitación al grupo de operaciones tecnológicas relacionada con los procedimientos de custodia externa; así mismo, se observó que en el año 2018 la auditoría interna revisó el cumplimiento de las remisiones de las copias al externo, cumpliendo con el diligenciamiento del formato en el momento de dicha revisión.

Aunque la unidad de medida del hallazgo fue la capacitación, se verificó el cumplimiento del procedimiento, calidad de uso de formatos y las evidencias aportadas a la auditoría interna en septiembre de 2018; en el desarrollo de la

auditoría se realiza un análisis de las evidencias entregadas, para lo cual se verificó el diligenciamiento y uso del formato "*Formato único de inventario documental – fuid.xls*" y la aplicación del "*Instructivo para la generación de backups.pdf*", donde se describe que los envíos de copias externas se realizan mensual y semanal y en la verificación de efectividad se demostró que:

La fecha registrada en el campo "*Registro de Entrada*" del "*Formato Único de Inventario Documental*" no tiene una relación cronológica con las fechas registradas en el campo "*Fechas Extremas"* que corresponden al periodo inicial y final del backup efectuado, esto se evidencia en cinco (5) de los nueve (9) periodos solicitados, donde se incluyen formatos de los años 2020 y 2021; se observa que la fecha final de la copia es el 30-09-2020 y la fecha de entrada es el 27-01-2021, siendo aproximadamente cuatro meses después de realizado el backup, el cual debería corresponder a un lapso de periodo cercano a la fecha final registrada.

Basados en lo anterior **se concluye que el hallazgo no se cierra**, por lo tanto, es importante plantear una nueva acción que permita corregir la debilidad identificada y de lugar al cierre del hallazgo.

Hallazgo 5.1.3 Falta de Evidencia para la restauración de copias de respaldo: Verificados los soportes entregados por la entidad, se observó que se dio cumplimiento al 100% de las acciones de capacitación prevista en el plan, **razón por la cual se cierra el hallazgo.**

Hallazgo 5.1.4 Controles ambientales del Centro de Cómputo: La Dirección de Tecnología implementó tres acciones para subsanar el hallazgo de la siguiente manera:

a. Para la verificación de la "implementación de control (1. Techo ignifugo, 2. Sistema de extinción de incendios)", se solicitó el avance de la reubicación el centro de cómputo, identificando que cuentan con un proyecto aprobado para la construcción de un nuevo centro de cómputo con adecuados controles físicos y ambientales; no se evidenciaron los soportes de ejecución o avance del mismo, por lo anterior **no se cierra la acción.**

b. Para la acción de actualizar el documento de la Circular Normativa N° 093 incluyendo el procedimiento de arqueo físico de medios, se verificó y observó que se incluyó el Anexo N°15 Instructivo para realizar arqueo de medios electrónicos el 05 de abril de 2019, **razón por la cual se cierra la acción.**

c. En la revisión del cumplimiento de la acción **"Incluir actividad de arqueo físico dentro del alcance del contrato del custodio externo de medios"**, se observó la inclusión de la cláusula en el contrato suscrito con el Custodio de Medios (Arprotec), el Numeral 19 de la Cláusula Cuarta – Obligaciones específicas del contratista**, por lo cual se cierra la acción**.

Hallazgo 6.2 Falta de trazabilidad en el control de acceso al centro de cómputo: Se verificó la instalación del sistema biométrico - ZKAccess3.5 Security System y el informe de registro de acceso al centro de cómputo. Razón por la cual **se concluye el cierre del hallazgo.**

Observación 5.2.1 Control de Cambios en la aplicación: Se evidenció en el soporte entregado "2. Actores Flujos.xlsx", la definición del estado "Verificación de la Calidad del Soporte" para los flujos de: "Soporte de

Aplicativos Institucionales", "Gestión de Requisitos de Software" y "Desarrollo Software a Terceros", que se incluyó el estado "Pendiente realizar pruebas de calidad y/o apoyo"; no obstante es importante precisar que se han realizado actualizaciones como los nombres de los flujos, en este caso el flujo llamado "Desarrollo Software Terceros", cambio su nombre a "Soporte aplicativos a Terceros", **lo cual no afecta el cierre de la observación.**

Observación 5.2.2 Control de Cambios directos en la base de datos: Revisados los flujos de los procesos de Tecnología se evidencio que para el flujo "Solicitud modificación o adición información en BD" se incluyó el estado "Pendiente Revisión Oficial de Seguridad de la información"; sin embargo, en el análisis a las solicitudes efectuadas utilizando este flujo se identificó que las áreas operativas solicitan cambios a la información directamente sobre la base de datos, lo cual hace que no se tengan en cuenta controles implementados para la gestión de los procesos y dar transparencia a los mismos afectado la confiabilidad e integridad de la información, **lo anterior conlleva a la reclasificar la observación como hallazgo.**

Observación 6.4 Diagnóstico sobre la implementación ISO27001: Se implementaron cláusulas de auditabilidad en temas de seguridad de la información para proveedores críticos de la entidad y en el Comité Institucional de Gestión y Desempeño se incluyeron funciones de monitoreo y seguimiento al Modelo de Seguridad y Privacidad de la Información. Se concluye que las evidencias suministradas **soportan el cierre de la observación.**

Observación 6.5.1 Diseño de los procedimientos de gestión de cambios: El equipo auditor revisó los flujos de los procesos de Tecnología en donde para el flujo "Gestión de cambios", se evidenció el estado "Pendiente Revisar Criterios de Operaciones Tecnológicas y Programar Reunión CAB", se realizó la revisión de una muestra de 30 solicitudes, observando que no se cuenta con dicha evidencia ni digital ni física, por lo tanto, **la observación se mantiene abierta.**

Observación 6.5.2: La Dirección de Tecnología implementó tres acciones para subsanar la observación de la siguiente manera:

a. **Fábrica de Software**: Se realizó la adquisición de dos herramientas para realizar la gestión de las actividades de la fábrica de software, llamadas Celoxis y DevOps desde agosto de 2020, las cuales se encuentran en implementación, por esta razón al momento de la auditoría no se pudo evidenciar el detalle de la asignación de horas a los recursos del área y los proyectos de la Dirección de Tecnología, concluyendo que **la acción se mantiene abierta.**

b. **Manuales de usuario de los aplicativos**: Los Manuales de los aplicativos COBRA, TEMIS y OLYMPUS se encuentran desactualizados en el SIG respecto a los que se encuentran en el SharePoint de la Dirección de Tecnología, por lo tanto, l**a acción continúa abierta.**

c. **Manuales técnicos:** estos se encuentran actualizados y almacenados en el repositorio del SharePoint de la Dirección de Tecnología, para la consulta del personal de la fábrica de software, por esta razón **esta acción se cierra.**

Observación 6.5.3 Aplicación de la metodología SCRUM para el área de desarrollo: al revisar la actualización de la Circular Normativa N° 093 "Política y procedimiento de gestión tecnológica" versión 62 de 30 de diciembre de 2020 subnumeral "5.9. Políticas de desarrollo" y Circular Normativa N°127 "Política y procedimiento para gestión de proyectos de tecnología" versión 16 de 1 de diciembre de 2020 numeral "8. Metodología Gestión de Proyectos", donde se evidencia que los documentos y actividades hacen referencia al uso de metodologías ágiles mediante la metodología Scrum**, se cierra la observación.**

Observación 6.6.2 Cargue de pagos de usuarios en Cobra: En revisión del descargue y custodia del archivo de pagos de la entidad bancaria se observó que este se encuentra restringido por el directorio activo solo al personal encargado de esta labor de cargue al sistema Cobra, no requiriendo un sistema de encripción, por lo tanto, **se cierra esta observación.**

4.1.2. Plan de Mejoramiento CGR / TI: Revisado el Plan de Mejoramiento suscrito con la Contraloría General de la República CGR y CISA, se observó que la Dirección de Tecnología es responsable de seis (6) acciones de mejora, las cuales se encuentran relacionados con la actualización de los manuales: técnicos, de usuario y código fuente, como se observa en el Anexo 2.

Al verificar los manuales de usuario en el Sistema Integrado de Gestión – SIG en el Banco de Documentos, se evidenció que los manuales para los aplicativos de CISA no se encuentran actualizados respecto a los documentos del Sharepoint de la Dirección de Tecnología, al verificar el manual de la aplicación Olympus – Manual de Convenios se observa que en los documentos del SharePoint de la Dirección de Tecnología se realizó una modificación el 09/12/2020 y en el documento del Sistema de Gestión – SIG no se encuentra esta modificación y tampoco se observa el cambio realizado por la Jefatura de Procesos y Productividad del 30/12/2020, donde se actualizó la nueva imagen corporativa. Adicionalmente, en las consultas realizadas se observó lo siguiente:

- el manual de usuario Olympus, manual de usuario Cobra / Gestión de Clientes, manual de usuario IMC y manual de usuario Aplicativo Olympus - Parámetros del Banco de documentos se encuentran sin información.

- los manuales de usuarios en el Sistema Integrado de Gestión, no se encuentran actualizados con la versión de la Dirección de Tecnología.

Como resultado del análisis se observó que no se ha dado cumplimiento a la acción de mejora con respecto a la actualización de los manuales de usuario, la actualización del repositorio documental y la divulgación de la nueva versión a los usuarios de CISA y a Terceros, **por lo que no se cierra el hallazgo.**

4.2. EVALUACIÓN AL COMPONENTE DE PLANEACIÓN Y ADMINISTRACIÓN DE TECNOLOGÍA DE INFORMACIÓN

4.2.1. Plan Estratégico de Tecnología PETI: La Dirección de Tecnología y Sistemas de información, desarrolló en diciembre de 2019, el Plan Estratégico de Tecnología de la Información PETI, en el cual se pudo evidenciar que se contemplaron los elementos mínimos a tener en cuenta en la elaboración de dichos ejercicios, y que fueron registrados por la Dirección de Tecnología como se detalla en el siguiente cuadro:

Imagen 1. Componentes PETI

	Componentes PETI	Referencias PETI			Características
		Estructura del Plan Estratégico de TI Guía Técnica	G.ES.01 Guía del dominio de Estrategia TI- Guía	MODELO DE GESTIÓN IT4+ V02	
1	*Presentación*				Qué es el PETI, Por qué y Para qué?
2	*Objetivo*	x	x		Objetivos alineados a la Estrategia de la Entidad
3	*Alcance*	x	x		Realizable y medible
4	*Principios*	x			Lineamientos y principios que guían la definición del PETI
5	*Marco Normativo*	x	x		Alineación con el marco normativo, relación con la normatividad asociada y de referencia
6	*Situación Actual*	x	x	x	Estrategia TI, Gobierno TI, Gestión de Información, Sistemas de Información, Servicios TI, Uso y Apropiación
7	*Estrategia de TI*	x	x	x	Alineación con el plan sectorial, con la estrategia de la Entidad, Misión, Visión, Objetivos Estratégicos, Mapa Estratégico, Indicadores, Seguimiento y Evaluación
8	*Gobierno de TI*	x	x	x	Políticas TI, Toma de decisiones, Estructura Organizacional TI, Roles y Perfiles, Procesos, Gestión de Riesgos, Indicadores, Gestión de Relaciones, Gestión de Proyectos, Gestión del Conocimiento, Gestión de Proveedores, Gestión de Niveles de Servicio
9	*Gestión de Información*	x	x	x	Gobierno de datos, Necesidades de Información, Arquitectura de Información, Seguridad de la Información
10	*Sistemas de Información*	x	x	x	Intervenciones de los sistemas de información, Arquitectura de los sistemas de información
11	*Servicios Tecnológicos*	x	x	x	Infraestructura, conectividad, Operación, Mesa de Servicio, Soporte, Procedimientos, Catálogo de Servicios.
12	*Iniciativas*	x	x	x	Para la estrategia de TI, para el gobierno de TI, para la gestión de la información, para los sistemas de información, para los servicios tecnológicos, para el uso y apropiación, de implementación o mejora de procesos, de comunicación, de portafolio, Gestión de Iniciativas (medición y desempeño)
13	*Presupuesto*	x	x	x	Gestión de presupuesto, Presupuesto del periodo medido
14	*Recursos*	x	x	x	Recursos humanos, recursos tecnológicos

Fuente: Información de la Dirección de Tecnología del 15 de enero de 2021

Del cuadro anterior en el numeral 6 se realizó el análisis de la situación actual de todo el componente tecnológico de la entidad, para lo cual se tuvo como referente el modelo de Arquitectura Empresarial que contempla (6) seis dominios como la Estrategia de TI, Gobierno de TI, Gestión de la Información, Sistemas de Información, Servicios de TI y Uso y Apropiación. Para el numeral 7, la Dirección de Tecnología identificó, entre otros aspectos, la alineación del plan con los planes sectoriales y con los de la entidad, y para el numeral 12 se detallaron los aspectos relacionados con las iniciativas/proyectos estratégicos claves.

El PETI 2019-2022, se articula con el Plan Estratégico Institucional 2019-2022 y Plan de Acción Institucional 2019 en los siguientes aspectos generales:

a) Rediseño tecnológico: Acelerar las capacidades de entrega de proyectos TI, fomentando nuevas capacidades para integrar la innovación en el mejoramiento del rendimiento y la eficiencia.
b) Reestructuración Operativa: Actualización de procesos para el ámbito empresarial y tecnológico, para que la entidad pueda adaptarse a un entorno cambiante.
c) Nuevas fuentes de ingresos: Nuevos modelos de negocio sostenibles que equilibre de manera óptima las demandas y necesidades del estado.

En el PETI 2019-2022 se definieron los siguientes doce (12) proyectos, en donde se relaciona el nivel de avance para los años 2019 y 2020:

Imagen 2. Proyectos PETI

PETI	Peso	Fecha inicio	Fecha fin	Avance 2019	Avance 2020	Avance 2021	Avance 2022	Avance Acumulado
Cierre de Brecha - Ambitos de AE	35%	01/02/19	15/12/22	47%				16%
Subasta y Puja electrónica	10%	01/02/19	30/07/19	100%	N/A	N/A	N/A	10%
Liquidación Cuota Única Cartera	10%	01/02/19	31/10/19	100%	N/A	N/A	N/A	10%
Costeo ABC -Proceso de inclusión e interoperabilidad con el ERP	5%	01/03/19	31/10/19	100%	N/A	N/A	N/A	5%
Diagnóstico SIAF Activos Fijos	3%	01/04/19	31/10/19	100%	N/A	N/A	N/A	3%
Análisis Brecha TEMIS WEB CISA	2%	15/02/19	30/04/19	100%	N/A	N/A	N/A	2%
Actualización Infraestructura TI	6%	01/03/19	15/12/19	100%	N/A	N/A	N/A	6%
Gestión de Capacidad y Disponiblidad Infraestructura TI	5%	01/02/19	30/03/20	20%	100%	N/A	N/A	5%
Mecanismo de Análisis de Datos	4%	01/02/19	15/12/19	100%	N/A	N/A	N/A	4%
Fortalecimiento de la PMO TI - Gestión, Control y Resultados	6%	01/02/19	30/09/19	100%	N/A	N/A	N/A	6%
Actualización códigos fuentes - Control obsolescencia	10%	01/06/19	30/06/21	5%	30%			3%
Mecanismo Colaborativo para la Gestión de Conocimiento CISA	4%	01/08/19	30/06/20	100%	N/A	N/A	N/A	4%
	100%							**74%**

Fuente: Información de la Dirección de Tecnología del 15 de enero de 2021

Se evidenció en la revisión de la información del cuadro anterior que contiene un error de transcripción en el proyecto "*Cierre Brecha – Ámbitos de AE*", para el indicador de avance del año 2019 el cual corresponde al 36%; el 47% es el avance del 2020, de acuerdo con la información aportada por el proceso de los indicadores Plan Estratégico - Metas 2020, el detalle del análisis de puede observar en el numeral 4.2. del informe emitido el día 23 de abril de 2021 de la evaluación al Componente de Planeación y Administración de Tecnologías de la Información, ver Anexo 3.

4.2.2. Evaluación de Indicadores

4.2.2.1. Indicadores Plan Estratégico: Para las vigencias 2019 y 2020, la Dirección de Tecnología y Sistemas de Información realizó la medición y reporte de los siguientes indicadores, que están relacionados con la implementación del Plan Estratégico de Tecnología – PETI y el cierre de brechas en la implementación de la Arquitectura Empresarial, detalladas a continuación:

Imagen 3. Indicadores Plan Estratégico

Objetivo, Estrategia, Plan	Nombre Objetivo, Estrategia o Plan	Indicador	Meta 2019	Meta 2020	Meta 2021	Meta 2022	Total	Responsable de Medición	Resultado Acumulado (2019-2020)	Análisis frente a incumplimiento
Estrategia	Implementar el Plan estratégico de Tecnología - PETI	Porcentaje de Avance del PETI	48%	65%	82%	100%	100%	D. Tecnología	74%	A pesar de superar la meta planeada acumulada para el cierre 2020, en 2021 deberán integrarse proyectos PETI de Cierre de Brecha AE y de apoyo a la estrategia de la organización que modificarán el peso y avance global para el cuatrenio 2019-2022. Los siguientes se discutiran en las reuniones de estrategia corporativa el primer trimestre de 2021 (- Actualización del módulo comercial Cobra - Re-fabricación del sistema PAC - Construcción del sistema de gestión de activos fijos - Inclusión de modelos de liquidación de obligaciones distintos a cuota única (tasa fija y variable) en Cobra - Reingeniería a Temis CISA, inclusión de Temis Web - Subasta electrónica fase II)
Plan de Acción	Cierre de la brecha identificada en el diagnósito del avance de implementación de la Arquitectura Empresarial (AE) para los 6 dominios declarados en el Marco de Referencia.	% de implementación de la AE	42%	60%	75%	100%	100%	D. Tecnología	47%	En 2020 se logró un avance acumulado del 11%, pasando del 36% acumulado en 2019 al 47%. La principal causa respecto a no lograr la meta planeada corresponde a la reorientación del esfuerzo de la Dirección de Tecnología a la atención de la operación de la organización en las condiciones de la crisis y emergencia sanitaria C-19, priorizando los proyectos estratégicos de comercialización, los servicios tecnológicos de comunicación y colaboración y los esquemas de trabajo remoto para todas la organización, su soporte y mantenimiento continuo.

Fuente: Información de la Dirección de Tecnología del 15 de enero de 2021

La revisión de los indicadores en los aplicativos ASE e ISOLUCION, mostró que la Dirección de Tecnología y Sistemas de Información, viene registrando y monitoreando el cumplimiento de los proyectos definidos para el área, los indicadores muestran que para el año 2020 no se logró obtener el porcentaje planeado en el cierre de las brechas de Arquitectura Empresarial, el cual estaba definido en el 60% y su logro fue del 47%, fue argumentado por parte de la Dirección de Tecnología y Sistemas de Información así: "*En 2020 se logró un avance acumulado del 11%, pasando del 36% acumulado en 2019 al 47%. La principal causa respecto a no lograr la meta planeada corresponde a la reorientación del esfuerzo de la Dirección de Tecnología a la atención de la operación de la organización en las condiciones de la crisis y emergencia sanitaria C-19, priorizando los proyectos estratégicos de comercialización, los servicios tecnológicos de comunicación y colaboración y los esquemas de trabajo remoto para todas la organización, su soporte y mantenimiento continuo*.", donde se resalta la reorientación que fue necesario realizar a los planes de trabajo para atender lo relacionado con la operatividad de los procesos de CISA, hacia el esquema de trabajo remoto.

4.2.2.2. Indicadores de desempeño: Los indicadores definidos para el proceso de Gestión Tecnológica, se encuentran configurados en la herramienta ISOLUCION, a continuación, se evalúa cada uno:

a. Disponibilidad del Servicio

Se consulta el resultado del indicador "Disponibilidad del servicio", para el periodo del 14 de abril de 2020 al 14 de abril del 2021, observando que la periodicidad estipulada es mensual, con último reporte del 28 de febrero de 2021, lo que no genera oportunidad en la identificación de situaciones que requieran la implementación de planes de acción para subsanar las fallas que se puedan presentar.

El cálculo de este indicador se obtiene con la siguiente fórmula:

((HOM x CSO) - (HNDM x CSND)) / (HOM x CSO) * 100

HOM (Horas Ofrecidas al Mes Lunes a Viernes de 7am - 7 pm)
CSO (Cantidad de Servicios Ofrecidos)
HNDM (Horas no Disponibles al mes)
CSND (Cantidad de Servicios No Disponibles al mes)

El objetivo de este indicador es "Determinar el nivel de disponibilidad de los servicios Tecnológicos ofrecidos por CISA, tanto para usuarios como para partes Interesadas"; al analizar la fórmula, esta mezcla los tiempos no disponibles de los servicios con el total de servicios, es decir, sobrestimando la cantidad de horas no disponibles, por lo cual se requiere ajustar el diseño de la formulación del indicador.

b. Soporte Solucionados en el Tiempo

El indicador "Soporte solucionados en el tiempo"; está desactualizado según su frecuencia mensual, descrita en la ficha técnica, dado que al 14 de abril de 2021 no se había reportado la medición correspondiente al mes de marzo de 2021.

El objetivo de este indicador es "*determinar el nivel de atención oportuna de los soportes técnicos o incidentes tecnológicos que generan cada uno de los procesos*"; se observó que, para la vigencia de abril de 2020 a abril de 2021, el proceso de Gestión Tecnológica realizó la medición y reporte al 28 de febrero de 2021, evidenciando que cumplió la meta del 90%; los casos fueron solucionados en un tiempo menor o igual a 8 horas en el rango de 8 am-5pm.

El cálculo se obtiene con la siguiente formula:

(No. de soportes atendidos en el tiempo (Zeus) / No. de soportes reportados) * 100
En el cálculo del indicador "Soporte solucionados en el tiempo"; basado en la fórmula: (No. de soportes atendidos en el tiempo (Zeus) / No. de soportes reportados) * 100.

Se identificó que éste incluye los casos que fueron solucionados en el mes anterior y el usuario no los ha cerrado, aspecto que genera inconsistencias en el cálculo del indicador y/o inadecuada medición en el monitoreo y gestión de los servicios de soporte de TI.

c. Atención de las solicitudes de soporte de aplicativos institucionales y de terceros

Para el periodo de enero – diciembre 2020, la Dirección de Tecnología realizó la medición y reporte con el siguiente resultado:

De acuerdo con el reporte revisado en ISOLUCION se evidencio que el indicador cumplió la meta del 90% de las solicitudes de soporte de aplicativos institucionales y de terceros, con excepción del mes de julio que registró una medición del 67%, esto debido a la priorización de la implementación del proyecto Procesamiento de Cartera y el de subasta electrónica, lo que implicó orientar los recursos a estos proyectos para dar cumplimiento a las fechas de entrega establecidas.

Al realizar el análisis de la fórmula para el cálculo del indicador se evidencia que dentro del denominador no se tienen en cuenta las solicitudes de los periodos anteriores que no fueron resueltas, ya que las pendientes ingresan como recibidas en el período actual, al no tener en cuenta las no atendidas de los periodos anteriores hace que el indicador sea mayor, por tal razón se recomienda revisar la estructura del indicador, con el fin de refleje la atención del volumen real de solicitudes.

d. Cumplimiento del Plan de Proyectos y Requisitos de Desarrollo de Software CISA

Para la vigencia 2020, la Gerencia de Tecnología realizó la medición y reporte con el siguiente resultado:

Se observó que el indicador obtuvo la meta propuesta de acuerdo al porcentaje de avance del plan de proyectos y requisitos planeado para el periodo, la cual fue definida al 70%, no obstante, al realizar el análisis de la fórmula para el cálculo del indicador se evidencia que se está midiendo en el mismo indicador dos criterios que pueden ser diferentes como *la medición del plan de proyectos* que se define para el año junto con el *avance del cumplimiento de los requisitos solicitados* para el software, no mostrando de manera independiente el avance real de los proyectos siendo este de mayor peso en el indicador en comparación con el cumplimiento de los requisitos de software, por tal razón se recomienda analizar la estructura del indicador de tal forma que se muestre la medición real ya sea de los proyectos como de los requisitos de software.

4.2.3. Gestión de Riesgos de Tecnología de Información

4.2.3.1. Metodología de Riesgos: Central de Inversiones S.A tiene definido en la Circular Normativa N° 107 "*Política de Administración de Riesgos en Central de Inversiones S.A*" Versión 22 del 18 de diciembre de 2020, los lineamientos relacionados con la gestión de los riesgos que se aplican en los procesos de la organización, dentro de los cuales se encuentra los del proceso de Infraestructura Tecnología de la entidad. La metodología está alineada con los aspectos definidos en la guía de riesgos de la Función Pública y el estándar internacional ISO 31000 sobre Administración de Riesgos.

4.2.3.2. Valoración y Tratamiento de los Riesgos: La información de riesgos aportada por el proceso auditado, refleja que la Dirección de Tecnología y Sistemas de Información viene aplicando la metodología definida en la Circular Normativa N°107 "*Política de Administración de Riesgos en Central de Inversiones S.A*" Versión 22 del 18 de diciembre de 2020, y que se ha realizado el monitoreo periódico correspondiente. En el mapa relacionado a continuación se describen los dos riesgos identificados del proceso, clasificados como riesgo de corrupción y riesgo operativo:

Imagen 4. Matriz de Riesgos de TI

Matriz de riesgos - Infraestructura tecnológica

Procesos	Clase	Nombre	Descripción	Agentes generadores
* Infraestructura Tecnológica	Riesgo de Corrupción	RC-IT-01 Recibir y/o pagar bienes o servicios sin el cumplimiento de los requisitos establecidos contractualmente para beneficio propio o de terceros	Materialización del riesgo: Se entenderá como materializado el riesgo cuando en la instancia correspondiente se establezca la culpabilidad sin lugar a dudas. Certificar el cumplimiento del objeto contractual sin que se de cumplimiento a las obligaciones y condiciones establecidas buscando beneficio propio o para un tercero.	* Comportamiento humano
* Infraestructura Tecnológica	Riesgo Operativo	RO-IT-01 Indisponibilidad de los servicios tecnológicos que provee la Dirección de Tecnología a la entidad y a terceros	Materialización objetiva: Esta materialización de riesgo solo se evaluará de forma interna ya que los servicios de terceros estan en nube, implicando que los riesgos están en el proveedor de servicio y contemplados en los contratos. Con respecto a los servicios internos se entenderá materializado el riesgo cuando en el cuatrimestre evaluado el indicador asociado a la disponibilidad de servicios del SIG, haya estado por debajo del limite inferior en dos (2) de los tres (3) periodos evaluados. Fallas en los servicios tecnologicos que provee la Dirección de TI a todas las areas de negocio de la entidad y que afecten la normal operación de los servicios y accesos a los sistemas de información propios y de terceros que tiene CISA. Adicionalmente, Inconvenientes en la conectividad de terceros a los servicios tecnologicos que provee la entidad a las areas y terceros que requieren acceder para realizar su gestión (VPN, telefonia, servicios de red MPLS, portal web).	* Circunstancias políticas * Aspectos tecnológicos

Fuente: Información de la Dirección de Tecnología del 15 de enero de 2021

Se evidenció que en el mapa de riesgos no se está reflejando un análisis detallado respecto a los elementos definidos en la caracterización del proceso, como, por ejemplo, Administración de la Infraestructura Tecnológica, Desarrollo de Software y Soporte a los Desarrollos y Gestión de Nuevos Proyectos; sin embargo, la Dirección de Tecnología se encuentra realizando un análisis de riesgos, valoración de riesgos y controles para el subproceso de "Construcción de software" en sus diferentes etapas, a continuación, se relacionan los riesgos que se encuentran en proceso de aprobación y divulgación:

- R1: Posibilidad de afectación económica por reprocesos producto de ajustes de historias en usuario en etapas tardías (pruebas de aceptación o fase de producción) por especificaciones de requerimientos incompletas o incorrectas.
- R2: Posibilidad de afectación económica por reprocesos debido a Incidentes o solicitudes nuevas de desarrollo de software futuros asociados a problemas de arquitectura del producto.
- R3: Ficha Riesgo: Posibilidad de pérdidas económicas debido a reprocesos por baja calidad en las entregas de producto de Software al equipo de Aseguramiento de Calidad de Software.

Y los riesgos que se encuentran en construcción y aprobación:

- R4: Posibilidad de afectación económica por reprocesos debido a la identificación de hallazgos en ambientes y fases posteriores a QA que obliguen la ejecución de Rollback y/o detención de despliegues en ambiente productivo.
- R5: Posibilidad de afectación por sobrecostos debido a la atención de incidentes recurrentes en producción de los desarrollos implementados.

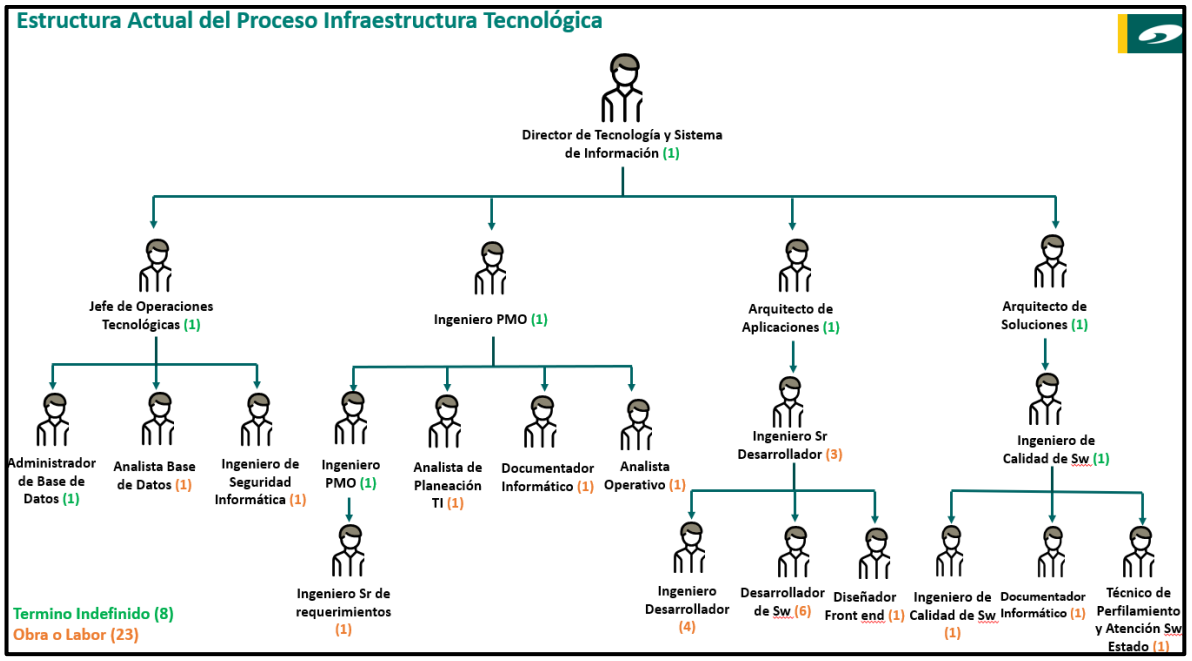
No obstante, lo anterior y considerando que se tiene el esquema de fábrica de software se puede presentar diferentes factores de riesgo relacionadas con la alta rotación de personal que puede afectar el cumplimiento de compromisos pactados con internos y externos, así como la gestión del conocimiento; por esto es importante que en la gestión de riesgos se pueda evaluar este aspecto de la rotación de personal para que se pueda minimizar los impactos generados.

De igual manera no se han identificado eventos de riesgo que puedan afectar los objetivos estratégicos del proceso de Infraestructura Tecnológica.

4.2.4. Estructura de la Dirección de Tecnología

La Dirección de Tecnología y Sistemas de Información tiene definida la siguiente estructura orgánica que le permite desarrollar las funciones y responsabilidades:

Imagen 5. Estructura Dirección tecnológica



Fuente: Información de la Dirección de Tecnología del 15 de enero de 2021

Se verificó que la Dirección de Tecnología y Sistemas de Información tuviera definidas los roles y responsabilidades para los diferentes perfiles, identificándose que actualmente se tienen diecisiete (17) manuales establecidos para los cargos actuales, de los cuales se realizó la verificación, observando su cumplimiento por parte de los servidores públicos adscritos al proceso; el detalle del análisis de puede observar en el numeral 4.4. del informe emitido el día 23 de abril de 2021 de la evaluación al Componente de Planeación y Administración de Tecnologías de la Información, ver Anexo 3.

4.2.5. Planes de Capacitación

Se evidenció que para el año 2020 se realizaron capacitaciones al recurso humano que apoya los procesos de tecnología, las cuales cubrían necesidades identificadas y que requerían ser abordadas por la Dirección. Se observó en la auditoria que en la vigencia 2020, se recibieron cursos y certificaciones en temas como Scrum, Itil, DevOps, Ciberseguridad, Integridad, Transparencia y Lucha contra la Corrupción, Fundamentos de MIPG, entre otros.

4.2.6. Gestión de proyectos de Tecnología

4.2.6.1. Metodología y Políticas para la Gestión de Proyectos: La Dirección de Tecnología y Sistemas de Información de CISA, tiene definido en la Circular Normativa N°127 "*Políticas y Procedimientos para la Gestión de Proyectos de Tecnología"* Versión 16 del 1 de diciembre de 2020, los lineamientos que se aplican en el desarrollo de los proyectos, tanto los definidos en la planeación estratégica de tecnología, como los que han venido generándose por requerimientos del negocio y/o de entes externos.

4.2.6.2. Planes, Programas y Proyectos del PETI: La revisión de la información relacionada con la ejecución de los proyectos, definidos en el PETI, evidenció que la Dirección de Tecnología y Sistemas de Información, ejecutó

en el año 2020, el 100% de 10 de los 12 proyectos definidos, como se puede apreciar en la siguiente imagen, tomada del Aplicativo para el Seguimiento a la Estrategia ASE:

Imagen 6. Proyectos PETI

Nombre de la tarea	Fecha inicial planeada (Tarea	Fecha final planeada (Tarea	Estado (Tare	Respons	Descripc	Total entrega
Actualizar los componentes de la In. Tecnológica para el respaldo de información y su almacenamiento	01/mar/2019 00:00	15/dic/2019 23:59	Finalizada	Sergio A	Garanti	-Infraestruct
Diagnosticar el sistema de gestión de activos fijos y generar un plan de trabajo para su operación.	01/abr/2019 00:00	31/oct/2019 23:59	Finalizada	Sergio A	Es solici	-Diagnóstico
Entregar el procesamiento de cartera con modelo de liquidación cuota única en del sistema Cobra	01/feb/2019 00:00	14/dic/2019 23:59	Finalizada	Sergio A	Limitar	-Funcionalid
Entregar la caracterización del costeo ABC y su estrategia de implementación en operación contable.	01/mar/2019 00:00	31/oct/2019 23:59	Finalizada	Sergio A	Garanti	-Documento
Entregar los módulos de subasta y puja electrónica para bienes muebles, inmuebles Sistema Olympus CE	01/feb/2019 00:00	20/sep/2019 23:59	Finalizada	Sergio A	Platafor	-Sistema de
Entregar un mecanismo de análisis de datos que le permita disponer de información para decisiones	01/feb/2019 00:00	15/dic/2019 23:59	Finalizada	Sergio A	Favorec	-Mecanismo
Realizar el análisis de brecha para la integración del sistema TEMIS WEB en CISA.	15/feb/2019 00:00	30/abr/2019 23:59	Finalizada	Sergio A	Ayudar	-Análisis de
Robustecer la acción de la oficina de proyectos de TI en la gestión, control y entrega de resultados	01/feb/2019 00:00	30/sep/2019 23:59	Finalizada	Sergio A	Exactitu	-Procedimie
Construir un mecanismo colaborativo para la gestión del conocimiento de la entidad	01/ago/2019 00:00	31/dic/2020 23:59	Finalizada	Sergio A	Contar	-Mecanismo
Diseñar e implementar los mecanismos para la gestión de la capacidad y disponibilidad de la IT	01/feb/2019 00:00	30/mar/2020 23:59	Finalizada	Sergio A	Fortalec	-Procedimie

Fuente: Información de la Dirección de Tecnología del 15 de enero de 2021

Se seleccionó como muestra aleatoria los siguientes tres proyectos estratégicos, sobre los cuales se revisó el cumplimiento de lo definido en la Circular Normativa N°127 "*Políticas y Procedimientos para la Gestión de Proyectos de Tecnología"* versión 16 del 1 de diciembre de 2020, evidenciando que no se han desarrollado todos los anexos establecidos en la Circular Normativa, como *Anexo 1: Matriz de Calificación y Priorización de proyectos, Anexo 6: Encuesta de Satisfacción del Servicio de software y Anexo 10: Matriz de Riesgos por tipo de proyecto:*

- POTENCIACION INFRAESTRUCTURA TECNOLÓGICA,
- ACTIVOS FIJOS – GIITIC
- COSTOS, PUJA, SUBASTAS Y OTRAS MEJORAS OLYMPUS CISA-SAE 2020

Verificada la información con la Dirección de Tecnología sobre los anexos se identificó que existen variables que hace que dependiendo del tipo de proyecto se apliquen diferentes anexos, por lo tanto, es importante que se implemente el uso de una herramienta (ejemplo: tabla de referencia, lista de chequeo, tabla de contenido) que permita identificar los elementos y anexos aplicables en cada proyecto desde su fase de planeación, como se describe el numeral 4.5. del informe emitido el día 23 de abril de 2021 de la evaluación al Componente de Planeación y Administración de Tecnologías de la Información, ver Anexo 3.

La Dirección de Tecnología y Sistemas de Información definió diferentes comités de proyectos como son los de Arquitectura, Priorización, General de Proyectos, Evaluación de Inicio de Proyectos y Daily, en los cuales se gestionan las iniciativas y proyectos del área, así mismo se realiza el seguimiento y cumplimiento de estos.,

4.2.7. Cumplimiento Normativo de TI

Evaluados los lineamientos definidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones – Mintic, se evidenció que la Dirección de Tecnología ha venido implementando las directrices relacionadas con la Política de Gobierno Digital, en lo correspondiente al modelo de Arquitectura Empresarial.

La política de Gobierno Digital establecida por Gobierno Nacional define los lineamientos, estándares y proyectos estratégicos, que permiten llevar a cabo la transformación digital de la Entidad, a fin de lograr una mejor interacción

con ciudadanos, usuarios y grupos de interés, permitiendo resolver necesidades satisfactoriamente, problemáticas públicas, posibilitar el desarrollo sostenible y en general, crear valor público.

En la revisión de la documentación por parte de la Auditoría, se pudo evidenciar que la Dirección de Tecnología y Sistemas de Información viene cumpliendo con los lineamientos normativos definidos por los entes de regulación y control, el detalle del análisis de puede observar en el numeral 4.6. del informe emitido el día 23 de abril de 2021 de la evaluación al Componente de Planeación y Administración de Tecnologías de la Información, ver Anexo 3.

Se sugiere que la relación de las normas que son aplicadas en la Planeación y Gestión del proceso de Infraestructura Tecnológica se ajuste a lo definido en la Matriz de Requisitos Legales de la Seguridad de la Información.

4.2.8. Gestión Financiera de TI

4.2.8.1. Plan de Inversión: La Dirección de Tecnología y Sistemas de Información definió el plan de inversión para los años 2019 y 2020, en el cual se detallaron presupuestos para las inversiones en recursos de tecnología como Certificados y Firmas Digitales, Software CRM, Continuidad del Negocio, Mantenimientos Tecnológicos, Servicio de Análisis de Vulnerabilidad, Seguridad en la Información, Mantenimiento Novasec, Mantenimiento SGSI, Mantenimiento Isolucion, Compras, entre otros, en la siguiente imagen se muestra los presupuestos definidos para el año 2020:

Imagen 7. Plan de inversión de TI

Centro Costo	PROYECTO	CGN	CUENTA	TOTAL PRESUPUESTO 2020
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	CERTIFICADOS Y FIRMAS DIGITALES	5111800101	SERVICIOS	**4,389,624**
DESARROLLO	SOFTWARE CRM	5111800101	SERVICIOS	**48,000,000**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	CONTINUIDAD DEL NEGOCIO	5111800101	SERVICIOS	**143,000,000**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	MANTENIMIENTOS TECNOLÓGICOS	5111150103	EQUIPO DE COMPUTACION	**94,500,001**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	SERVICIO DE ANALISIS DE VULNERABILIDAD	5111790101	HONORARIOS	**60,000,000**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	SEGURIDAD EN LA INFORMACION	5111800101	SERVICIOS	**24,000,000**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	MANTENIMIENTO NOVASEC	5111150103	EQUIPO DE COMPUTACION	**40,000,000**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	MANTENIMIENTO SGSI GUARDIUM	5111150103	EQUIPO DE COMPUTACION	**30,000,000**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	MANTENIMIENTO ISOLUCION	5111150103	EQUIPO DE COMPUTACION	**12,000,000**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	COMPRAS	1670020501	EQUIPO DE COMPUTACION	**1,392,000,000**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	MANTENIMIENTO APLICATIVO NOMINA	5111150103	EQUIPO DE COMPUTACION	**3,000,000**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	IMPRESION	5111150103	EQUIPO DE COMPUTACION	**50,000,000**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	ARRENDAMIENTO NUBE	5111180105	ARRENDAMIENTO NUBE	**45,310,517**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	CANALES DE COMUNICACION	5111180104	CANALES DE COMUNICACION	**144,968,064**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	ARRENDAMIENTO PLANTA TELEFONICA	5111180102	MAQUINARIA Y EQUIPO	**142,308,096**
DIRECCION DE TECNOLOGIA Y SISTEMAS DE INFORMACION	ARRENDAMIENTO EQUIPOS DE COMPUTO	5111180103	EQUIPO DE COMPUTO	**316,572,256**
			TOTAL	**2,550,048,558**

Fuente: Información de la Dirección de Tecnología del 8 de febrero de 2021

La Dirección de Tecnología se apoya en el aplicativo Sistema de Gestión Presupuestal - SIGEP, Sistema de información que controla, en donde se registra y ejecuta el presupuesto de gastos de CISA por cada rubro identificado en él presupuesto.

4.2.8.2. Gastos de Funcionamiento: La Dirección de Tecnología y Sistemas de Información generó los registros contables en los cuales se evidenciaron los gastos generados para el funcionamiento del área:

Imagen 8. Gastos de funcionamiento de TI

Etiquetas de fila	Suma de DÉBITOS	Suma de CRÉDITOS	Suma de SALDO FINAL
ARRENDAMIENTO NUBE	130.918.723,00	-	130.918.723,00
BODEGAJE ARCHIVO	131.103,00	-	131.103,00
CANALES DE COMUNICACION	32.470.011,85	540.970,00	31.929.041,85
CUMPLIMIENTO	9.327.479,00	-	9.327.479,00
EQUIPO DE COMPUTACION	430.194.339,00	9.266.666,00	420.927.673,00
EQUIPO DE COMPUTO	33.741.560,50	2.076.016,00	31.665.544,50
HONORARIOS	76.893.199,00	-	76.893.199,00
MAQUINARIA Y EQUIPO	82.878.805,00	7.217.994,00	75.660.811,00
PASAJES AEREOS	974.206,00	-	974.206,00
PROVISIONES DIVERSAS FUNCIONAMIENTO	783.153.914,00	797.077.000,00	- 13.923.086,00
R.C. EXTRACONTRACTUAL	64.838,00	-	64.838,00
SALUD OCUPACIONAL	2.162.700,00	-	2.162.700,00
SERVICIOS	240.834.846,00	4.285.642,00	236.549.204,00
SUMINISTROS	2.372.000,00	-	2.372.000,00
TAXIS Y BUSES	4.548.457,00	607.914,00	3.940.543,00
UTILES Y PAPELERIA	6.189.565,00	-	6.189.565,00
(en blanco)	-		1.015.783.544,35
Total general	**1.836.855.746,35**	**821.072.202,00**	**2.031.567.088,70**

Fuente: Información de la Dirección de Tecnología del 12 de enero de 2021

Los gastos relacionados con "*Provisiones Diversas de Funcionamiento*", el cual representa el 42,64% del gasto de la Dirección Tecnología, corresponde a pagos realizados durante el año por servicios a los siguientes proveedores de tecnología: MICROHARD SAS, AXEDE SA, CONJUNTO COMERCIAL ALMACENTRO PH, ETB SA ESP, COMSEM LIMITADA, E.S.P. EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A., siendo los proveedores MICROHARD SAS Y AXEDE SA los que consumieron aproximadamente el 92% de este gasto, igualmente se observa que para la gestión y seguimiento para las facturas y documentos recibidos se apoya en el aplicativo ZEUS, el cual es un sistema de información que administra los flujos de trabajo de CISA.

En el siguiente cuadro se evidencia el resultado final de lo presupuestado versus lo ejecutado en el año 2020, para los servicios en la nube, y la variación con respecto al año 2019:

Imagen 9. Presupuesto planeado vs Ejecutado de TI

CONCEPTO GASTO	ÁREA ORDENADOR	TOTAL EJECUCION 2020	TOTAL PRESUPUESTO 2020	% EJECUCION	VARIACION $	TOTAL EJECUCIÓN 2019	% VAR.	VARIACION $
BODEGAJE ARCHIVO	VP FINANCIERA Y ADMINISTRATIVA	946	1,631	58%	-685	1,074	-12%	-128
SERVICIOS PUBLICOS	GERENCIA DE RECURSOS / INMUEBLES	337	359	94%	-22	365	-8%	-29
SERVICIO DE ASEO	GERENCIA DE RECURSOS / INMUEBLES	296	272	109%	24	401	-26%	-105
CORREO	GERENCIA DE RECURSOS / CARTERA	171	211	81%	-40	260	-34%	-89
AVALUOS	GERENCIA DE RECURSOS / INMUEBLES	121	197	61%	-76	204	-41%	-83
LIBROS, SUSCRIPCIONES, AFILIACIONES	GERENCIA DE RECURSOS	101	95	106%	5	120	-16%	-19
TAXIS Y BUSES	VP FINANCIERA Y ADMINISTRATIVA	44	124	35%	-80	124	-65%	-80
SERVICIO NUBE	GERENCIA DE TECNOLOGÍA	167	61	275%	106	61	173%	106
CENTRALES DE RIESGO	GERENCIA NORMALIZACIÓN CARTERA	255	218	117%	37	250	2%	6
CERTIFICADO DE BOMBEROS	GERENCIA DE RECURSOS	9	0	NA	9	1	1202%	9
BODEGAJE BIENES MUEBLES	GERENCIA INMUEBLES Y OTROS ACT.	3	10	30%	-7	8	-60%	-5
MANTENIMIENTOS INMUEBLES	GERENCIA INMUEBLES Y OTROS ACT.	1	0	NA	1	27	-95%	-26
RECARGA DE EXTINTORES	GERENCIA DE RECURSOS	0	1	31%	0	1	-75%	-1
FUMIGACIONES	GERENCIA INMUEBLES Y OTROS ACT.	2	3	54%	-1	2	-34%	-1
TOTAL SERVICIOS		**2,452**	**3,182**	**77%**	**-729**	**2,897**	**-15%**	**-445**

Fuente: Información de la Dirección de Tecnología del 8 de febrero de 2021

4.2.8.3. Evaluación Financiera Servicio SaaS: La Dirección de Tecnología y Sistemas de Información ha realizado diferentes actividades relacionadas con el establecimiento de los costos de los servicios SaaS, dentro de los cuales se tiene la Optimización del Modelo de Costos para la Fábrica de Software CISA que define el modelo conceptual y el cálculo de las tarifas.

Se formuló un modelo de costos de TI a partir de la proyección de la demanda de cada servicio y los costos asociados a cada uno de éstos, con base en lo anterior, se definen un conjunto de tarifas unitarias por transacción/unidades representativas de cada servicio; el modelo de costos planteado define los drivers de valor que identifica cuando se satisface las necesidades de los clientes en cada una de las partes del ciclo de vida del desarrollo de software, como: *Entendimiento, Diseño, Construcción, Aseguramiento y Mantenimiento.*

Es así como la Dirección de Tecnología y Sistemas de Información, describe los porcentajes de distribución de cada rol que participa en los pasos del ciclo de fabricación del software, sin embargo, no se evidencia una descripción de los criterios o un procedimiento de cómo estos fueron obtenidos los valores o costos asociados a cada una de las etapas, situación que se describe en el numeral 4.4.6. del presente informe.

4.2.9. Gestión de Proveedores

4.2.9.1. Procedimiento de Selección y Gestión de Proveedores: Central de Inversiones S.A tiene definido en la Circular Normativa N° 044 *"Manual de Contratación"* versión 17 del 30 de diciembre de 2020 y el Memorando Circular N°024 *"Procedimiento de Contratación para las Operaciones Conexas a la Operación mediante Órdenes de Servicio y Contratos"* versión 12 del 30 de diciembre de 2020, los lineamientos relacionados con la contratación y gestión de los proveedores de servicios, y en especial las actividades del supervisor de los contratos; en cumplimiento de esta normatividad, la Dirección de Tecnología y Sistemas de Información basa la selección, contratación y supervisión de los dieciocho (18) proveedores contratados por la Dirección de Tecnologías y Sistemas de Información, se seleccionaron cinco (5) , tomando como base el nivel de ejecución presupuestal en el año 2020, así: MICROHARD SAS, AXEDE S.A., COLUMBUS, COMSEM LTDA. y NEWNET S.A. INTERNETWORKING SOLUTIONS.

Estos proveedores representan aproximadamente el 55% de los gastos de la Dirección de Tecnología durante el 2020, y correspondió a los siguientes servicios definidos en el Plan Anual de Adquisiciones para esta vigencia:

- ARRENDAMIENTO EQUIPOS DE COMPUTO
- CANALES DE COMUNICACIÓN
- ARRENDAMIENTO NUBE
- MANTENIMIENTOS TECNOLÓGICOS
- SERVICIO DE ANALISIS DE VULNERABILIDAD

Para el caso de la evaluación en la selección de los servicios prestados por los proveedores, la Dirección de Tecnología aplica el anexo 001 *"Formato para Sondeo de Estudio de Mercado"* establecido en la Circular Normativa N° 001 *"Procedimiento de Procesos de Gestión Administrativa y Suministros"* versión 46 del 17 de noviembre de 2020, en el cual se consigna la recomendación para la selección del mejor proveedor, de acuerdo a los criterios allí calificados.

La Dirección de Tecnología y Sistemas de Información, mantiene los registros correspondientes a la evaluación y selección de los proveedores de servicios de tecnología, así mismo, realiza las evaluaciones periódicas de los servicios prestados en las que se califican los diferentes criterios generando una calificación que determina el nivel de satisfacción de la Dirección de Tecnología y los aspectos evaluados en este no arrojaron situaciones que puedan estar afectando la operación y ejecución de las actividades de la Dirección de Tecnología y Sistemas de Información, en el desarrollo de la Auditoría se efectuó la evaluación a la gestión de los Acuerdos de Niveles de Servicio – ANS de los proveedores en el numeral 4.3.5. del presente informe.

El detalle de la evaluación al Componente de Planeación y Administración de Tecnologías de la Información se puede observar en el Informe emitido el día 23 de abril de 2021, ver Anexo 3.

4.3. EVALUACIÓN DEL COMPONENTE DE CENTRO DE DATOS Y OPERACIONES DE RED

4.3.1. Control de Acceso Físico y Ambientales al Centro de Cómputo

La Circular Normativa N° 093 "*Política y Procedimiento de Gestión Tecnológica*" – versión 62 del 30 de diciembre de 2020, en su numeral 5.2 define los controles de acceso físico y ambiental, el equipo auditor realizó prueba de recorrido a las instalaciones de la Dirección General en Bogotá el 1 de marzo de 2021 con el fin de validar la implementación de los mismos, solicitando los siguientes soportes documentales para evaluar la eficacia de los controles existentes:

- El listado de usuarios autorizado con acceso al centro de cómputo.
- Listado del personal que ingresó al centro de cómputo durante los meses de noviembre, diciembre de 2020 y enero de 2021 en los formatos de ingreso al CPD.
- Registro del sistema biométrico del año 2020 con los ingresos al centro de cómputo para compararlos con el registro manual en el formato del área de tecnología.

En la inspección del centro de cómputo ubicado en el ercer piso y los centros de cableado localizados en el primer y segundo piso, se verificó que existen controles ambientales de humedad, techo, piso falso a prueba de fuego, planta generadora, UPS y aires acondicionados, etc.; sin embargo, existen debilidades en los controles ambientales del centro de cómputo debido a la ausencia de un techo ignifugo, sistema de supresión de incendios y cableado sin etiquetas.

4.3.2. Mantenimiento de Equipos Tecnológicos

En la evaluación del mantenimiento de los equipos de controles ambientales y eléctricos del centro de cómputo se verificaron los documentos establecidos en el anexo 2 de la Circular Normativa N°093 "*Política y Procedimiento de Gestión Tecnológica"* – versión 62 del 30 de diciembre de 2020, los cuales se detallan a continuación:

- Los formatos de "mantenimiento preventivo equipos de aire acondicionado" generados por el proveedor.
- El documento "Plan mantenimiento 2020.xls" describe los mantenimientos de software y Hardware planeados para el 2020.
- Se validó la existencia de un procedimiento de control que verifique la calidad del servicio y que incluya el mantenimiento de los otros componentes de seguridad ambiental del centro de datos.

Se evidenció que se ejecutó al 100% el plan de mantenimiento de conformidad con el numeral 5.2.4 de la CN N°093. Así mismo, se observaron los mantenimientos del sistema UPS (Servicio de respaldo eléctrico y supresor de picos) realizados en las sedes de Medellín, Barranquilla y Cali realizados el 16/01/2021 y Bogotá el día 26/12/2020, cumpliendo con las actividades de mantenimiento y en las redes de datos se realiza internamente por los mismos especialistas del área de tecnología y su funcionamiento se encuentra sin eventos adversos identificados.

En la planta telefónica de la Dirección general y en Cali, se realiza mantenimiento predictivo que incluye: Back up en CPU, copia de seguridad, limpieza de equipo, medición de voltaje, pruebas de carga satisfactoria, verificación aplicaciones y tarificación.

4.3.3. Gestión de la Capacidad y Desempeño

Con base en el documento Circular Normativa N° 093 "*Política y Procedimiento de Gestión Tecnológica*" – versión 62 del 30 de diciembre de 2020, numeral 5.14 se pudo establecer que el área de Gestión Tecnológica "*debe monitorear el uso de recursos, así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro, con el fin de asegurar el funcionamiento de las aplicaciones o servicios tecnológicos.*", producto del análisis realizado a la información suministrada por la Dirección de Tecnologías y Sistemas de Información, se identificó que la Entidad tiene un modelo definido de servicios y operación de las aplicaciones que están en producción, con una arquitectura establecida del centro de cómputo para los elementos que conforman la infraestructura virtual y física.

Al no existir un plan de capacidad y de gestión de desempeño de TI, el equipo auditor realizó reuniones con la Dirección de Tecnologías y Sistemas de Información y en el análisis de los soportes se observó que:

- El Proceso TI cuenta con la herramienta de control PRTG que permite verificar la disponibilidad de los componentes, umbrales de uso, la internet provista por terceros y estado actual de los componentes, entre otros.

- Para el monitoreo de la Operación de TI, han definido en la herramienta (PRTG), 500 sensores para medir el desempeño y la capacidad de los sistemas tecnológicos de CISA. Esto tiene una categoría por colores como, rojas de alta criticidad y existe una falla, amarilla alerta una situación de posible falla y verdes se opera en normalidad. En el evento que se genere una alerta roja se genera de manera automática un correo electrónico al ingeniero de procesos de infraestructura para su atención.

De lo anterior, no se evidencia trazabilidad de las acciones preventivas que se toman ante las alertas arrojadas en los sensores configurados con alertas amarillas, esto puede generar demoras en la atención y respuesta a incidentes e interrupciones del servicio originadas por falta de capacidad o degradaciones del desempeño.

4.3.4. Mesa de ayuda y Gestión de Incidentes

Con base en la Circular Normativa N°093 "*Política y Procedimiento de Gestión Tecnológica*" – versión 62 del 30 de diciembre de 2020, Anexo 11 denominado *"Instructivos para gestionar los procedimientos de gestión tecnológica*", que relaciona los instructivos para la atención de soporte de aplicativos Institucionales y para la atención y soporte tecnológico, se efectuaron reuniones con el Jefe de Operaciones donde se validó el procedimiento de soporte de atención a usuarios, con el fin de corroborar la gestión y monitoreo que realiza el proceso de Gestión Tecnológica en la entrega de respuesta oportuna y efectiva a los requerimientos de usuarios y la resolución de incidentes.

La entidad cuenta con una mesa de ayuda de microinformática proveída por Microhard mediante el contrato de prestación de servicios No.029-2014 y adicionalmente brindan soporte técnico a los usuarios, dando cumplimiento al numeral 3.5 de la cláusula tercera del contrato, donde indica que "*Por cada 80 equipos de cómputo de escritorio y/o portátiles, el contratista deberá poner a disposición de CISA y sin costo, un (1) técnico exclusivo en un horario de ocho (8) horas por cinco (5) días a la semana, en la sucursal o sede de CISA que disponga el supervisor del contrato*".

Adicionalmente los incidentes presentados en los aplicativos institucionales desarrollados internamente por CISA, son reportados a través de los Usuarios Líderes de Aplicación – ULA a través del flujo en ZEUS "*Soportes Aplicativos Institucionales*" y los requerimientos de servicio técnico, pueden ser registrados por cualquier usuario a través del flujo ZEUS "*Atención y Soporte Tecnológico*" o comunicándose telefónicamente con la mesa de ayuda.

Como soporte de las actividades realizadas por la Dirección de Tecnología, al equipo de Auditoría le fue suministrada documentación soporte en el cual se refleja el modelo de operación que planea implementar la Dirección de TI para la gestión de problemas e incidentes y mesa de servicio, no obstante, a la fecha no cuentan con un procedimiento e indicadores para la gestión y medición de incidentes y problemas, que permita el aseguramiento de la atención y resolución de eventos que se puedan presentar en la infraestructura y servicios de TI. Se sugiere fortalecer el diseño de controles para el aseguramiento en la administración, gestión y monitoreo de la mesa de ayuda e incidentes en los servicios de Tecnología.

4.3.5. Gestión de Acuerdos de Niveles de Servicio – ANS

De acuerdo a la Circular Normativa N°093 versión 62 del 30 de diciembre de 2020, se observa que en el numeral 5.11 describen las "*políticas de gestión de acuerdos de servicios*" y el anexo 6 *"Instructivo para la Gestión de Nivel de Servicios"* donde se menciona la metodología para la definición y gestión de los acuerdos de niveles de servicio para mantener y mejorar la calidad de los servicios de TI a través de un constante ciclo de establecimiento, seguimiento y reporte de cumplimiento de acuerdos, en cuanto a los alcances del servicio de TI.

Respecto a lo anterior se analizó el "*Instructivo atención soporte aplicativos institucionales*" el cual contiene los Acuerdos de Niveles de Servicios Internos, donde se relaciona la atención para incidentes presentados sobre los aplicativos en ambiente productivo; se establece el horario, la disponibilidad, los tipos de incidencias y nivel de soporte al mismo; sin embargo, no incluyen todos los servicios provistos por el área de tecnología tales como: Telefonía, Internet, Correo, Impresoras, Red, Hardware, etc.

Así mismo, se seleccionaron los proveedores críticos acorde con lo informado por el área de Gestión Tecnológica y se solicitaron los contratos de COLUMBUS Networks Colombia Ltda., IFX Networks Colombia S.A.S y MICROHARD S.A.S. identificando que:

- En el contrato de COLUMBUS Networks Colombia Ltda., se tienen establecidos Acuerdos de Niveles de Servicios- ANS, mediante el Anexo 1 del contrato N° 030-2019 para la prestación de los servicios de infraestructura virtual e implementar un esquema de recuperación de desastres – DRP, se definen acuerdos medidos por disponibilidad del servicio e indisponibilidad, no obstante en el contrato no se establece una periodicidad de entrega de reportes a la Entidad con las variables de medición que permitan reflejar la gestión de los servicios contratados, dificultando el monitoreo oportuno de la calidad y cumplimiento de los servicios de TI.

- En el contrato de IFX Networks Colombia S.A.S, se tienen establecidos ANS, entre la Dirección General, sucursales y proveedores mediante el Anexo 1 del contrato N°007-2020, donde se estableció la obligación de un reporte mensual del cálculo del indicador "*disponibilidad de cada canal*", de igual forma CISA verificará estos resultados ingresando al software de gestión del proveedor y comparará dicha información ejecutando la misma fórmula con base a los resultados vistos en el software.

- En el contrato de prestación de servicios N° 029-2014 suscrito con MICROHARD S.A.S., el proveedor se compromete a entregar a título de arrendamiento equipos de cómputo a CISA y se establecieron ANS relacionadas con la entrega de equipos y atención de requerimientos (atención de la mesa de servicios), sin evidenciarse seguimientos e informes de gestión por parte de la jefatura de operaciones tecnológicas que permita la verificación del cumplimiento del nivel de calidad y eficiencia de los servicios contratados.

De acuerdo a lo definido en la Circular Normativa N° 044 *"Manual de Contratación"* versión 17 del 30 de diciembre de 2020 y el Memorando Circular N°024 *"Procedimiento de Contratación para las Operaciones Conexas a la Operación mediante Órdenes de Servicio y Contratos"* versión 12 del 30 de diciembre de 2020, los lineamientos

relacionados con la contratación y gestión de los proveedores de servicios, y en especial las actividades del supervisor de los contratos; en cumplimiento de esta normatividad, la Dirección de Tecnología realiza sus actividades de evaluación de proveedores soportado en el flujo de Zeus de reevaluación de proveedores.

Así mismo se revisó el formato de evaluación de los proveedores de los servicios de tecnología para el año 2020 de COLUMBUS NETWORKS DE COLOMBIA LTDA y MICROHARD S.A.S, observando que se han realizado las respectivas evaluaciones y al analizar dicho formato se observa que no se cuentan con escalas o rangos de los criterios de medición de las variables definidas para calificar el proveedor, al indagar con el jefe de operaciones tecnológicas indicó que da la puntuación de acuerdo al comportamiento y conocimiento que tiene del servicio, siendo una práctica subjetiva y que debería estar atada al resultado del ANS con el fin de contar con elementos formales y objetivos de soporte a los procesos de gestión y evaluación.

4.3.6. Procesos Automáticos en Batch o Lotes – Jobs

De acuerdo con el marco de referencia de COBIT (Objetivos de control para la información y tecnologías relacionadas) dominio "*Entregar y Dar Soporte – Administración de Operaciones*" se debe tener un procedimiento y/o instructivo que refleje las actividades críticas en tecnología, que son ejecutadas mediante procesos automáticos (Batch o lotes) o tareas programadas (Jobs), por lo tanto, se revisó la existencia de controles sobre estos procesos, identificando que parte del procesamiento sobre los sistemas de información se efectúan mediante tareas programadas (*System Jobs*), los cuales son monitoreados y configurados a través de la pantalla de control del manejador de base de datos.

Respecto a la información solicitada sobre la gestión de Jobs fue suministrada una lista y documentación de las tareas automáticas y se validó junto con el Jefe de Operaciones Tecnológicas la configuración de estas, no obstante, no se identificó un procedimiento formalizado para describir los controles y actividades que se deben seguir en caso de diseñar, ejecutar, eliminar y monitorear un Job.

4.3.7. Procedimientos de Copias de Respaldo de la Información

Para la revisión del cumplimiento de políticas de generación y restauración de backups, el equipo de auditoria se basó en la Circular Normativa N°093 "*Política y Procedimiento de Gestión Tecnológica"* versión 62 del 30 de diciembre de 2020, numeral 5.3 y 5.10; se realizaron reuniones y evaluación de documentos para el entendimiento e identificación de controles en los procedimientos de copias de respaldo de la información observando lo siguiente:

La entidad cuenta con un sistema de replicación al centro de datos alterno localizado en Tocancipá – Cundinamarca, con las siguientes estrategias de respaldo:

- FullServer – Todo lo que se hace en Producción, Fileserver, Prometeo y Webserver.
- Replica de SQL – Se replica la data de las bases de datos SQL.

Así mismo, cuentan con un instructivo para la generación y restauración de Backup y el uso de Dataprotector como herramienta para configurar los backups, observando que:

- Diariamente se realiza una copia incremental del fileserver que tiene la carga transaccional más grande.
- Semanal se realiza backup full - completo.
- Administra el inventario de cintas.

Para el análisis de las backups realizados diarios y mensual, se solicitaron 35 de 262 ejecutados diariamente y se evidencia que todos fueron completados satisfactoriamente; posteriormente, se evaluaron cinco (5) logs de los backups realizados semanalmente, evidenciando que el resultado fue satisfactorio para las copias seleccionadas.

Adicionalmente, se revisó el inventario de medios magnéticos entregado al equipo auditor, observando que se cuenta con 3719 cintas de copias de respaldo con información desde septiembre de 2005 en el custodio externo hasta el 30 de septiembre de 2020.
Se analizó el informe del plan de pruebas de restauración, con un periodo evaluado desde febrero a diciembre de 2020; basado en la información del archivo "InformeGeneralPlandeRestauracion.xls", identificando que se cumple con este plan y que en la herramienta Novasec se registran las pruebas de integridad y calidad ejecutadas por parte del Operador que las ejecuta y posteriormente son revisadas por la Oficial de Seguridad.

4.3.8. Control de Licenciamiento de Software

Con base en la Circular Normativa N°093 "*Política y Procedimiento de Gestión Tecnológica*" – versión 62 del 30 de diciembre de 2020 se identificó que la entidad cuenta con una política de Gestión de Activos de Información en el numeral 5.8.1. donde se refiere al uso de software y menciona que ***este "debe ser legalmente adquirido o licenciado mediante distribuidores autorizados a empresas o compañías que lo provean, también se menciona que en caso de necesitarse software diferente al autorizado o de uso libre, se debe tener autorización de la Oficial de Seguridad de la Información***". Sin embargo, no se identificó un procedimiento formal que rijan las actividades de monitoreo de software instalado en los equipos.

En el documento suministrado por la Jefatura de Operaciones Tecnológicas denominado *"Matriz_Software.xlsx"* se identificó el software aplicativo de ofimática y utilitarios que utiliza la entidad el cual es autorizado por la Oficial de Seguridad por ser de uso gratuito; como control de instalación de software para los usuarios finales se cuenta con la restricción de acceso desde el directorio activo, esto para que solo le permita instalar software al usuario que tenga asignado perfil de administrador.

También se cuenta con la herramienta *Spiceworks* que permite efectuar una validación del software de los equipos conectados a la red y se identificó que el análisis se efectuó sobre 106 equipos de la entidad, situación que se ha presentado debido a la implementación del esquema de trabajo en casa por la emergencia sanitaria ocasionada por el COVID, lo que ha conllevado a que no todos los equipos se encuentran conectados como parte de la red LAN, además que existen usuarios que se soportan en sus equipos personales para el trabajo de oficina, presentado desde el 2020, estos tampoco serían objeto de verificación de la herramienta Spiceworks. Estas situaciones hacen que no se efectué un monitoreo completo y efectivo sobre el software instalado en los equipos, además de que se generan brechas de seguridad informática sobre la red de la Entidad al no identificar y contener conexiones de *"end-points"* vulnerables no corporativos (computadores portátiles, teléfonos inteligentes, tabletas, entre otros), que

pueden tener sistemas desactualizados, no contar con soluciones antivirus e incluso podrían estar infectados con malware.

Respecto a lo anterior la Dirección de Tecnología mencionó que se encuentra en el proceso de adquisición de nuevos equipos para asignarlos al personal que no cuenta con este recurso corporativo y con la implementación del proyecto de la red extendida para dar cobertura a todas las conexiones válidas de la red de CISA.

4.3.9. Plan de Continuidad del Negocio (BCP – DRP)

La Entidad cuenta con el Manual N° 022 *"Manual de Continuidad del Negocio"* – versión 6 del 23 de diciembre de 2020, el cual fue estructurado en el año 2019 y basado en la norma ISO22301 gestión de continuidad del negocio, en revisión de este documento y en entrevista con la analista de procesos y continuidad del negocio se estableció que el plan de continuidad de la Entidad cuenta con los elementos y estrategias requeridos para soportar la operación en los eventos y escenarios allí identificados, a continuación se presentan los más relevantes para este tipo de planes:

4.3.9.1. Política de Continuidad del Negocio

En el Manual N° 022 *"Manual de Continuidad del Negocio"* – versión 6 del 23 de diciembre de 2020, numeral 4 se declara como política "*garantizar la generación de valor en la gestión de activos para las entidades del Estado, en las diferentes zonas de CISA, cuando se produce un evento de interrupción".*

4.3.9.2. Análisis del Impacto al Negocio – BIA

La Entidad efectuó un análisis de impacto al negocio a los procesos críticos soportado en el Manual N° 022 *"Manual de Continuidad del Negocio"* – versión 6, anexo 1 "*Análisis de Impacto al Negocio – BIA*", estableciendo seis (6) procesos críticos:

- Proceso de servicio integral al ciudadano
- Proceso de gestión de activos (cartera)
- Proceso de gestión de activos (inmuebles)
- Proceso gestión jurídica del negocio
- Procesos de gestión tecnológica
- Proceso financiero y contable

Así mismo en el BIA, CISA establece las prioridades y tiempo de recuperación de dichos procesos, definiendo que el RTO (Tiempo objetivo de recuperación) en los periodos más críticos es de 24 horas, tiempo prudencial dada la naturaleza del negocio para priorizar las estrategias a seguir en caso de activarse la contingencia.

4.3.9.3. Identificación y Selección de Estrategias BCP y DRP

En la Circular Normativa N° 093 "Política y Procedimiento de Gestión Tecnológica" – versión 62 del 30 de diciembre de 2020, numeral 5.16 y en el Manual N°022 "*Manual de Continuidad del Negocio*" versión 6, numeral 7, se revisó que CISA estableció unas estrategias de recuperación ante interrupciones como se observa a continuación:

Imagen 10. Estrategias de recuperación de TI

A continuación, se presentan las estrategias de recuperación definidas como mecanismo de respuesta, frente a la materialización de cualquier evento de interrupción que pueda conllevar a la indisponibilidad de la operación de CISA:

Indisponibilidad de la infraestructura física	Indisponibilidad de los colaboradores	Indisponibilidad de proveedores y/o terceros	Indisponibilidad de la Tecnología
• Trabajo en casa • Acuerdo con Proveedores • Respaldo entre Zonas	• Personal alterno formalmente definido del mismo proceso • Personal alterno formalmente definido de otro proceso • Capacitación/ Entrenamiento y Gestión del conocimiento	• Acuerdos de nivel de servicio en aspectos de Continuidad de Negocio • Desarrollo de pruebas de continuidad conjuntas con los proveedores críticos	• Estrategia de Recuperación ante Desastres (DRP) – DraaS • Operación de Actividades Manuales

Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

La entidad apoyada en el análisis del BIA ha definido las estrategias de recuperación para suplir el riesgo tecnológico denominado *"Interrupción de la operación de los procesos críticos*", el cual tiene impacto moderado y la probabilidad de ocurrencia es "rara vez", reflejando que los procesos de CISA están conformados para no ser impactados gravemente y que con los antecedentes y la infraestructura actual la operación es estable.

Respecto al DRP, la entidad cuenta con un servicio contratado con COLUMBUS Networks Colombia Ltda., para la recuperación de desastres con disponibilidad 7x24x365, lo que permite contar con respaldo para aplicar los planes de continuidad cuando se genere algún incidente que interrumpa las operaciones basadas en tecnología de la información, el Servicio contratado de DRP, se encuentra configurado con las características descritas por el área de tecnología, basadas en la Circular Normativa N° 093 "*Política y Procedimiento de Gestión Tecnológica"*– versión 62 del 30 de diciembre de 2020, numeral 5.16 y en el Manual N°022 " *Manual de Continuidad del Negocio*" Anexo 9 versión4, numeral 3.4 "*Estrategia de Recuperación de Ante Desastres – DRP*" para la seguridad y operatividad, contando así con un firewall y un VPN applying, el control de la navegación a internet recae sobre el cliente.

De acuerdo con lo analizado, el DRP está compuesto por cinco máquinas, servicio que incluye el espacio para las máquinas en la nube, herramienta de replicación, configuración y administración de los servicios que están replicados con el servidor de base de datos, fileserver, servidor de aplicaciones Prometeo, servidor Webserver y un servicio secundario que controla los perfiles de acceso a la información en contingencias; es un sistema configurado de forma Activo-Pasivo para el trabajo de réplica y se conecta con un mecanismo de transporte de datos estándar (MPLS), así mismo, cada usuario tendría una VPN para tener a acceso a los servicios en el esquema de operación en contingencia para que puedan ingresar a los sistemas críticos establecidos por la Compañía, como son los procesos misionales, la página web y fileserver.

Los planes de continuidad del negocio (BCP) definen acciones y tareas propias de los procesos de CISA para actuar durante y después de alguna situación de contingencia, esto se encuentra documentado en los anexos del Manual N°022 versión 6, con guías de acción para Presidente – Anexo 46 versión 3, Vicepresidente Jurídico- Anexo 48 versión 4, Director de Tecnología y Sistemas de Información – Anexo 51 versión 3, entre otros, identificando el personal clave en cada una de estos procesos, revelando que tienen un diseño organizado donde se incluyen los interesados y define las acciones a seguir por los mismos.

4.3.9.4. Plan de Pruebas del BCP y DRP

De conformidad con el numeral 5.16 de la Circular Normativa N° 093 "*Política y Procedimiento de Gestión Tecnológica"* – versión 62 del 30 de diciembre de 2020,y en el Anexo 56 "*Programa de ejercicios y/o pruebas del Manual de Continuidad del negocio*" del Manual N° 022 "*Manual de Continuidad del Negocio"*, donde se establecen las actividades que se deben realizar para mantener actualizados planes BCP y DRP se solicitó el soporte del Ejercicio de Escritorio – Planes de Continuidad BCP planeado para el año 2020, en el cual se consideraban escenarios de indisponibilidad de servicios de tecnología; sin embargo, se identificó que las actividades de pruebas planeadas no fueron realizadas en su totalidad para llegar a simular una situación de contingencia real y activar el DRP, debido a la crisis sanitaria presentada.

El escenario actual de Pandemia no ha requerido activar el DRP pero si se ha requerido el esquema de trabajo en casa que inicialmente se contemplaba como una estrategia de continuidad, esta nueva forma de trabajo se debe considerar en los ejercicios de pruebas a estos planes, de acuerdo a la metodología estándar ISO /FDIS 22398, la analista de procesos y continuidad del negocio ejecutó el método de escritorio o juego de pruebas con complejidad baja.

La ausencia de pruebas de continuidad y recuperación de desastres puede ocasionar interrupciones en los procesos y operación de negocio ante la debida preparación y alistamiento de información, componentes tecnológicos y recursos necesarios para actuar ante un evento de anormalidad en las operaciones de los procesos o infraestructura tecnológica.

4.3.9.5. Incidente Sucursal Zona Andina

Como proceso adicional a lo establecido en el alcance de la auditoría y dada las circunstancias presentadas durante el período de desarrollo de esta, el 28 de abril de 2021 se presentó un acto vandálico atacando la infraestructura física y robo de equipos de cómputo en la Zona Andina de CISA ubicada en la ciudad de Medellín.

Con el fin de establecer los protocolos activados por la Entidad para reaccionar a dichos eventos, el equipo auditor efectuó una reunión con el Director de Tecnología, la Oficial de Seguridad y la Analista de Procesos y Continuidad quienes estuvieron a cargo de realizar los respectivos análisis y valoraciones de los eventos presentados en la oficina, se activó el comité de crisis y se declaró el evento como un incidente. Se identificó que la Entidad actuó acorde con lo establecido en el procedimiento de gestión de incidentes, referenciado en el Manual de Continuidad del negocio N°022, anexo 10 denominado "*Plan de Manejo del Incidente – Oficial de Continuidad*", para lo cual se llevaron a cabo las siguientes actividades:

- Inspeccionar el lugar para identificar daños físicos.
- Contactar el proveedor MICROHARD S.A.S., responsable de entregar a título de arrendamiento equipos de cómputo para efectos de reemplazar los equipos hurtados y dañados.
- Verificar la conectividad a la red.
- Verificar conexiones remotas.
- Bloquear rack de comunicaciones para evitar conexiones físicas no autorizadas en la sede.

No fue necesario activar el DRP dado que no se presentaron eventos que superaran el RTO (Tiempo objetivo de recuperación) de 24 horas, período establecido de recuperación para los procesos críticos, se realizaron entrevistas a los usuarios afectados con el fin de establecer el nivel de riesgo por la pérdida de información tanto física como digital y/o acceso no autorizado a información confidencial.

Se sugiere dar continuidad y priorización a la culminación del análisis del incidente con el propósito de cumplir los lineamientos establecidos para gestionar dicho evento, implementando oportunamente las acciones correctivas, lecciones aprendidas y actualizaciones que deban ser incorporadas en el Manual de Continuidad, asegurando las respectivas capacitaciones a todos los interesados.

4.3.10. Migración de IPV4 a IPV6

Para la migración de protocolos de IPV4 a IPV6, en el año 2020 se aprobó el presupuesto, no obstante, el Director de Tecnología informó que no se ha implementado por los eventos nacionales de salud del año 2020. La fase de diagnóstico fue completada por lo cual existe un entregable por el consultor contratado Innovate Operational

Infraestructure SAS y se observa que para el análisis se tomó cada artefacto de TI y fue comparado con la ficha técnica del fabricante para el diagnóstico de viabilidad técnica, contando con la configuración requerida para la migración, las cuales se deben tener en cuenta por parte de la entidad cuando se efectué la fase de implementación y se revelan las siguientes excepciones en el informe del consultor:

- Los servidores de versiones Windows Server 2003 – Requiere ajustes tecnológicos.
- Algunas impresoras deben ser actualizadas.
- Se requiere coordinar con el proveedor de servicios para la migración a dual stack.
- Estandarizar el uso de FQDN "Fully Qualified Domain Name "donde se puedan tener IPs estáticas, esto permitirá a los sistemas la comunicación optima por resolución de los DNS por IPv4 e IPV6.

De acuerdo al documento "*Plan de Diagnostico IPv6v1.pdf*" entre las recomendaciones de la consultoría se encuentra: "*Revisar el siguiente modelo de transición desde el punto de vista del recurso humano y recurso técnico, a seguir para todo el ciclo de transición hacia IPv6*."; el Director de Tecnología informó que se realizó lo sugerido en el *"Plan Implementación de IPv6 - Proyecto IPv6 CISA"* y en "*Plan de Diagnostico IPv6 v1*", logrando identificar que el 95% de los artefactos tecnológicos soportan el IPV6; sin embargo, a marzo de 2021 no se ha implementado el proyecto de migración a IPV6.

El detalle de la evaluación al Componente de Centro de Datos y Operaciones de Red se puede observar en el Informe emitido el día 19 de mayo de 2021, ver Anexo 4.

4.4. EVALUACIÓN DEL COMPONENTE DE DESARROLLO DE SOFTWARE Y CONTROL DE CAMBIOS

4.4.1. Ciclo de Vida de Desarrollo del Software

La Dirección de Tecnología de CISA, tiene definido en la Circular Normativa N°127 "*Políticas y Procedimientos para la Gestión de Proyectos de Tecnología"* Versión 16 del 1 de diciembre de 2020, los lineamientos que se aplican en el desarrollo de software, el cual involucra elementos de metodologías ágiles e incluye elementos de la metodología tradicional mediante la definición de las siguientes fases: Inicio, Planificación, Ejecución/Implementación, Seguimiento y Control y Cierre en el numeral "*8. Metodología gestión de proyectos*" de dicha circular.

Durante la auditoría se realizaron reuniones con la Dirección de Tecnología, a quien se les solicitó un listado con todos los requerimientos realizados a través del flujo de Zeus llamado "*Gestión de requisitos mejorado*" de enero de 2020 a abril de 2021, flujo donde se registran los desarrollos nuevos y clasificados como proyectos, para ello se realizó el ejercicio de verificación de fases en conjunto con la Líder de la Oficina de Proyectos de TI quien explicó la metodología de desarrollo de software para el proyecto de desarrollo llamado "Temis para la UGPP del año 2020", como se muestra a continuación:

a. Fase Inicio Proyectos: En esta etapa se realiza la admisión del proyecto validado por el Comité de Arquitectura que se registra en el aplicativo Celoxis, priorización del proyecto incluyendo el contrato, la oferta comercial y se nombra el Scrum Owner o el Gerente de Proyectos; estos documentos son almacenados en el Sharepoint de la Dirección de Tecnología.

b. Fase Planificación Proyectos: En donde se puede encontrar toda la planeación y especificación de los requerimientos como son arquitectura, historia de usuarios, escenarios, prototipos, criterios de aceptación, estimación de los esfuerzos, Sprint Backlog – Sprint Goal o cronograma y matriz de riesgos.

Así mismo, CISA cuenta con la aplicación DevOps donde se registra las estimaciones de las actividades; sin embargo, en este momento la herramienta se encuentra en un período de implementación y no se tiene el detalle de los desarrollos asignados por horas (minutograma); se debe realizar la actualización de la CN N°127, ya que el documento todavía hace referencia la aplicación TFS, la cual era la anterior versión de la herramienta DevOps para asignación de actividades de Microsoft.

Adicionalmente, para la ejecución de los proyectos del cliente externo según la Circular Normativa N°127 "*Políticas y Procedimientos para la Gestión de Proyectos de Tecnología*" versión 16 del 1 de diciembre de 2020, se establecen métricas específicas para cada uno de los proyectos que se miden semanalmente, éstos son:

- Porcentaje de cumplimiento del cronograma (desviación).
- Porcentaje de ejecución presupuestal.
- Satisfacción del servicio o proyecto

Para los proyectos internos se llevan a cabo las métricas del porcentaje de cumplimiento del cronograma y satisfacción del servicio o proyecto, estos indicadores se registran en una ficha en un archivo de Excel denominado "*Indicadores de Proyectos 2020 VF.xls";* adicionalmente, la Líder de la Oficina de Proyectos TI envía semanalmente un informe denominado "*Informe Portafolio Proyectos TI",* mediante la herramienta Celoxis, la cual fue adquirida en septiembre de 2020, donde se presentan las desviaciones de los proyectos, se revisan los proyectos que superan una desviación del 10% y se informa al negocio el avance del proyecto y las acciones a implementar ante las desviaciones.

c. Fase Ejecución/Implementación: En esta fase se ejecutan las actividades definidas en el proyecto, se generan los entregables y se asegura la calidad del producto a entregar.

d. Fase de Seguimiento y Control: En esta fase CISA realiza las actividades de monitoreo y control del proyecto como: seguimiento al cronograma, alcance del proyecto, cumplimiento de compromiso, seguimiento a los acuerdos de nivel de servicio y registro de lecciones aprendidas, la documentación de esta fase reposa en el Sharepoint en la carpeta de "*Ejecución Seguimiento y Control*", en donde se puede encontrar la información de capacitaciones, entrega de mejoras, facturación, modificaciones a bases de datos, comités, controles de cambios asociados al cronograma o a las historias de usuario y otros ítems de acuerdo al proyecto.

Adicionalmente, se tiene definido en la metodología los Daily, los cuales son registrados en la herramienta Microsoft Planner, también llamado tableros Kanban para el seguimiento de cada equipo de trabajo.

e. Fase de Cierre: En esta etapa se genera el informe del cierre del proyecto, la encuesta de satisfacción del cliente, el registro final de lecciones aprendidas que se registra en la aplicación Celoxis, aceptación del usuario y manuales de usuario.

Para la aceptación de proyectos de terceros se genera un "*Acta de Aceptación*" donde se deja constancia de la aprobación de la funcionalidad, la cual se encuentra firmada por CISA, el tercero y el supervisor del proyecto, actualmente este proceso se realiza mediante mensaje de datos (correo electrónico) en cumplimiento del Memorando Circular 59 versión 2 del 8 de octubre de 2020.

Se evidencia que CISA cuenta con un procedimiento diseñado e implementado para dar cumplimiento a la ejecución del ciclo de vida de los sistemas de información, tal como lo enmarca el documento "*G.SIS.01 Guía del dominio de Sistemas de Información*" del MINTIC (Ministerio de Tecnología de la Información y las Comunicaciones) versión 1.1. de octubre de 2019; con el fin de validar la aplicación metodológica expuesta anteriormente en cada una de las fases de la Gestión de Proyectos y de acuerdo a los tipos de proyectos que se definen en la CN N°127 versión 16 en el numeral 6. *"Tipos de proyectos*", se tomó una muestra de 30 solicitudes de las 300 registradas en el flujo "*Gestión requisitos mejorado*" para la vigencia 2020 y se revisaron los soportes en la herramienta Zeus, encontrando las siguientes situaciones:

- Veintitrés (23) radicados no cuentan con la Matriz Priorización, ni el Acta de Inicio (461619, 461744, 461751, 463456, 465906, 465911, 477585, 478150, 479810, 490164, 491295, 494759, 498007, 500449, 501708, 508077, 535425, 548256, 549645, 564037, 580890, 583727, 587261).
- Los documentos de "Plan de Proyecto y Backlog Priorizado" no han sido relacionados en la herramienta de Zeus para los veintidós (22) radicados (461619, 461744, 461751, 463456, 465906, 465911, 477585, 478150, 479810, 490164, 491295, 494759, 498007, 500449, 501708, 508077, 535425, 548256, 549645, 564037, 580890, 583727).
- No se encuentra el cronograma requerido en la fase de planeación para ocho (8) radicados (465911, 477585, 478150, 479810, 501708, 548256, 564037, 587261).
- Dieciocho (18) radicados no cuentan con el acta de aceptación (461619, 461744, 461751, 463456, 465906, 465911, 477585, 478150, 479810, 490164, 491295, 494759, 498007, 500449, 508077, 535425, 548256, 564037).
- Documento de pruebas unitarias sin información para el radicado 570784.
- No se evidencian lecciones aprendidas asociadas a los treinta (30) radicados seleccionados.

Por lo anterior se identifica la falta de soportes o archivos sin información de las solicitudes en el registro de las salidas en la aplicación Zeus en cada una de las fases de la *"Metodología Gestión de Proyectos*" mencionados en la CN N° 127 "*Políticas y Procedimientos para la Gestión de Proyectos de Tecnología*", el equipo auditor no evidenció el cumplimiento del *"Ciclo de vida del software"*.

Así mismo, al validar con la Dirección de Tecnología se evidenció la existencia de otros repositorios y herramientas que son utilizadas para el registro de los documentos entre ellos: Sharepoint de la Gestión Tecnológica denominado "*Dirección TI*", la aplicación Celoxis y la aplicación Zeus, entre otros, por esta razón se sugiere que se defina un único repositorio para los soportes correspondientes y para las lecciones aprendidas generar una bitácora que permita tenerlas en cuenta en los futuros proyectos, con el fin de proporcionar elementos de análisis para no reincidir en oportunidades de mejora o errores ya presentados.

En la revisión de las solicitudes del flujo "*Gestión requisitos Mejorados*" no se evidenció cuales corresponden a un proyecto de más de 180 horas de desarrollo, tal como lo define la CN N°127 en el numeral *"3. Definiciones",* dato que no se muestra en la documentación o herramienta Zeus, lo cual no permite evidenciar que elementos de la metodología del Desarrollo de Software se deben aplicar.

Se sugiere que se incluya la identificación de las salidas o soportes que pertenezcan a este tipo de solicitud, que se defina las horas asignadas a cada solicitud y un único repositorio que maneje la documentación completa que soporte la implementación de la metodología.

4.4.2. Gestión de Cambios

La entidad tiene definido en la Circular Normativa N°093 versión 62 el anexo N°7 "*Instructivo para la Gestión de Cambios"* versión 21 del 20 de octubre de 2020, donde se encuentra el detalle de la gestión y control de los cambios para la liberación e implementación efectiva de los mismos.

Durante la etapa de ejecución de la auditoría para la vigencia 2020 de los 299 radicados de Gestión de Cambios se determinó una muestra de 30 solicitudes para verificar el cumplimiento del anexo 7 de la CN N° 093, tal como se detalla a continuación: 522782, 560279, 560430, 561336, 562152, 563060, 567804, 575848, 577953, 577965, 578650, 579214, 579516, 583913, 585813, 586067, 586581, 586683, 588071, 589099, 589134, 593723, 593997, 593998, 594002, 594006, 594661, 594938, 595344 y 595556, encontrando las siguientes situaciones:

- El 100% de la muestra no cuentan con evidencia física o digital donde se identifique las decisiones tomadas por parte del Comité Asesor del Cambio – CAB, de acuerdo al anexo 7 de la Circular Normativa N° 093 versión 63 del 30 de diciembre de 2020.
- En el 100% de la muestra no se evidenció el Formato de Requerimiento de Cambios – RFC, que incluya los datos básicos de la solicitud formal para la implementación del cambio, como lo menciona la G.SIS.01 "*Guía del dominio de Sistemas de Información*" del MINTIC versión 1.1 de octubre de 2019, subnumeral "*4.2.2 Formato de Cambios*", sin embargo, la Dirección de Tecnología, indica que se utiliza el documento denominado "*Plan de trabajo*", el cual no contiene la información inicial de la solicitud.
- En la muestra seleccionada se evidenció que CISA define los cambios por la prioridad "*Critica*" y "*Programada"* de acuerdo al anexo 7 de la CN N° 093 en el numeral 5 subnumeral "*5.1 Solicitudes de Gestión de Cambios*"; sin embargo, al revisar el documento *"G.SIS.01 Guía del dominio de Sistemas de Información"* del MINTIC versión 1.1 de octubre de 2019, en el numeral "4.2 Procedimiento de cambios" la guía sugiere que exista por lo menos tres (3) tipos de cambios: cambio estándar, cambio normal y cambio de emergencia, por lo tanto se

recomienda definir los tipos de cambios como lo sugiere la Guía, con el fin establecer mayores criterios para el análisis de su clasificación, priorización y gestión de este tipo de requerimientos.

Dado lo anterior es importante la aplicación de la documentación soporte sugerida en el Instructivo para la Gestión de Cambios respecto al Comité asesor del cambio y el Formato de Requerimientos de cambios, además de generar una nueva tipología de los cambios e implementación de indicadores operativos que puedan medir la eficacia de este.

4.4.3. Versionamiento de Software

La Dirección de Tecnología adquirió en agosto de 2020 la herramienta Azure DevOps, la cual está construida para el desarrollo de software ágil y control de versiones, dicha herramienta apoya a los desarrolladores a crear, probar, implementar y supervisar las aplicaciones de la entidad.

En reunión con el Arquitecto de Software Carlos Usma se realizó el recorrido de las funcionalidades de la aplicación que han sido implementadas tal cómo se relaciona en el documento "*Política de Desarrollo*" versión 1.1. del 12 de marzo 2021, numeral "*7.1 Control de Versiones*" entregado por el proceso de Gestión Tecnológica; así mismo, DevOps genera información de evolución ascendente de entrega de desarrollos por debajo de la curva planeada, la velocidad de acuerdo a la cantidad de tareas a desarrollar, evolución ascendente de tareas y promedio de días, entre otras funcionalidades, la herramienta funciona a partir de equipos completos asignados a cada uno de los servicios o productos de valor de la entidad, los cuales constituyen células, con el fin de que el equipo tenga el conocimiento del desarrollo, este también se puede realizar por ramas asignando el desarrollo (Feature) a un recurso específico asociado a un líder que maneja la línea master y protege lo que realizó el desarrollador a través de una inclusión que el desarrollador le solicita al líder, de esta manera una misma célula puede realizar diferentes desarrollos y la línea master es la que no se modifica y así ninguna célula puede sobre escribir las demás modificaciones de las otras células.

En el desarrollo de la auditoría se evidenció que DevOps se encuentra en implementación, no se tiene en este momento el módulo de Continuous Integration (Integración Continua), Continuous Release (Paso a Producción automático), el Pull request (validación del código), estas actividades se realizan de forma manual, es decir el versionamiento no es automático. Se sugiere implementar estos módulos de la herramienta DevOps con el fin de optimizar el proceso de control de versiones del software.

4.4.4. Derechos de Autor ante Dirección Nacional de Derechos de Autor – DNDA

La Dirección de Tecnología tiene definido el procedimiento para el Registro de software desarrollado en CISA, el cual se encuentra documentado en la CN N° 093 *"Política y Procedimiento de Gestión Tecnológica*", Versión 62 del 30 de diciembre de 2020, donde se detalla el procedimiento en el subnumeral 6.2 para generar el "*Certificado de Registro de Soporte Lógico*" del Ministerio del Interior Dirección Nacional de Derecho de Autor DNDA.

La Dirección de Tecnología suministró los últimos registros realizados en febrero de 2020 para las aplicaciones de: SIGA, GIP, CONCISA, ZEUS y PAC.

Si bien, se evidencia la existencia de los *"Certificados de Registros de Soporte Lógico"*, se sugiere que se eleve una consulta al área Jurídica con el fin de identificar el procedimiento que se debe realizar ante la Dirección Nacional de Derechos de Autor para la actualización de éstos Certificados, es decir, cual es el criterio, por ejemplo de porcentajes de cambio, donde se defina cómo hacer la actualización, teniendo en cuenta que el objetivo de este registro es la protección de derechos de autor, reconocimiento de derechos morales y patrimoniales de la entidad.

4.4.5. Control de Acceso para los Ambientes de Desarrollo, Pruebas y Producción

Se solicitó a la Dirección de Tecnología, los usuarios que tienen acceso a los ambientes de Desarrollo, Calidad QA, Preproducción y Producción, los cuales se encuentran distribuidos en los servidores de desarrollo y QA: Devposserver, Aquiles, Tartaro, Vidar y Hela y los servidores de producción: Prometeo, Mdbserver y preproducción Hera, mediante consulta al directorio activo de cada uno, evidenciando que se encuentran asignados los usuarios de acuerdo a su función y cargo, lo cual está alineado al documento "Política de Desarrollo de Software", versión 1.1 de marzo de 2021, numeral "7.8 Ambientes de Desarrollo y Pruebas".

4.4.6. Identificación de Costos de la Fábrica de Software

Para el establecimiento de los costos la Dirección de Tecnología para los servicios Saas (Software as a Service) cuenta con un modelo conceptual de precios y cálculos de tarifas, esté formula costos de TI a partir de la proyección de la demanda de cada servicio y los costos asociados a cada uno de éstos, definiendo las tarifas unitarias correspondientes, la Dirección de Tecnología realiza el análisis de los costos administrativos y de personal mediante matrices en Excel; en el área administrativa se tiene en cuenta los costos administrativos por puesto de trabajo como son: equipo de cómputo, licencia de office, antivirus, extensión telefónica e internet, el costo administrativo por servicios básicos (acueducto, energía, parqueaderos, arriendo, etc.) y las licencias especializadas.

De acuerdo a los reportes suministrados por la Gerencia Contable se observa que en la estructura de gastos para el 2020 se tienen $592 millones, en donde se registran gastos por servicio de nube, nómina y puesto de trabajo, en el rubro de ventas se identifica un ingreso de $1.292 millones generando una utilidad neta de $447 millones, a continuación, se muestra la imagen del archivo enviado por el área Financiera:

Imagen 11: Información Contable

	SUBASTAS	LEVANTAMIENTO DE HIPOTECAS	FONVIVIENDA	INVIAS	COMERCIALIZACION SAE	SOFTWARE	TOTAL
INGRESO	145	90	7.355	1.105	2.492	1.292	12.480
GASTOS	174	96	2.317	635	2.385	592	6.200
AVALUOS	0			14			14
COMISION - PUBLICIDAD	27				332		360
VIGILANCIA			1.992	348			2.340
ASEO				101			101
SEGUROS			46		0	6	52
GASTOS DE VIAJE			3	3	5		11
HONORARIOS ABOGADOS							0
LEVANTAMIENTO TOPOGRAFICO							0
SERVICIO NUBE						167	167
NOMINA	122	70	170	146	1.801	365	2.674
PUESTO DE TRABAJO	24	26	106	23	247	55	481
UTILIDAD OPERACIONAL	-29	-5	5.038	470	107	700	6.280
MARGEN OPERACIONAL	-20%	-6%	69%	42%	4%	54%	50%
Impuestos (Renta, ICA, 4*1000)	-7	0	1.781	174	83	253	2.284
UTILIDAD NETA	-23	-5	3.257	295	24	447	3.996
MARGEN OPERACIONAL	-16%	-6%	44%	27%	1%	35%	32%

Fuente: Información de la Dirección de Tecnología del 24 de febrero de 2021

Para el costo de personal se utiliza un modelo de asignación del recurso por porcentaje de dedicación tanto para el software estado como el software interno, el cual es definido por la Dirección de Tecnología de una manera estimada sin un soporte detallado de la dedicación real de cada integrante del equipo de la fábrica, siendo subjetiva la asignación de los porcentajes de cada proyecto afectando la rentabilidad real y que son reportados al área financiera, así mimo, en reunión realizada con la Dirección de Tecnología se corroboró que esta estimación de dedicación por recurso se realiza mediante la experiencia del líder desarrollador quien tiene el conocimiento del esfuerzo (horas) que puede invertir un recurso para el desarrollo tal como se observa en la siguiente imagen:

Imagen 12: Porcentajes de dedicación – Segundo semestre 2020

CÉDULA	NOMBRE DEL EMPLEADO	DESCRIPCIÓN CARGO	PROYECTO SOFTWARE ESTADO	SOFTWARE ESTADO	PROYECTO(S) CISA	SOFTWARE INTERNO	Total
1032446023	ARENAS ESPITIA PAOLA ANDREA	ANALISTA DE PLANEACION TI	TEMIS (UGPP)	30%	COBRA FUNCIONAMIENTO	22%	
1032446023	ARENAS ESPITIA PAOLA ANDREA	ANALISTA DE PLANEACION TI	TEMIS (FINAGRO)	1%	COBRA PLAN DE MEJORA	30%	
1032446023	ARENAS ESPITIA PAOLA ANDREA	ANALISTA DE PLANEACION TI	TEMIS (SNS)	1%	TEMIS FUNCIONAMIENTO	6%	
1032446023	ARENAS ESPITIA PAOLA ANDREA	ANALISTA DE PLANEACION TI	TEMIS (NUEVOS CLIEN	8%	TEMIS PLAN MIGRACIÓN WEB	2%	
				40%		60%	**100%**
1073691873	MONTOYA PUENTES YULY CAROLINA	DESARROLLADOR DE SOFTWARE	TEMIS (UGPP)	15%	REPORTES (TODOS LOS SISTEMAS)	85%	
				15%		85%	**100%**
1018406435	RODRIGUEZ MUÑOZ ZULMA ROCIO	ARQUITECTO DE TECNOLOGIA	COBRA (SNS)	3%	FUNCIONAMIENTO (TODOS LOS SISTEMAS Y SERVICIOS TI)	90%	
1018406435	RODRIGUEZ MUÑOZ ZULMA ROCIO	ARQUITECTO DE TECNOLOGIA	TEMIS (UGPP)	3%			
1018406435	RODRIGUEZ MUÑOZ ZULMA ROCIO	ARQUITECTO DE TECNOLOGIA	OLYMPUS (ANI)	2%			
1018406435	RODRIGUEZ MUÑOZ ZULMA ROCIO	ARQUITECTO DE TECNOLOGIA	ZEUS (SAE)	2%			
				10%		90%	**100%**

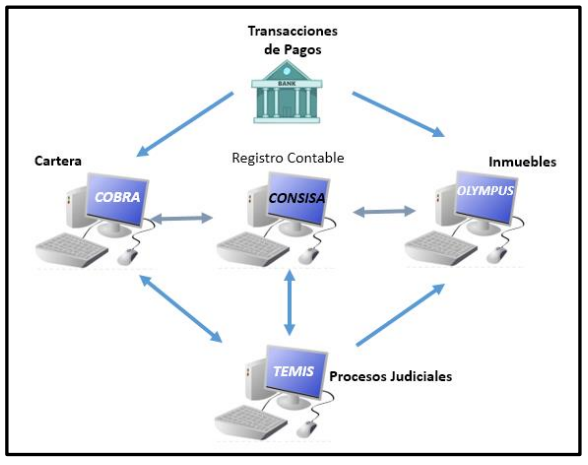
Fuente: Información de la Dirección de Tecnología del 24 de febrero de 2021

Se espera que con la implementación de la herramienta Devops, se optimice el proceso de estimación de tiempos y costos, con el fin de tener un detalle real de las horas ejecutadas vs. las horas planeadas y así generar la información de la rentabilidad por cada uno de los proyectos externos e internos, teniendo en cuenta la identificación de los tiempos dedicados a cada proyecto (desarrollo, soporte, mantenimiento), actividades administrativas, capacitación, imprevistos (incapacidades), tiempos muertos y tiempos extras, toda vez que la rentabilidad se calcula basados en estimaciones de los tiempos dedicados a cada proyecto.

4.4.7. Integridad, Confiabilidad y Confidencialidad de la Información en las Aplicaciones

Los procesos misionales de la entidad están soportados principalmente por las aplicaciones de Cobra, Concisa, Temis y Olympus con una interacción como se muestra a continuación:

Imagen 13: Integración de Aplicaciones



Fuente: Información Dirección TI – Mapa dependencias del 1 de marzo de 2021

Para identificar la integración de las aplicaciones, la Dirección de Tecnología suministró el documento *"Mapa de dependencias SI CISA.xls"* (formato MINTIC), en este archivo se observa todas las relaciones entre las aplicaciones de CISA, además, las aplicaciones cuentan con los procedimientos de cargue de la información, interfaces, totales de control y procedimientos de conciliación.

Todos los meses se hace una conciliación en Cobra, con el fin de que no existan diferencias entre las carteras, el archivo de los Bancos se carga a Cobra y Olympus afectando cada una de las obligaciones y se genera la contabilización automática en Concisa, además, se identificó que las aplicaciones cuentan con diferentes tipos de controles de aplicación, interfaces y de control de acceso para minimizar afectaciones a la integridad, confidencialidad y confiabilidad de la información, el detalle que se encuentra en el numeral 4.4.7. del informe emitido el día 16 de junio de 2021 del Componente Desarrollo de Software y Gestión de Cambios y el numeral 4.11 del informe emitido el día 10 de mayo de 2021 del Componente Seguridad de la Información y Ciberseguridad.

4.4.7.1. Solicitud de Modificación o Adición de Información a las Bases de Datos

Se identificó la existencia de un "*Procedimiento para solicitar Modificación o Adición de información en Base de Datos*", el cual se incluye en el numeral 6. descripción de actividades, subnumeral 6.1 de la CN N°093 versión 62, que permite a las áreas usuarias solicitar cambios en la información de las aplicaciones directamente a las bases de datos, por lo tanto el equipo auditor validó este procedimiento revisando el flujo de Zeus "*Solicitud Modificación o Adición Información en BD*" para el periodo de enero de 2020 a febrero de 2021, encontrando que se radicaron 610 solicitudes de modificación a las bases de datos ejecutándose 594 cambios, una cifra considerable de cambios directo a las bases de datos de la entidad, incrementado el riesgo de manipulación y/o perdida de información.

Al analizar el detalle de estas solicitudes observamos que se encuentran distribuidas por aplicación de la siguiente manera:

Imagen 14: Total de solicitudes Modificación BD

Aplicativos Afectados	Solicitudes
COBRA	206
OLYMPUS SAE	125
TEMIS	123
OLYMPUS	93
IMC	19
CONCISA	12
NUEVO SIGEP	9
PÁGINA WEB	9
SIGA	7
ZEUS	4
GESCAM	1
IMC-FONVIVIENDA	1
Total:	**609**

Fuente: Aplicativo Zeus – Reunión 23 de abril de 2021

Se efectuó una verificación a los conceptos por los cuales se generan este tipo de solicitudes para las aplicaciones COBRA, OLYMPUS, OLYMPUS SAE, TEMIS y CONCISA y se estableció lo siguiente:

a. Para el caso de las 206 solicitudes que afectan el sistema COBRA se encuentran, entre otros conceptos las siguientes:

- ✓ 176 solicitudes de cargues masivos de carteras para cambiar información relacionada con tipos de crédito, actualización de obligaciones, **saldo a capital**, valor de compra, contratos, gestiones de los clientes y depuración de bases de datos de deudores.
- ✓ 29 solicitudes de modificaciones a información específica de alguna obligación, como: saldo de compra, valor de pago, tasa de interés de mora y corriente, naturaleza del cliente, fecha de pago, **acuerdo de pago**, plan de pago, asignar sucursal, porcentaje de participación, agregar pago, **valor obligación**, **propuesta de pago y saldo de capital**.
- ✓ Una solicitud para generar un reporte.

b. Para el sistema OLYMPUS SAE se identificaron 125 solicitudes para la modificación de información relacionada con: base de venta, valor del inmueble, **fecha de cierre de la puja, valor de la oferta, valor propio**, porcentaje de propiedad, acta de inclusión, **precio de venta**, ciudad, sucursal, unificar inmuebles, área del inmueble, matrícula, **fecha de comité**, **orden de elegibilidad**, **valor comercial y precios mínimos**.

Entre las situaciones que llaman la atención en este flujo están las siguientes:

- ✓ El flujo del sistema Zeus denominado "*Procedimiento para solicitar Modificación o Adición de información en Base de Datos*" puede ser iniciado por usuarios del nivel operativo como es el caso del señor Brayan Steven Grijalba Peñuela, Técnico de Datos SAE de la Gerencia de Inmuebles que tiene 39 solicitudes a su nombre.
- ✓ 22 solicitudes se refieren a cambiar el **precio base de venta** porque son inmuebles que pertenecen a otra zona.
- ✓ Solicitudes de cambio por errores de digitación en el campo Nit, **en el plan de pagos de la oferta**, en la fecha de la oferta y en la fecha de promesa de compraventa, como también por errores de transmisión de la SAE.

c. En el sistema OLYMPUS se encontraron 93 solicitudes para la modificación de información relacionada con: número de escritura, estado del inmueble, **valor del inmueble, oferta comercial**, porcentaje de propiedad, **fecha de VPN del inmueble**, número del comprobante, **fecha de cierra de la puja**, fecha de escrituración, **fecha de acta de comité, precios mínimos**, correo electrónico del cliente**, fecha de subasta**, ciudad, días máximo de forma de pago, tipo de documento del cliente, **ID de la puja**, información de la oferta y cambio de observador a participante de clientes inscritos (seis (6) solicitudes).

Al analizar las justificaciones de las solicitudes de cambio a la base de datos se identifican las siguientes:

- ✓ Errores en la digitación en la creación del inmueble, en la asignación del vendedor, fecha del acta de comité, marcación de desistimiento del inmueble, inscripción del cliente como observador y fecha de aprobación de la oferta.
- ✓ Error en el cargue de la oferta y orden de elegibilidad.

d. Se identificaron 123 solicitudes asociadas al aplicativo TEMIS donde se requiere modificar información relacionada con la asignación de tareas a otro usuario, estado de los procesos judiciales, nombres de los apoderados, asignación de los abogados, tipo de proceso, eliminación de obligaciones repetidas, marcación de procesos judiciales, número de radicado y actualización del radicado; situaciones que pueden gestionarse con controles de aplicación que permitan ajustar los datos de acuerdo a las reglas de negocio definidas y con los niveles de aprobación correspondientes.

e. Las 12 solicitudes efectuadas para el sistema CONCISA se refieren a cambio de periodo a comprobantes, crear y actualizar información de terceros, cambio de tercero en un comprobante, **ajuste saldos en cierres contables de mayo y junio de 2020 por duplicidad de registros y corrección de errores en cierre contable**, actualización de una cuenta por pagar y actualizar tabla de giros, es de mencionar que ajustes a saldos en periodos ya cerrados y cambios en comprobantes contables deben efectuarse por procedimientos contables y soportados por documentos contables formales y no modificando datos directamente en la base de datos de la aplicación contable.

Se observa que el flujo incluye en los estados niveles de aprobación como los de la oficial de seguridad y por el área financiera que evalúa el impacto contable; sin embargo, efectuar modificaciones de los datos directamente a las bases de datos hace que se no se tengan en cuenta controles implementados para la gestión de los procesos y dar transparencia a los mismos afectado la confiabilidad e integridad de la información y es una práctica no alineada a un buen gobierno de datos, tal como se establece en la CN N°093 versión 62 de 30 de diciembre de 2020, en el numeral 5.9. Políticas de desarrollo, subnumeral 5.9.1. Capa datos que menciona "*Todos los procesos que ejecute la capa de datos con la base de datos deben ser realizados por medio de procedimientos almacenados, nunca por medio de sentencias DML (Data Manipulation Languaje)"; t*eniendo en cuenta el volumen de estas solicitudes pueden considerarse como una actividad rutinaria que genera carga operativa en el proceso de Gestión Tecnológica.

4.4.7.2 Pruebas de Integridad a las Bases de Datos

Se efectuó una verificación de integridad a las bases de datos de las aplicaciones Temis, Concisa, Olympus y Cobra donde se consideró el análisis de campos vacíos, fechas no válidas, campos negativos y registros duplicados sobre la información suministrada por la jefatura de operaciones tecnológicas el 4 de mayo de 2021, a continuación, se presentan los resultados:

a. Aplicación Concisa: Se obtuvo una tabla con el detalle de los movimientos contables para los periodos comprendidos entre enero y diciembre de 2020 para la cual no se identificaron situaciones de integridad objeto de ser reportadas.

b. Aplicación Temis: Se obtuvo una tabla con el detalle de los procesos judiciales la cual contiene en total 76.619 registros y al analizar duplicados por el campo "*PROCESO*" que es el identificador único en la base de datos de los procesos judiciales se observaron 2.158 casos en los cuales estaban duplicados y 17 casos con tres registros por número de proceso.

c. Aplicación Olympus: En tabla "*Informacion_General*" se estableció que el inmueble identificado con el número 8447 tiene en el campo "*FECHARECEPCION*" registrada en el 2100-12-14 y en tabla "*cedulas_catastrales*" existen avalúos de cuatro inmuebles con fechas fuera del rango normal, como años de 2300, 2219, 5005 y 3012.

En la tabla "*cedulas_catastrales*" se identificó que el inmueble número (campo: IdInmueble) 9678 tiene 11.025 registros de avalúos catastrales en valor (campo: ValorAvaluoCatastral) cero y con fecha (campo: FechaAvaluoCatastral) del 2204-01-01.

d. Aplicación Cobra: Se obtuvo la tabla N_OBLIGACION con el detalle de las obligaciones, la cual contiene en total de 854.705 registros y al analizar duplicados por el campo "*NumeroObligacion*" que es el identificador de las obligaciones se encontraron las siguientes situaciones:

- 943 casos en los cuales estaban duplicados.
- 33 obligaciones con tres (3) registros asociados al mismo número de obligación.
- 5 obligaciones con cuatro (4) registros asociados al mismo número de obligación.

De acuerdo a lo anterior se puede establecer que las bases de datos de las diferentes aplicaciones contienen errores de datos que pueden afectar un correcto procesamiento o confiabilidad en la información, esto se genera por falta de controles de cargue o de reglas de negocio que no están adecuadamente definidas o configuradas en las aplicaciones, por lo tanto, es importante que se identifique la causa raíz de cada una de las situaciones.

El detalle de la evaluación al Componente de Desarrollo de Software y Control de Cambios se puede observar en el Informe emitido el día 16 de junio de 2021, ver Anexo 5.

4.5. EVALUACIÓN DEL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

4.5.1. Evaluación de Riesgos de Seguridad de la Información

La información de riesgos aportada por el proceso auditado refleja que el Oficial de Seguridad de Información viene aplicando la metodología definida en la Circular Normativa N°107 "*Política de Administración de Riesgos en Central de Inversiones S.A*" versión 22 del 18 de diciembre de 2020, y que se ha realizado el monitoreo periódico correspondiente. En el mapa relacionado se evidencian 51 riesgos enfocados a la seguridad de la información, sin embargo, en el análisis realizado a estos riesgos se identifican que algunos de ellos no tienen asociadas causas que puedan afectar la integridad, disponibilidad y confidencialidad de la información y también se confunden causas con riesgos.

En la matriz de riesgos de seguridad de la información suministrada por la Oficial de Seguridad de la Información se evidencia que algunos controles implementados para mitigar los riesgos se enfocan a mitigar la probabilidad de ocurrencia más no al impacto; existen seis (6) riesgos con calificación pura extrema y alta que siguen manteniendo la misma calificación en el riesgo residual, dejando a la entidad en un perfil de riesgo alto.

Es importante señalar que los riesgos de seguridad de la información siempre serán adversos, es decir, que siempre que se presenten podrán afectar cualquiera de los principios de seguridad de la información, por lo tanto, la aplicación de controles debería estar enfocados a mitigar probabilidad de ocurrencia e impacto.

Adicionalmente, se debe tener en cuenta que Central de Inversiones S.A.- CISA es una entidad que entre sus servicios se identifica el diseño y desarrollo de software para terceros, además con este software también se soportan los procesos misionales, en este sentido se recomienda que el perfil de riesgo de seguridad de la información esté por lo menos en un nivel moderado.

4.5.2. Evaluación de Indicadores de Desempeño de Seguridad de la Información y Ciberseguridad

Se revisaron los indicadores del Proceso de Seguridad de la Información registrados y monitoreados, a través del sistema ISOLUCION. Este proceso tiene definido tres (3) indicadores cuyo análisis se presenta a continuación:

a. **Acciones para el Tratamiento de Riesgos:** El objetivo de este indicador es medir el cumplimento de los planes de tratamiento definidos para los riesgos encontrados en la valoración de los activos de información de SGSI; observando en los dos 2 seguimientos realizados en la vigencia 2020 un cumplimiento del 100%

b. **Gestión de Vulnerabilidades Técnicas:** El objetivo de este indicador es realizar la medición de las vulnerabilidades técnicas críticas que sean tratadas en los tiempos definidos para su mitigación después de su identificación observando en los dos 2 seguimientos realizados en la vigencia 2020 un cumplimiento del 100%

c. **Porcentaje de Incidentes de Seguridad de la Información:** El objetivo de este indicador es medir los incidentes de seguridad de la información atendidos, observando en el seguimiento del último trimestre de 2020 se atendieron todos los incidentes de seguridad presentados.

Los indicadores acá mencionados y evaluados están acorde con el nivel de madurez del cumplimiento del Modelo de Seguridad y Privacidad de la Información que tiene CISA y cumplen con lo establecido por MINTIC.

4.5.3. Gestión de Vulnerabilidades Técnicas

A finales del 2020 la Entidad contrató los servicios del proveedor NEWNET para realizar un análisis de vulnerabilidades técnicas a 10 activos considerados críticos, a continuación, mostramos un resumen de los resultados de la evaluación realizada:

Imagen 15. Vulnerabilidades

ACTIVO	DIRECCIÓN IP	CRÍTICAS	ALTAS	MEDIAS
vpn.cisa.gov.co	201.217.201.197	0	0	3
www.cisa.gov.co	201.217.201.202	0	1	3
junta.cisa.gov.co	201.217.201.203	0	0	1
prometeo.cisa.gov.co	201.217.201.210	0	0	2
ase.cisa.gov.co	201.217.201.215	0	2	2
monitoreo.cisa.gov.co	201.217.201.216	0	0	4
informes.cisa.gov.co	201.217.201.220	0	0	3
TemisAAA.cisa.gov.co	201.217.201.223	0	0	3
MDBSERVER	172.30.1.106	1	1	4
PROMETEO	172.30.1.139	0	0	2

Fuente: Tomado del Informe de vulnerabilidades de NewNet – Febrero 2021 suministrado por la Oficial de Seguridad

Se solicitó el plan de remediación de las vulnerabilidades críticas y altas, donde se evidencia que no se tienen actividades claras y definidas para mitigar la vulnerabilidad crítica encontrada en el servidor MDBSERVER, así mismo se evidencia que no se tienen establecidas actividades para mitigar las vulnerabilidades críticas y altas encontradas en el servidor ASE.CISA.GOV.CO.

No obstante, consideramos que el plan de mitigación para la vulnerabilidad crítica del servidor MDSERVER es procedente y debe quedar como las acciones posteriores a la evaluación por parte de la Auditoría, es decir, que las observaciones realizadas por la Oficial de Seguridad de la Información en la mesa de trabajo del día 5 de mayo de 2021 y la documentación soporte y comentarios escritos vía correo electrónico del día 6 de mayo de 2021 deben ser consideradas como plan de mejoramiento.

Es importante mencionar que la vulnerabilidad critica encontrada en el servidor MDBSERVER podría afectar la integridad y disponibilidad de las bases de datos instaladas en este servidor, por lo que se hace imprescindible la ejecución inmediata del plan de mitigación elaborado por la Dirección de Tecnología.

4.5.4. Políticas de Seguridad de la información y Ciberseguridad

CISA cuenta con la Circular Normativa N° 093 "*Política y Procedimiento de Gestión Tecnológica*" – versión 62 del 30 de diciembre de 2020 en la cual se establecen directrices de seguridad informática y operación de tecnología, pero no establece ningún lineamiento sobre seguridad de la información; en el año 2020 se presentó a la Alta Dirección un documento que consolida la política general y las políticas específicas de seguridad de la información (Políticas y Procedimientos del SGSI v1); dentro del análisis realizado al documento se evidencia que CISA adopta las siguientes políticas de seguridad: dispositivos móviles, trabajo en casa, política de mensajes y correos electrónicos, manejo de medios, medios de almacenamiento externo, reutilización o eliminación de equipos de cómputo, control de acceso, usuarios y contraseñas, desbloqueo de cuentas de usuario, eliminación de usuarios, superusuario, usuarios de red, gestión de derechos de acceso privilegiado, monitoreo, gestión de activos de información, seguridad física y del entorno, gestión de capacidad y disponibilidad, adquisición, desarrollo y mantenimiento de sistemas de información, política de generación y restauración de backup, sincronización de relojes, gestión de vulnerabilidades técnicas, política de desarrollo seguro y política para el uso de recursos de internet.

En el análisis realizado a la política general de seguridad de la información se evidencia que esta política no cuenta con los siguientes elementos:

- Compromiso de la Alta Dirección para asegurar los activos de información.
- La entidad requiere recurso humano, económico y tecnológico para que pueda gestionar los riesgos de seguridad de la información a los que está expuesta la entidad.
- El compromiso del cumplimiento legal y de buenas prácticas.
- Gestión de incidentes de seguridad de la información.
- Gestión de seguridad con los proveedores.
- Roles y responsabilidades.
- Seguridad de la información en la continuidad de negocio.
- Cumplimiento.
- Esta política debe estar aprobada y oficializada en el SIG.

La Oficial de Seguridad de la Información informó al equipo auditor que este documento había sido presentado en el Comité Institucional de Gestión y Desempeño del mes de diciembre de 2020, pero no se evidenció el acta de aprobación y su correspondiente formalización en la intranet de CISA.

4.5.5. Procedimientos de Seguridad de la Información

CISA cuenta con los siguientes procedimientos que soportan el cumplimiento de algunas políticas de seguridad de la información establecidas por la entidad las cuales se muestran a continuación y que son parte de la Circular Normativa N° 093 "*Política y Procedimiento de Gestión Tecnológica*" – versión 62 del 30 de diciembre de 2020:

- Procedimiento para gestionar las vulnerabilidades de la plataforma tecnológica
- Instructivo de Identificación, Clasificación y Plan de tratamiento de Activos de Información
- Instructivo para la copia de Información en medios extraíbles

- Procedimiento para el borrado seguro de dispositivos móviles, discos y volúmenes lógicos
- Instructivo Gestión de Cambios
- Instructivo para la generación y restauración de backup
- Instructivo para la atención de incidentes y requerimientos de seguridad de la información
- Procedimiento para el registro de software desarrollado en CISA
- Matriz de requisitos legales de Seguridad de la Información
- Formato de cadena de Custodia
- Planilla de Control Ingreso al Centro de Computo

Sin embargo, no se evidencian procedimientos que soporten el cumplimiento de las siguientes políticas de seguridad de la información: criptografía, seguridad de las comunicaciones y relaciones con proveedores tal como lo establece la *"Guía No 3 Numeral 6 Procedimientos de Seguridad de la Información establecidos por el Modelo de Seguridad y Privacidad de la Información"* de MINTIC.

4.5.6. Roles y Responsabilidades de Seguridad de la Información

La Entidad cuenta con un Oficial de Seguridad de la Información quién tiene la responsabilidad de planear, coordinar y administrar las actividades que soportan el Sistema de Gestión de Seguridad de la Información como lo son, entre otras:

- Gestión de Activos de Información
- Gestión de Riesgos de Seguridad de la Información
- Gestión de Incidentes de Seguridad de la Información
- Plan de Cultura y Sensibilización de Seguridad de la Información
- Elaboración, formalización y seguimiento al cumplimiento de las Políticas de Seguridad de la Información
- Participación en las actividades de Desarrollo de Software y Control de cambios

Así mismo, el Comité Institucional de Gestión y Desempeño tiene establecidas funciones con el fin de asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información en la entidad.

El equipo auditor observó que el área de Seguridad de la Información tiene fortalezas enfocadas al Gobierno de Seguridad de la Información (elaboración y formalización de políticas, lineamientos y procedimientos de seguridad), no obstante, también se observa que se tienen falencias en la operación y seguimiento del Modelo de Seguridad y Privacidad dado que no se cuenta con el personal suficiente para atender los requerimientos, seguimiento y cumplimiento del gobierno de seguridad.

4.5.7. Gestión de Activos de Información

La entidad cuenta con los siguientes documentos e instrumentos para realizar la gestión de activos de información:

- Circular Normativa N°093 – Anexo 09 "*Instructivo de Identificación, Clasificación y Plan de tratamiento de Activos de Información."*
- Aplicativo Novasec – Módulo Activos de Información.
- Matriz de registro de activos de información publicada en la página web de CISA.

En los instrumentos anteriormente señalados se encuentran controles de seguridad de la información tales como: Propietario de los activos, Uso apropiado de los activos, Devolución de los activos, Clasificación de la Información, Manejo de los activos y Etiquetado de los activos; no se evidencia el rotulado de la información de acuerdo con la clasificación establecida por la entidad (información pública, información pública clasificada e información pública reservada).

4.5.8. Gestión de Incidentes de Seguridad de la Información

CISA cuenta con los siguientes elementos para realizar la gestión de incidentes de seguridad de la información en la entidad:

- Instructivo para la atención de incidentes y requerimientos de seguridad de la información. (incluir codificación)
- Herramienta tecnológica ZEUS cuya función es ingresar y categorizar los incidentes de seguridad de la información para que éstos sean gestionados por el Oficial de Seguridad de la Información.

4.5.9. Evaluación de Controles de Seguridad de la Información

Durante el desarrollo de la auditoría se evidenció el cumplimiento de los siguientes controles de seguridad de la información: Cancelación o Ajuste a los Derechos de Usuarios, Sistema de Gestión de Contraseñas, Seguridad del Cableado, Mantenimiento a los Equipos, Política de Escritorio y Pantalla Limpia, Protección Contra Código Malicioso, Seguridad de los servicios de red, Sincronización de relojes, Perímetro de seguridad física, Controles de acceso físico, Protección contra amenazas externas y ambientales, Trabajo en áreas seguras, Revisión y verificación de perfiles-usuarios en las aplicaciones, Seguridad en bases de datos y Hardening de servidores.

Producto de la revisión de la auditoría se observaron las siguientes situaciones:

a. No se realiza una revisión periódica de las políticas de seguridad de las bases de datos por parte del Oficial de Seguridad de la Información, la última revisión de estas políticas fue realizada en el año 2019.

b. No se cuenta con controles ambientales en las instalaciones físicas de la entidad, se identificó una oportunidad de mejora número 1199 registrada en ISOLUCION la cual se encuentra en desarrollo y cuyo objetivo es implementar controles de seguridad ambiental en el Centro de Cómputo.

c. No se cuenta con evidencia que soporte la revisión de los roles y perfiles de las aplicaciones por parte de los líderes de los procesos misionales, el administrador IMC remite mensualmente el listado de usuarios, roles y

perfiles de las aplicaciones misionales a los líderes de los procesos, pero en algunos casos no se evidencian las actividades de revisión por parte de dichos líderes.

El detalle de la evaluación al Componente de Seguridad de la Información y Ciberseguridad se puede observar en el Informe emitido el día 10 de mayo de 2021, ver Anexo 6.

5. HALLAZGOS

5.1. Evaluado los controles de acceso físico y ambiental del Centro de Cómputo, se evidenció que no se ha realizado implementación de control Techo ignifugo, sistema de extinción de incendios y controles ambientales, persistiendo aún los riesgos identificados en la auditoría de 2017 relacionados con la implementación de controles ambientales del Centro de Cómputo, incumpliendo lo establecido en el numeral 5.2 de la Circular Normativa N° 093 "*Política y Procedimiento de Gestión Tecnológica*" – versión 62 del 30 de diciembre de 2020, tal como se desarrolla en el numeral 4.3.1. del presente informe y en el numeral 4.4.1. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

5.2. Evaluada la gestión y monitoreo de los recursos tecnológicos, se evidenció que no se cuenta con un plan formal que contenga el análisis de capacidad de la infraestructura tecnológica de CISA, que incluya los procesos, tecnologías y personas necesarias para el correcto funcionamiento de los servicios de TI de la entidad a mediano y largo plazo en cuanto a desempeño, disponibilidad y optimización de la utilización de recursos que soportan la plataforma tecnológica, incumpliendo el numeral 5.14. de la Circular Normativa N° 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, tal como se desarrolla en el numeral 4.3.3. del presente informe y en el numeral 4.5. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

5.3. Evaluado los indicadores "Soporte solucionados en el tiempo" y "Disponibilidad del servicio", se observó que la medición del mes de marzo no había sido registrada en el aplicativo ISOLUCION, incumpliendo lo establecido en el numeral 5 del anexo 9 del Manual 13 *"Manual del SIG"*, tal como se desarrolla en el numeral 4.2.2.2. del presente informe y en el numeral 4.3. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

5.4. Evaluados los acuerdos de niveles de servicios se evidenció que no se identifica el tipo de acuerdo por diferentes procesos de negocio para aplicativos internos y de servicios prestados por los proveedores donde no se identifica la periodicidad de los reportes con variables de medición, informes de seguimiento y evaluación, incumpliendo lo establecido numeral 5.11 "*Políticas de Gestión de Acuerdos de Servicios* y el anexo 6 "*Instructivo para la Gestión de Nivel de Servicios*" de la Circular Normativa N°093, tal como se desarrolla en el numeral 4.3.5. del presente informe y en el numeral 4.7. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

5.5. Evaluado el cumplimiento de la política de generación y restauración de backups, se evidenció que no se cumple con la periodicidad establecida de envió de cintas al custodio externo, no se diligencia correctamente el Formato Único de Inventario Documental – FUI, ni se encuentra firmado por los responsables, incumpliendo lo establecido en los numerales numeral 5.3 y 5.10 de la Circular Normativa N° 093– "*Política y Procedimiento de Gestión Tecnológica*", tal como se desarrolla en el numeral 4.3.7. del presente informe y en el numeral 4.10. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

5.6. Evaluado el cumplimiento del uso de software relacionado con la política de Gestión de Activos de Información, no se identificó un procedimiento formal que rija las actividades de monitoreo de software instalado en los equipos para dar cumplimiento al numeral 5.8.1. "*Responsabilidad por los activos de información*" de la Circular Normativa N° 093 – versión 62 del 30 de diciembre de 2020, tal como se desarrolla en el numeral 4.3.8. del presente informe y en el numeral 4.11. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

5.7. Evaluado el plan de pruebas del BCP y DRP del año 2020, se evidenció que las actividades de pruebas planeadas no fueron realizadas en su totalidad para llegar a simular una situación de contingencia real y activar el DRP, ocasionada por la emergencia sanitaria presentada por el COVID-19, incumpliendo lo establecido en el Anexo 6 "*Programa de ejercicios y/o pruebas*" del Manual N° 022 "*Manual de Continuidad del Negocio"*, donde se establecen las actividades que se deben realizar para mantener actualizados los planes BCP y DRP, tal como se desarrolla en el numeral 4.3.9. del presente informe y en el numeral 4.12. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

5.8. Evaluando el plan de remediación de vulnerabilidades críticas y altas encontradas en el servidor ASE.CISA.GOV.CO producto de la evaluación realizada por el proveedor NEWNET y presentadas en el informe entregado en febrero de 2021, se evidenció que no se tienen actividades claras y definidas para mitigar dichas vulnerabilidades, incumpliendo con lo establecido en el numeral 5.13.3. "*Remediación de Vulnerabilidades*" de la Circular Normativa N° 093 – versión 62 del 30 de diciembre de 2020, tal como se desarrolla en el numeral 4.5.3. del presente informe y en el numeral 4.4. del informe detallado del componente de Seguridad de la Información y Ciberseguridad emitido el día 10 de mayo de 2021, ver Anexo 6.

5.9. Revisado el cumplimiento metodológico del ciclo de vida del software se revisó una muestra de 30 solicitudes del flujo "Gestión Requisitos Mejorado" y se identificó la falta de soportes o archivos sin información de las solicitudes en el registro de las salidas en la aplicación Zeus o repositorios del Sharepoint, incumpliendo lo establecido en la Circular Normativa N°127 "*Políticas y Procedimientos para la Gestión de Proyectos de Tecnología"* – versión 16 del 1 de diciembre de 2020, tal como se desarrolla en el numeral 4.4.1. del presente informe y en el numeral 4.4.1. del informe detallado del componente de Desarrollo de Software y Gestión de Cambios emitido el día 16 de junio de 2021, ver Anexo 5.

5.10. En la revisión de las solicitudes del flujo "*Gestión requisitos Mejorados*" no se evidenció cuales corresponden a un proyecto de más de 180 horas de desarrollo, dato que no se muestra en la documentación, lo cual no permite evidenciar que elementos de la metodología del Desarrollo de Software se deben aplicar, incumpliendo lo definido en el numeral 3. "*Definiciones",* de la Circular Normativa N°127 "*Políticas y Procedimientos para la Gestión de Proyectos de Tecnología"* – versión 16 del 1 de diciembre de 2020, tal como se desarrolla en el numeral 4.4.1. del presente informe y en el numeral 4.4.1. del informe detallado del componente de Desarrollo de Software y Gestión de Cambios emitido el día 16 de junio de 2021, ver Anexo 5.

5.11. Evaluado las solicitudes que se efectúan por medio del flujo de Zeus denominado "*Modificación o adición información en BD*", se evidenció que cuando se presentan inconsistencias en la información, errores de digitación, problemas de funcionamiento o de información en los aplicativos de CISA, las áreas operativas solicitan modificaciones a través de dicho flujo, las cuales son ejecutadas por el área de Tecnología, a través de acciones directamente sobre la base de datos, para el periodo de enero de 2020 a febrero de 2021 se identificó que se radicaron 610 solicitudes de modificación a las bases de datos ejecutándose 594, esto genera que se no se tengan en cuenta los controles implementados para la gestión de los procesos y dar transparencia a los mismos afectando la confiabilidad e integridad de la información, además es una práctica no alineada a un buen gobierno de datos, como lo establece el numeral 5.9. "*Políticas de Desarrollo*", subnumeral 5.9.1. "*Capa datos*" de la Circular Normativa N° 093 – versión 62 del 30 de diciembre de 2020 que menciona "*Todos los procesos que ejecute la capa de datos con la base de datos deben ser realizados por medio de procedimientos almacenados, nunca por medio de sentencias DML (Data Manipulation Languaje)"*, tal como se desarrolla en el numeral 4.4.7.1. del presente informe.

5.12. Verificada una muestra de 30 solicitudes del flujo denominado "Gestión del cambio", no se registra la evidencia física o digital donde se identifique las decisiones tomadas por parte del Comité Asesor del Cambio CAB, tal como la menciona en el Anexo N°7 "Instructivo para la Gestión de Cambios" de la Circular Normativa N° 093 – versión 62 del 30 de diciembre de 2020, tal como se desarrolla en el numeral 4.4.2. del presente informe y en el numeral 4.4.2. del informe detallado del componente de Desarrollo de Software y Gestión de Cambios emitido el día 16 de junio de 2021, ver Anexo 5.

6. OBSERVACIONES

6.1. Se observó que en la matriz de riesgos de la Dirección de Tecnología y Sistemas de Información, no se está reflejando un análisis detallado respecto a los elementos definidos en la caracterización del proceso para la Administración de la Infraestructura Tecnológica, Desarrollo de Software y Soporte a los Desarrollos y Gestión de Nuevos Proyectos, tal como se desarrolla en el numeral 4.2.3. del presente informe.

6.2. Se observó que él normograma aportado por la Dirección de Tecnología y Sistemas de Información, no contiene los elementos que permitan evidenciar la manera en la que se está dando cumplimiento a los requerimientos de entes externos, emitidos a través de leyes, decretos, resoluciones y otros instrumentos, por parte de organismos de regulación y/o control, tal como se desarrolla en el numeral 4.2.7. del presente informe

y en el numeral 4.6. del informe detallado del componente de Planeación y Administración de Tecnología de Información emitido el día 23 de abril de 2021, ver Anexo 3.

6.3. Evaluadas las actividades y documentación para el desarrollo de los proyectos se observó que no se encuentran definidos los criterios aplicables por cada tipo de proyecto, siendo subjetiva la aplicación de lo definido en la Circular Normativa N°127 "*Políticas y Procedimientos para la Gestión de Proyectos de Tecnología"* – versión 16 del 1 de diciembre de 2020, tal como se desarrolla en el numeral 4.2.6. del presente informe y en el numeral 4.5. del informe detallado del componente de Planeación y Administración de Tecnología de Información emitido el día 23 de abril de 2021.

6.4. En el análisis de los indicadores "Disponibilidad del Servicio", "Cumplimiento Plan de Proyectos y Requisitos de Software" y "Soporte solucionados en el tiempo", se observó que la formula mezcla criterios que no son comparables entre sí, lo que conlleva a inexactitudes en el cálculo, generando sobre o sub estimaciones de los mismos tal como se desarrolla en el numeral 4.2.2.2. del presente informe y en el numeral 4.3. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

6.5. Al realizar el análisis de la fórmula para el cálculo del indicador "Atención de las solicitudes de soporte de aplicativos institucionales y de terceros" se observa que en el denominador no se tienen en cuenta las solicitudes de los periodos anteriores que no fueron resueltas, ya que las pendientes de periodos anteriores se ingresan como recibidas en el período actual, al no tener en cuenta las no atendidas de periodos anteriores hace que el indicador sea sobreestimado, no incluyendo los datos reales de la medición , tal como se desarrolla en el numeral 4.2.2.2. del presente informe y en el numeral 4.3. del informe detallado del componente de Desarrollo de Software y Gestión de Cambios emitido el día 16 de junio de 2021, ver Anexo 5.

6.6. Evaluando los controles de acceso físico y ambiental del Centro de Cómputo se observaron las siguientes debilidades:

a. Puerta de madera al ingreso inicial del centro de Datos.
b. Localización en el último piso (3er) de la sede principal.
c. El cableado de fibras redundantes en el primer piso está próximo a una ventana que da al exterior de las oficinas, con flujo peatonal sin control.
d. Algunos cables no cuentan con marquillas de identificación para facilitar su mantenimiento y adecuado.
e. Las llaves para el ingreso al centro de cómputo no cuentan con una marcación, lo que dificulta en un momento de emergencia identificar la llave de apertura.

Tal como se desarrolla en el numeral 4.3.1. del presente informe y en el numeral 4.4.1. del informe detallado del componente de Centro de Datos y Operaciones de Red el día 19 de mayo de 2021, ver Anexo 4.

6.7. Se observó que el formato "*Reevaluación de proveedores Críticos de Bienes y Servicios de CISA*" no cuenta con escalas o rangos definidos por cada uno de los criterios para la medición de las variables de calificación para el proveedor objeto de la evaluación, tal como se desarrolla en el numeral 4.3.5. del presente informe y

en el numeral 4.7. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

6.8. Se observó que no se está efectuando la validación del software de los equipos conectados a la red de manera completa y efectiva por el esquema de trabajo en casa en donde no todos los equipos se encuentran conectados como parte de la red LAN, además que existen usuarios que hacen uso de sus equipos personales para el trabajo de oficina, generando brechas de seguridad informática sobre la red de la Entidad, tal como se desarrolla en el numeral 4.3.8. del presente informe y en el numeral 4.11. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

6.9. Realizado el análisis de la gestión de capacidad y desempeño no se identificó la trazabilidad de las acciones preventivas que se toman ante las alertas arrojadas en los sensores configurados con alertas amarillas, esto puede generar demoras en la atención y respuesta a incidentes e interrupciones del servicio originadas por falta de capacidad o degradaciones del desempeño, tal como se desarrolla en el numeral 4.3.3. del presente informe y en el numeral 4.5. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

6.10. Se observó que la Dirección de Tecnología cuenta con personal técnico para atender las situaciones presentadas por los usuarios internos; sin embargo, no está estructurado como un servicio de la mesa de ayuda para la atención y resolución de incidentes y problemas que sean registrados, analizados, diagnosticados y escalados para su resolución de acuerdo con la clasificación de niveles de atención (1er, 2do y 3er nivel), tal como se desarrolla en el numeral 4.3.4. del presente informe y en el numeral 4.6. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

6.11. Se observó que la Dirección de Tecnología no tiene un procedimiento formalmente establecido para la gestión de incidentes y problemas que permita el aseguramiento en la atención y resolución de eventos que afecten la funcionalidad y operación en la infraestructura y servicios de TI, tal como se desarrolla en el numeral 4.3.4. del presente informe y en el numeral 4.6. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

6.12. Se observó que no se tiene identificado un procedimiento formalizado para describir los controles y actividades que se deben seguir en caso de diseñar, ejecutar, eliminar y monitorear un Job, aumentando la probabilidad de una eventual falla en las operaciones por posible error humano en la modificación de las instrucciones configuradas en una tarea programada, tal como se desarrolla en el numeral 4.3.6. del presente informe y en el numeral 4.8. del informe detallado del componente de Centro de Datos y Operaciones de Red emitido el día 19 de mayo de 2021, ver Anexo 4.

6.13. Evaluado el avance del proyecto de migración de los protocolos de IPV4 a IPV6, se observó que no se ha iniciado la fase de implementación, tal como se desarrolla en el numeral 4.3.10. del presente informe.

6.14. Realizada la verificación de los manuales de usuario de las aplicaciones que se consolidan en el Sistema Integrado de Gestión – SIG contra los del Sharepoint de la Dirección de Tecnología se observó que no se encuentran actualizados, dado que las versiones son diferentes de acuerdo al control de cambios de cada manual, tal como se desarrolla en el numeral 4.1.2. del presente informe y en el numeral 4.1.2. del informe detallado del componente de Desarrollo de Software y Gestión de Cambios emitido el día 16 de junio de 2021, ver Anexo 5.

6.15. Se observó que en la metodología "*Gestión de Proyectos de Tecnología*", se registran las Lecciones Aprendidas, no obstante, no se cuenta con la consolidación de dichas lecciones junto con los planes de acción que permitan minimizar la ocurrencia de errores presentados en el pasado, tal como se desarrolla en el numeral 4.4.1. del presente informe y en el numeral 4.4.1. del informe detallado del componente de Desarrollo de Software y Gestión de Cambios emitido el día 16 de junio de 2021, ver Anexo 5.

6.16. Se observó que el Formato de Requerimiento de Cambios, no incluye los datos básicos de la solicitud formal para la implementación del cambio, como lo menciona la G.SIS.01 "*Guía del dominio de Sistemas de Información*" del MINTIC versión 1.1 octubre de 2019, subnumeral 4.2.2 "*Formato de Cambios*", tal como se desarrolla en el numeral 4.4.2. del presente informe y en el numeral 4.4.2. del informe detallado del componente de Desarrollo de Software y Gestión de Cambios emitido el día 16 de junio de 2021, ver Anexo 5.

6.17. Se observó que la entidad no se encuentra alineada con el documento G.SIS.01 "*Guía del dominio de Sistemas de Información*" del MINTIC versión 1.1 octubre de 2019 en la definición de los tipos cambios, donde se menciona que las solicitudes de cambios deben ser clasificadas como estándar, normal y emergencia, tal como se desarrolla en el numeral 4.4.2. del presente informe y en el numeral 4.4.2. del informe detallado del componente de Desarrollo de Software y Gestión de Cambios emitido el día 16 de junio de 2021, ver Anexo 5.

6.18. En el desarrollo de la auditoría se observó que la Dirección de Tecnología no tiene claridad sobre los criterios a tener en cuenta para presentar la solicitud de actualización de los "*Certificados de Registro de Soporte Lógico*" ante la Dirección Nacional de Derechos de Autor – DNDA de las aplicaciones propias para mantener vigente la protección de derechos de autor, reconocimiento de derechos morales y patrimoniales de la entidad, tal como se desarrolla en el numeral 4.4.4. del presente informe.

6.19. Realizada la validación de la definición de los costos de los servicios SaaS prestados a los clientes externos y de los servicios internos, se observa que para el costo de personal se utiliza un modelo de asignación del recurso por porcentaje de dedicación, el cual es definido por la Dirección de Tecnología de una manera estimada sin un soporte detallado de la dedicación real de cada integrante del equipo de la fábrica, siendo subjetivo los porcentajes asignados a cada proyecto y que son reportados al área financiera generando impresiones al determinar la rentabilidad de los mismos, tal como se desarrolla en el numeral 4.4.6. del presente informe y en el numeral 4.4.6. del informe detallado del componente de Desarrollo de Software y Gestión de Cambios emitido el día 16 de junio de 2021, ver Anexo 5.

6.20. Efectuadas las pruebas de verificación de integridad a las bases de datos de las diferentes aplicaciones Temis, Cobra y Olympus se identificó que contienen errores de datos y duplicidad de registros que pueden afectar un correcto procesamiento o confiabilidad en la información, esto se genera por la ausencia de controles de cargue o de reglas de negocio adecuadamente definidas o configuradas en las aplicaciones, tal como se desarrolla en el numeral 4.4.7.2. del presente informe y en el numeral 4.7.7.2. del informe detallado del componente de Desarrollo de Software y Gestión de Cambios emitido el día 16 de junio de 2021, ver Anexo 5.

6.21. Se observó que no se tiene documentado un manual de incidentes de seguridad de la información y ciberseguridad en donde se muestre de manera detallada las categorías y subcategorías de incidentes que determine la entidad, así como las actividades que se deben realizar en cada una de las fases sugeridas para la gestión de incidentes de seguridad (preparación, detección, contención, erradicación, recuperación, seguimiento), tal como se desarrolla en el numeral 4.5.7. del presente informe y en el numeral 4.10. del informe detallado del componente de Seguridad de la Información y Ciberseguridad emitido el día 10 de mayo de 2021, ver Anexo 6.

6.22. Se observó debilidad en la operación y seguimiento del Modelo de Seguridad y Privacidad para atender oportunamente los requerimientos, seguimiento y cumplimiento del gobierno de seguridad, tal como se desarrolla en el numeral 4.5.5. del presente informe y en el numeral 4.10. del informe detallado del componente de Seguridad de la Información y Ciberseguridad emitido el día 10 de mayo de 2021, ver Anexo 6.

6.23. Se observó que la entidad no cuenta con procedimientos que soporten el cumplimiento de las políticas de seguridad de la información relacionadas con la criptografía, seguridad de las comunicaciones y relaciones con proveedores tal como lo establece la Guía No 3, numeral 6 *"Procedimientos de Seguridad de la Información establecidos por el Modelo de Seguridad y Privacidad de la Información"* de MINTIC, tal como se desarrolla en el numeral 4.5.4. del presente informe y en el numeral 4.7. del informe detallado del componente de Seguridad de la Información y Ciberseguridad emitido el día 10 de mayo de 2021, ver Anexo 6.

6.24. Realizada la validación de la política general de seguridad de la información se observó que no cuenta con los siguientes elementos y que deberían estar incluidos de acuerdo con lo establecido en las buenas prácticas de la ISO 27001:2013 numeral 4.2.1 que cita:

- Compromiso de la Alta Dirección para asegurar los activos de información.
- La entidad requiere recurso humano, económico y tecnológico para que pueda gestionar los riesgos de seguridad de la información a los que está expuesta la entidad.
- El compromiso del cumplimiento legal y de buenas prácticas.

Esta política debe estar aprobada y oficializada en el SIG, tal cómo se desarrolla en el numeral 4.5.3. del presente informe y en el numeral 4.5. del informe detallado del componente de Seguridad de la Información y Ciberseguridad emitido el día 10 de mayo de 2021, ver Anexo 6.

6.25. Se observó que no se cuenta con evidencia que soporte la revisión de los roles y perfiles de las aplicaciones por parte de los líderes de los procesos misionales, el administrador IMC remite mensualmente el listado de usuarios, roles y perfiles de las aplicaciones misionales a los líderes de los procesos, pero en algunos casos no se evidencian las actividades de revisión por parte de dichos líderes, tal como se desarrolla en el numeral 4.5.8. del presente informe y en el numeral 4.11. del informe detallado del componente de Seguridad de la Información y Ciberseguridad emitido el día 10 de mayo de 2021, ver Anexo 6.

6.26. En el desarrollo de la auditoría se observó que durante la vigencia 2020 y corrido de 2021, no se realizó una revisión de las políticas de seguridad de las bases de datos por parte del Oficial de Seguridad de la Información, tal como se desarrolla en el numeral 4.5.8. del presente informe y en el numeral 4.11. del informe detallado del componente de Seguridad de la Información y Ciberseguridad emitido el día 10 de mayo de 2021, ver Anexo 6.

6.27. Evaluada la matriz de riesgos de seguridad de la información se observó que existen riesgos puros con calificación extrema y alta que tienen el mismo nivel de calificación de riesgo residual luego de la evaluación de controles, situación que se presenta dado que algunos controles implementados para mitigar los riesgos se enfocan a mitigar la probabilidad de ocurrencia más no al impacto, tal como se desarrolla en el numeral 4.5.1. del presente informe y en el numeral 4.2. del informe detallado del componente de Seguridad de la Información y Ciberseguridad emitido el día 10 de mayo de 2021, ver Anexo 6.

7. RECOMENDACIONES

7.1. Se recomienda que la Dirección de Tecnología considere las siguientes actividades para fortalecer la gestión de riesgos de tecnología:

a. Revisar y aplicar la caracterización del proceso e incluir lo correspondiente tanto al gobierno como a la gestión de tecnología, en donde se visualice con claridad los niveles estratégicos, tácticos y operativos.
b. Incorporar en la política y los procedimientos, los servicios prestados por el área, alineados al estándar COBIT.
c. Definir el nivel de riesgo del proceso y subprocesos, generando planes de mejoramiento de los controles que requieran ser fortalecidos.
d. Definir indicadores y actividades de monitoreo para la gestión del riesgo de tecnología.
e. Fomentar en los colaboradores del área una cultura de gestión de los riesgos y los controles, dejando registros de su aplicación.
f. Tener en cuenta los siguientes factores de riesgos relacionados con el desarrollo de software:

- Afectación de los servicios productivos por implementación de cambios fallidos.
- Afectación de los servicios productivos por inadecuada valoración del riesgo del cambio.
- Incumplimiento en la ejecución del presupuesto en los proyectos de desarrollo.
- Rotación de personal que puede afectar compromisos adquiridos por la fábrica de software.
- Gestión del conocimiento por dependencia del personal técnico.

En la medida que se consideren los diferentes factores de riesgo en una gestión de riesgos estos pueden ser medidos y administrados con estrategias que permitan mitigar sus impactos, para el caso de la rotación de personal técnico y dependencia del mismo se pueden establecer mecanismos como programas de retención junto con el área de gestión humana, esquemas de trabajo combinados con fábricas de software externas, personal temporal o freelance y acuerdos de bolsas de horas, entre otras estrategias.

7.2. Se recomienda revisar la estructura de los indicadores de "Atención de las solicitudes de soporte de aplicativos institucionales y de terceros", "Soporte solucionados en el tiempo" y "Cumplimiento Plan de Proyectos y Requisitos de Software" con el fin de que refleje la atención del volumen real de solicitudes por parte del proceso de Gestión Tecnológica y se muestre la medición real ya sea de los proyectos como de los requisitos de software, para el caso del indicador "Disponibilidad del servicio" se debe revisar y ajustar el diseño de la fórmula del indicador de tal forma que se mida realmente el tiempo que se presente como no disponibilidad y también considerar la definición de los límites inferiores y superiores para contar con un umbral claramente definido.

7.3. Se recomienda que la Dirección de Tecnología defina un documento o mapa de toda la normatividad externa, pertinente, en donde se describa con claridad los aspectos de la norma y cómo y con qué actividades se ha venido dando cumplimiento. Así mismo, se generen evidencias del monitoreo realizado y se defina un reporte periódico a la alta dirección sobre el cumplimiento; el normograma igualmente debería contemplar lo definido por entidades de normalización como es el caso de ISO, ISACA y otras que se hayan tomado como referentes en el proceso de Infraestructura Tecnológica.

7.4. Una vez construido y puesto en marcha el nuevo centro de cómputo se sugiere actualizar y complementar la política establecida para la administración y gestión del centro de cómputo, considerando aspectos como:

a. Procedimientos para otorgar, revocar y limitar el acceso a la instalación, considerando todo el personal autorizado que acceda a dicho lugar, como funcionarios, clientes, proveedores, visitantes o cualquier tercera persona.
b. Capacitar al personal del proceso de Gestión Tecnológica en el uso de extintores con simulacros de incendio y rescate para asegurar el conocimiento y las acciones que se deben tomar en caso de incendio o incidentes en el centro de cómputo.
c. Definir responsabilidades sobre el monitoreo, procedimientos de reporte y de resolución de incidentes de seguridad física.
d. Separar las llaves de acceso al centro de cómputo y etiquetarlas para facilitar su utilización.
e. Aseguramiento de la implementación de controles ambientales y físicos como:
    - Sistemas de prevención, detección y extinción de incendios. (Sistema de ingeniería que permite la extinción del fuego incipiente durante los primeros minutos de su generación, de manera automática a fin de salvaguardar personas, bienes e inmuebles).
    - Vigencia de Extintores.
    - Sistema de ventilación / Aire Acondicionado.
    - Control de temperatura y humedad.
    - Marquillas de cableado.

f. Evaluar los riesgos a los que se podrá ver expuesto el nuevo centro de cómputo, que permita prever la administración y gestión de riesgos.
g. Realizar un análisis de factores de riesgos para centro de cableado en los pisos 1 y 2 restringiendo el flujo peatonal.
h. Obtener las certificaciones pertinentes respecto al cableado de datos y eléctrico.

7.5. El proceso de Gestión Tecnológica actualmente se encuentra diseñando el plan de capacidad y desempeño de TI y adelantando el proyecto de migración de documentación histórica digital para conservar esta información en un repositorio dedicado a esta función que se denomina *historico.cisa.gov.co.,* es importante considerar que estos deben estar alineados con el Plan Estratégico de Tecnología de Información - PETI.

Se recomienda documentar el análisis de capacidad tecnológica de los activos críticos con el fin de proyectar la atención de los requerimientos y necesidades futuras como: recursos tecnológicos, cargas de trabajo, almacenamiento y contingencias, con el fin de garantizar la disponibilidad de manera continua en la infraestructura tecnológica que soporta el negocio.

El análisis de la Gestión de la Capacidad debe estar soportado en modelos y simulaciones de diferentes escenarios de capacidad, monitoreo del uso y rendimiento de la infraestructura de TI y la gestión de la demanda. Es importante diseñar indicadores que faciliten la medición de la gestión de capacidad, tales como:

- El uso de recursos.
- Desviaciones de la capacidad real sobre la planificada.
- Análisis de tendencias en el uso de la capacidad.
- Análisis de la capacidad y monitorización del rendimiento.
- Impacto en la calidad del servicio, disponibilidad y otros procesos TI.
- Porcentaje de picos donde excede la meta de utilización.
- Análisis de alertas preventivas y correctivas

El procedimiento de gestión de monitoreo de capacidad debe permitir identificar los análisis y acciones que se toman producto de las mediciones de alertas preventivas y correctivas, con el fin de establecer el adecuado cumplimiento y gestión del plan.

Un plan de capacidad facilita la asignación presupuestal para inversiones en recursos tecnológicos y la atención oportuna de requerimientos tecnológicos necesarios para soportar los procesos de negocio.

7.6. Se recomienda fortalecer la estructura actual de la mesa de ayuda, considerando el modelo de operación que se encuentra diseñando en la Dirección de Tecnología, cuyo enfoque está alineado con un esquema ITMS (Administración de servicios de Tecnología de Información), que permita evaluar el impacto de TI en los diferentes procesos de negocio que cuente con la definición roles, responsabilidades y Acuerdos de Niveles de Servicio, del equipo de funcionarios que deberá atender los incidentes.

El portafolio de los servicios ofrecidos por tecnología, deben ser administrados, gestionados y monitoreados mediante un proceso consolidado de mesa de servicio que asegure la administración de activos, problemas

e incidentes; este modelo debe estar soportado con una herramienta tecnológica robusta que permita la configuración, clasificación y medición de los servicios que deben ser administrados.

La documentación de un procedimiento de gestión de incidentes fortalece el flujo de las actividades e implementación de controles para el escalamiento de los niveles de atención de acuerdo con la criticidad o complejidad del evento.

El diseño y medición de indicadores contribuye a la mejora continua del proceso, es importante establecer en el modelo de operación indicadores que permitan el monitoreo de la resolución, cierre y análisis de tendencias de incidentes. Por ejemplo: Cantidad de incidentes repetidos, Cantidad de incidentes escalados, Tiempo de resolución del incidente y Esfuerzo de resolución del incidente, entre otros.

7.7. Con el propósito de fortalecer la gestión de los proveedores de la Dirección de Tecnología se recomienda implementar las siguientes actividades:

- Documentar y formalizar los acuerdos de niveles de servicio (ANS) para cada uno de los servicios prestados por el proceso de Gestión Tecnológica en los procesos de negocio.
- Definir de manera contractual con el proveedor COLUMBUS Networks Colombia Ltda, la entrega periódica de los informes de gestión del servicio prestado y para el proveedor MICROHARD S.A.S. la formalización de informes de gestión de los acuerdos de niveles de servicio establecidos, con el fin de mantener un monitoreo objetivo basado en indicadores y fortalecer la adecuada gestión de proveedores de tecnología.
- Junto con la jefatura de procesos y productividad definir escalas o rangos definidos por cada uno de los criterios para la medición de variables de calificación cuando es necesario reevaluar un proveedor crítico, de tal manera que no se llegue a incurrir en la subjetividad de una calificación.

7.8. Con el fin de mejorar la administración de las operaciones en la ejecución de procesos automáticos en batch o en lotes, se sugiere definir un procedimiento que incluya, entre otras actividades o controles:

- Que se identifique la periodicidad para la ejecución de los procesos automáticos y/o *Jobs.*
- Un cronograma de ejecución que involucre los responsables de la ejecución, hora de inicio, hora de finalización, insumo (pueden ser datos de entrada o salidas de otros procesos), salida, estado de finalización y número de reprocesos.
- Existan totales de control y/o listados de excepción que permitan identificar el número de registros cargados o no cargados y si aplica, el valor de la suma de los registros.
- Existan procedimientos de depuración y análisis de los listados de excepción.

7.9. Se recomienda dar continuidad a la fase de implementación de la migración al protocolo IPV6, con el fin de cumplir lo dispuesto por el MINTIC, se sugiere incluir los cambios en la infraestructura tecnológica que se hayan efectuado desde la fecha de la elaboración del diagnóstico, de tal forma que se pueda medir el impacto y posibles nuevas consideraciones a tener en cuenta.

7.10. Se recomienda dar cumplimiento al envío de copias externas al custodio en el periodo que define el actual procedimiento o considerar un análisis de riesgo donde se pueda efectuar una variación al periodo que se envía al sitio externo que permita el ajuste del procedimiento, así como establecer un control garantice la firma de quien entrega y recibe las cintas enviadas a custodia externa.

7.11. Se recomienda establecer un procedimiento formal que asegure la implementación de actividades de control para el monitoreo del software autorizado que debe estar instalado en los equipos de la entidad, que contemple la periodicidad de la ejecución de la herramienta, soporte del análisis efectuado respecto a la línea base de software, protocolo de desinstalación (si es necesario), con el fin de dar cumplimiento a la Ley 603 de derechos de autor.

7.12. Dar continuidad al proceso de adquisición de nuevos equipos para asignarlos al personal que no cuenta con este recurso corporativo y con la implementación del proyecto de la red extendida para dar cobertura a todas las conexiones válidas de la red de CISA y reforzar con la implementación de controles de protección de punto final que permitan generar alertas y tratar las amenazas identificadas en las conexiones remotas de equipos no corporativos, cuando no se cumplan las políticas del servidor, de antivirus y antispyware.

7.13. Se recomienda efectuar una revisión al plan establecido en los ejercicios de escritorio – planes de continuidad BCP´s diseñados en el año 2020, ajustándolo a la nueva normalidad que ha conllevado la pandemia, de tal forma que se identifiquen la totalidad de escenarios, infraestructura, medidas de control, análisis de riesgos como ciberataques, pérdida de funcionarios ante un evento desafortunado de muerte, que puede afectar el conocimiento o prestación de servicio definido actualmente para declarar un plan de continuidad de negocio o activar un DRP.

Es importante considerar que en la medida que se avance en las pruebas de continuidad se deben establecer planes de acción que les permitan cerrar las brechas presentadas en los ejercicios, de tal forma que a mediano plazo puedan escalar el nivel de madurez de complejidad del ejercicio hasta llegar al nivel Alto y Alto* para asegurar que la Entidad está preparada para reaccionar en una eventualidad por método de gestión integral o de cooperación por método de escala completa.

7.14. Se recomienda que los planes de acción sean diseñados e implementados de manera inmediata cuando se identifiquen vulnerabilidades críticas y altas en algún elemento de la infraestructura tecnológica (MDBSERVER y ASE.CISA.GOV.CO) relacionadas con la seguridad de la información ya que podrían afectar la disponibilidad y confidencialidad de la información de los procesos soportados. Lo anterior con el fin de dar cumplimiento a lo estipulado en la Circular Normativa No. 93 de diciembre de 2020 que establece en el numeral 5.13.1 Identificación de Vulnerabilidades Técnicas, que el Oficial de Seguridad de la Información debe planificar las actividades de identificación para prevenir efectos adversos en la ejecución de descubrimientos automáticos y aplicar medidas, tales como horarios no productivos, backups, protocolos de comunicación y monitoreo de servicios entre otros.

7.15. Se recomienda realizar monitoreo al cumplimiento de las políticas para el desarrollo de seguridad a las bases de datos con el fin de detectar de manera oportuna errores o problemas que se puedan presentar en la

configuración de las bases de datos y que podrían afectar la integridad, confidencialidad y disponibilidad de la información contenida en las mismas, lo anterior en concordancia con lo estipulado en la Circular Normativa No. 93 de diciembre de 2020 señalado en el capítulo 5.9.6 Políticas para el desarrollo de bases de datos.

7.16. Se recomienda que los líderes de proceso documenten la evidencia sobre la revisión del informe mensual de perfiles de usuarios que genera el administrador IMC y éste sea reportado al Oficial de Seguridad de la Información, en concordancia con el numeral 5.1.3.4 Actualización de las cuentas de acceso a los componentes tecnológicos y/o sistemas de información que establece que los líderes de proceso son los responsables de la creación, eliminación o modificación de perfiles de acceso.

7.17. Respecto a la gestión de riesgos de seguridad de la información se recomienda establecer controles de seguridad de la información que permitan disminuir el impacto sobre los riesgos que podrían afectar la confidencialidad, disponibilidad e integridad de la información, principalmente en los riesgos puros cuya calificación es alta y extrema. Lo anterior dará cumplimiento a los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas de la Función Pública Numeral 5.4 Controles Asociados a la Seguridad de la Información.

7.18. Se recomienda incluir los siguientes elementos en la política general de seguridad de la información con el fin de dar cumplimiento a lo establecido en la norma ISO 27001:2013 Numeral 4.1.2 que establece:

- Compromiso de la Alta Dirección para asegurar los activos de información.
- La entidad requiere recurso humano, económico y tecnológico para que pueda gestionar los riesgos de seguridad de la información a los que está expuesta la entidad.
- El compromiso del cumplimiento legal y de buenas prácticas.
- Esta política debe estar aprobada y oficializada en el SIG.

7.19. Se recomienda elaborar un manual o guía de gestión de incidentes de seguridad de la información que contenga las categorías y subcategorías de incidentes que determine la entidad, así como las actividades que se deben realizar en cada una de las fases sugeridas para la gestión de incidentes de seguridad (preparación, detección, contención, erradicación, recuperación, seguimiento), este documento ayudará a minimizar los impactos adversos de los incidentes en CISA y sus operaciones mediante las salvaguardas adecuadas como parte de la respuesta a los incidentes que se puedan presentar.

7.20. Se recomienda elaborar, formalizar y hacer seguimiento a los procedimientos que soporten el cumplimiento de las políticas de seguridad de la información relacionadas con la criptografía, seguridad de las comunicaciones y relaciones con proveedores tal como lo establece la Guía No 3 Numeral 6 Procedimientos de Seguridad de la Información establecidos por el Modelo de Seguridad y Privacidad de la Información de MINTIC.

7.21. Respecto al soporte documental del "Ciclo de vida de Sofware", se sugiere analizar la posibilidad de implementar una herramienta robusta para la gestión de proyectos en CISA, mediante la gestión de procesos

automatizados, flexibles y orientados a resultados, con el fin de tener unificado un repositorio donde se consoliden las salidas de cada una de las fases de la "Metodología Gestión de Proyectos", teniendo en cuenta los siguientes aspectos:

- Horas estimadas en los desarrollos para clasificación de los proyectos
- Definir los soportes o salidas de los radicados de acuerdo al tipo de solicitud.
- Evidencia física o digital Comité Asesor del Cambio CAB.
- Proceso revisión de calidad con el fin de verificar que el soporte documental sea válido.

Se debe considerar la implementación de una herramienta tipo lista de chequeo o tabla de referencia por cada proyecto desde su fase de planeación donde se identifique claramente la aplicabilidad de los elementos y salidas de la Circular Normativa No. 127, con el fin de apoyar las actividades de control de calidad y monitoreo del proyecto.

7.22. Efectuar un análisis junto con los dueños de los procesos de las causas que generan las solicitudes de corrección o cambio de información sobre las bases de datos, con el fin de establecer controles sobre las aplicaciones y ajustes a las reglas de negocio de los procesos que minimicen el volumen de estos cambios y en caso de requerirse por alguna situación de fuerza mayor se debe contar con las aprobaciones de alto nivel que involucren los dueños de los procesos e identifiquen las causas e implicaciones de este tipo de acciones.

7.23. Establecer actividades de monitoreo y control en los diferentes aplicativos con la finalidad de asegurar el cargue y registro de la información que fortalezcan los atributos de calidad e integridad de los datos. También es importante efectuar un análisis detallado de las bases de datos con el fin de identificar las causas por las cuales se están presentando situaciones que afecten la integridad de la información y depurar datos que no estén acordes con las reglas de negocio y el procesamiento de los datos.

7.24. En relación con la actualización de los manuales de usuario de las aplicaciones que soporta el proceso de Gestión Tecnológica se recomienda la unificación de estos con los que se encuentran en el Sistema Integrado de Gestión – SIG.

7.25. Se recomienda la implementación de una bitácora o herramienta de consolidación que permita identificar las acciones de mejora a partir de las Lecciones Aprendidas y tenerlas en cuenta en los futuros proyectos, con el fin de proporcionar elementos de análisis para no reincidir en oportunidades de mejora o errores ya presentados.

7.26. Respecto al procedimiento de gestión de cambios el equipo auditor recomienda:

a. Implementar un mecanismo de control que permita identificar y soportar la ejecución del Comité Asesor del Cambio CAB, las aprobaciones de los asistentes y las decisiones tomadas.

b. Alinear la normatividad interna con la G.SIS.01 Guía del dominio de Sistemas de Información" del MINTIC versión 1.1 octubre de 2019, subnumeral "4.2.2 Formato de Cambios", en relación con los formatos, tipos de cambios e indicadores.

7.27. Se recomienda que se eleve una consulta a la Gerencia Legal, con el fin de identificar el procedimiento que se debe realizar para la actualización de los "Certificados de Registros de Soporte Lógico" de las aplicaciones ante la DNDA, donde se defina si se debe generar una actualización del certificado, teniendo en cuenta que el objetivo de este registro es la protección de derechos de autor, reconocimiento de derechos morales y patrimoniales de la entidad, por lo tanto, también se debe tener en cuenta que en caso de actualizarse el registro ante la DNDA se debe considerar una nueva valorización de los aplicativos con el fin reflejar los valores reales de los activos intangibles de la entidad.

7.28. Se recomienda analizar, diseñar e implementar un modelo de costos de recursos, que considere diferentes factores para la estimación de las horas de esfuerzo del recurso humano en los proyectos, mediante la continuidad en la implementación de las herramientas Celoxis y DevOps, que permitan la identificación de los esfuerzos reales del tiempo invertido en cada uno de los servicios prestados (desarrollo, mantenimiento o soporte), con el fin de establecer la variación entre lo planeado y lo ejecutado y la identificación correcta de los costos reales del servicio para calcular la rentabilidad de cada proyecto de la línea de servicio de Software Estado.

8. CONCLUSIÓN DE AUDITORÍA

Efectuada la auditoría Integral al Proceso de Gestión Tecnológica, se concluye que este cumple con las políticas administrativas establecidas por la entidad para el desarrollo de actividades que soportan los procesos de Planeación, Desarrollo y Mantenimiento de Software, Operaciones Tecnológicas y Seguridad de la Información, no obstante se identificaron desviaciones en el sistema de control interno que requieren suscribir acciones de mejora para fortalecer el ambiente de control, la estandarización de las prácticas y el seguimiento de las mismas, tal como se describe en los numerales 5 y 6 del presente informe, situaciones que podrían impactar en la ejecución de controles y monitoreo de la gestión y operación tecnológica.

Se resalta por parte del equipo auditor, la disponibilidad y cumplimiento oportuno en la entrega de la información requerida y el profesionalismo por parte de los funcionarios del proceso de Gestión Tecnológica y Oficial de Seguridad de la Información para atender todo lo relacionado con la etapa de ejecución de la Auditoria, mostrando receptividad y compromiso para la mejora continua de los procesos y reafirmar la cultura de Control.

9. MESA DE TRABAJO

En atención al "Procedimiento para Auditorías Internas de Gestión", una vez remitidos los informes preliminares de los cuatro (4) componentes por el Auditor Interno, se realizaron las siguientes mesas de trabajo entre el Director de T.I y su equipo de trabajo, Equipo Auditor Bellicorp SAS y el Equipo de Auditoría Interna, con el fin de consolidar el informe definitivo, los ajustes y observaciones allí presentados quedaron soportados en las diferentes actas de

las mesas de trabajo que hace parte de los papeles de trabajo de la auditoría interna y estarán disponibles para su consulta en caso de ser requeridos de la siguiente manera:

- Componente de Planeación y Administración de Tecnología de Información, el día 13 de abril de 2021.
- Componente de Seguridad de la Información y Ciberseguridad, el día 5 de mayo de 2021.
- Componente de Centro de Datos y Operaciones de Red, el día 14 de mayo de 2021.
- En relación con el informe preliminar del componente de Desarrollo de Software y Control de Cambios el Director de Tecnología por medio de correo electrónico el día 10 de junio de 2021 informó que no era posible agendar la mesa de trabajo, remitiendo mediante este medio los comentarios al informe, observaciones que fueron analizadas y respondidas por el equipo auditor de Bellicorp el día 15 de junio de 2021.

10. ANEXOS

Anexo 1. Plan de Mejoramiento auditoria de TI año 2017
Anexo 2. Plan de Mejoramiento de la CGR
Anexo 3. Informe definitivo Componente de Planeación y Administración de Tecnología de Información.
Anexo 4. Informe definitivo Componente de Centro de Datos y Operaciones de Red.
Anexo 5. Informe definitivo Componente de Desarrollo de Software y Gestión de Cambios.
Anexo 6. Informe definitivo Componente de Seguridad de la Información y Ciberseguridad.

Aprobado por:	Elaborado por:	Fecha de aprobación
ORIGINAL FIRMADO	ORIGINAL FIRMADO	
Elkin Orlando Angel Muñoz Auditor Interno	**Bellicorp S.A.S** Auditor Líder **Equipo Interno de Auditoria de CISA** Auditores de apoyo	25/06/2021