INFORME DE AUDITORIA

NOMBRE DEL PROCESO, ÁREA O TEMA A AUDITAR: Auditoría Integral de Gestión al Proceso de Infraestructura Tecnológica Componente Desarrollo de Software y Control de Cambios

INFORME PRELIMINAR: (12/05/2021) **INFORME DEFINITIVO**: (16/06/2021)

1. INTRODUCCIÓN.

La gestión del cambio y el desarrollo de software de la entidad, se encuentran orientados a atender los requerimientos de los clientes internos y externos con el fin de garantizar la competitividad, productividad y sostenibilidad, es por ello que se debe asegurar la funcionalidad de automatización de lo desarrollado de acuerdo con las especificaciones de diseño, los modelos de desarrollo y documentación, los requerimientos de calidad y estándares de aprobación.

La información utilizada para la auditoría fue aportada por el área de Gestión Tecnológica, así como la recolectada a través de las entrevistas y mesas de trabajo con las diferentes áreas de la Entidad, soportando los hallazgos, las observaciones y las recomendaciones generadas en el presente informe.

2. OBJETIVO DE LA AUDITORÍA

El objetivo general de la auditoría es evaluar el desarrollo de software y control de cambios para los sistemas de información durante las fases de requerimientos, desarrollo y pruebas para cumplir con las políticas, estándares, procedimientos y los requerimientos externos aplicables a la entidad.

Los objetivos específicos definidos para la evaluación de este componente son los siguientes:

a. Revisión y análisis de cada una de las etapas del ciclo de vida del desarrollo de software levantamiento de requerimientos, análisis y diseño, planificación y control, desarrollo, pruebas (validación, aseguramiento de calidad) instalación (implantación), mantenimiento y soporte.
b. Análisis de la metodología utilizada para la definición de tarifas.

c. Análisis de rentabilidad de las soluciones ofrecidas por la fábrica de software y los procedimientos de medición utilizados que establezcan un adecuado monitoreo, con el fin de garantizar la rentabilidad mínima requerida para la operación.
d. Revisión y evaluación de los costos de los desarrollos, mantenimientos y soporte para cada uno de los clientes externos, de acuerdo con los requerimientos personalizados, tipos de contratos y personal disponible para cada desarrollo. (metodologías de estimación de esfuerzos)
e. Análisis de las políticas y procedimientos tendientes a garantizar que los derechos de autor sobre las soluciones informáticas y del KNOW-HOW (Conocimiento técnico y práctico), se encuentren protegidos (propiedad intelectual) y a favor de CISA.
f. Revisión y evaluación del control de versionamiento de los aplicativos que se encuentra en producción internos y con clientes externos.
g. Verificación del control y actualización de manuales técnicos, de usuarios, de administración y guías de capacitación de las aplicaciones desarrollas por fábrica de software.
h. Revisión y evaluación de la actualización de la siguiente documentación: Diccionario de datos, modelo de entidad, relación de las diferentes aplicaciones que está en producción.
i. Realización de prueba(s) en la(s) Base(s) de Datos:
   - Verificación de la calidad, integridad y calidad de la información.
   - Verificación de duplicados dentro de la base de datos.
   - Verificación de campos nulos o vacíos, validación de campos.
   - Evaluación del control de cambios sobre los datos (en las Base de Datos)
j. Revisión y verificación de las interfaces entre los aplicativos de la entidad.

3. ALCANCE

Se realizó Auditoría Interna al proceso de Desarrollo Software y Cambios de Programas, 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 de auditoria para entidades públicas versión 4, Estatuto

de Auditoria Interna, séptima dimensión y tercera línea de defensa del Modelo Integrado de Planeación y Gestión – MIPG, la auditoría se realizó del 23 de febrero al 5 de mayo de 2021.

4. DESARROLLO DE LA AUDITORÍA

4.1. EVALUACIÓN DE AUDITORIAS ANTERIORES

4.1.1. Auditorias Anteriores, La Gerencia de Tecnología es responsable de veinticuatro (24) acciones de mejora propuestas en el Plan de Mejoramiento suscrito para la Auditoria realizada al proceso en la vigencia 2017", seis (6) de las cuales se encuentran relacionadas con el proceso de Desarrollo y Cambios a programas. Las siguientes son las acciones del Plan relacionadas con este componente:

HALLAZGO	DESCRIPCION DE HALLAZGO	ACCION DE MEJORA	ACTIVIDADES / DESCRIPCIÓN	ACTIVIDADES / UNIDAD DE MEDIDA
5.2.1 Control de cambios en aplicación	En algunos casos identificados, la entidad aceleró las entregas de producto obligando a la fábrica a liberar los cambios en los sistemas sin el respectivo protocolo de pruebas integrales y aseguramiento QA	Integrar al flujo de desarrollo la actividad de aseguramiento del producto y hacer obligatorio el plan de pruebas para validación y aceptación de los roles integrantes del CAB (Comité de Cambios)	Inclusión del paso QA en flujo de aprobación del Cambio	Actualización a flujo de Desarrollo Zeus
5.2.2 Control de cambios directos en base de datos	No hace parte del flujo Zeus el aval del Oficial de Seguridad ni la aceptación post implementación del negocio	Integrar al flujo del cambio la aceptación del negocio una vez se implemente el mismo por tecnología.	Inclusión del paso de verificación del negocio post implementación para el cierre del Cambio	Actualización a flujo de "solicitud adición o modificación información base de datos" Zeus

HALLAZGO	DESCRIPCION DE HALLAZGO	ACCION DE MEJORA	ACTIVIDADES / DESCRIPCIÓN	ACTIVIDADES / UNIDAD DE MEDIDA
6.5.1 Diseño de los procedimientos de gestión de cambios	No se deja evidencia física de la celebración del CAB (Comité de Cambios) dado que la traza de aprobación previa, del CAB y conclusiones del mismo se registra en el flujo Zeus. Respecto a la actualización de la tipificación del CAB (crítico o programado) la CN 093 ya se encuentra actualizada, así como la solicitud de evidencia de ejecución de los casos de prueba antes de que el cambio sea considerado por el CAB para aprobación	Formato Evidencia física del CAB X 3 meses (4 CAB x mes)	Formato Evidencia física del CAB X 3 meses (4 CAB x mes)	Formato diligenciado
6.5.2 Fábrica de Software	No se cuenta con una herramienta que permita gestión por minutograma de las actividades de la fábrica, el control establecido parte del tiempo dimensionado para el desarrollo aprobado por Arquitectura y Desarrollador(es) y fecha final de entrega del producto para paso a Calidad.	Adquirir o rentar una herramienta tecnológica que permita el control por minutograma de las actividades propias de la construcción de código fuente en la fábrica de software.	Software de control por Minutograma contratado	Contrato de servicios

HALLAZGO	DESCRIPCION DE HALLAZGO	ACCION DE MEJORA	ACTIVIDADES / DESCRIPCIÓN	ACTIVIDADES / UNIDAD DE MEDIDA
	Al interior de la fábrica existe de manera parcial documentación sobre las líneas de producto entregadas como servicio a terceros	Crear y almacenar en el ServerFile CISA los documentos técnicos y funcionales de las líneas de software comercializadas con la última versión funcional liberada para los clientes.	Documentos técnicos y funcionales actualizados para los sistemas COBRA, TEMIS, OLYMPUS	Documentos creados en el ServerFile
	La información de arquitectura de aplicación y estructura de base de datos de los sistemas CISA no está actualizada con las últimas transformaciones de las líneas base.	Actualizar los documentos que soportan el diseño y arquitectura de aplicación de los diferentes sistemas de información	Arquitectura de Aplicación documentada para COBRA, TEMIS y OLYMPUS	Documentos creados o actualizados
6.5.3 Aplicación de la metodología SCRUM para el área de desarrollo	No se ha documentado la nueva práctica de construcción de software que toma como base la metodología SCRUM	Posterior a la finalización del plan remedial de TI, actualizar la CN093 con la nueva práctica de construcción de software.	Procedimiento de Ciclo de Vida de Software actualizado	Circular 093 actualizada
6.6.2 Cargue de pagos de usuarios en Cobra	Archivo de cargue de pagos sin cifrado	Asegurar el procedimiento de descarga, custodia, actualización y carga del archivo de pagos proveniente de entidad bancaria y con destino COBRA	Establecer el control de protección al archivo liberado por la entidad bancaria y con destino COBRA	Control establecido

Con el fin de determinar la efectividad de las acciones suscritas en el plan de mejoramiento y soportar el cierre de las mismas, el equipo auditor observó:

OBSERVACIÓN 5.2.1 Control de Cambios en la aplicación: Se evidencia 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", a continuación, se muestran los estados para el flujo "Soporte de Aplicativos Institucionales":

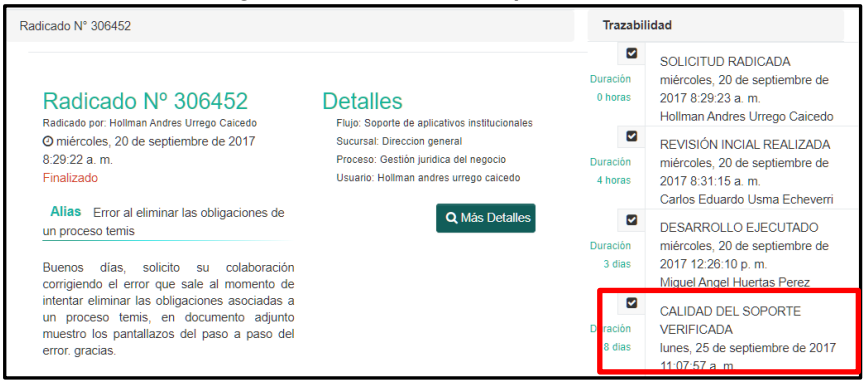
Imagen 1: Estados del flujo

No.	ESTADOS FLUJO DE SOPORTE APLICATIVOS TERCEROS
1	RADICADO
2	PENDIENTE VALIDACIÓN GERENCIA DE TECNOLOGIA Y SISTEMAS DE INFORMACIÓN
3	PENDIENTE EJECUTAR SOPORTE CONFORME A LA SOLICITUD
4	PENDIENTE REALIZAR PRUEBAS DE CALIDAD Y/O APOYO
5	PENDIENTE PASO A PRUEBAS
6	PENDIENTE DESPLIEGUE AMBIENTE PREPRODUCCIÓN
7	PENDIENTE REALIZAR PRUEBAS CLIENTE - AMBIENTE DE PREPRODUCCIÓN
8	PENDIENTE PASO A PRODUCCION
9	PENDIENTE ACEPTACIÓN USUARIO EXTERNO

Fuente: Información TI –Estados del Flujo – Aplicación Zeus –23 de marzo de 2021

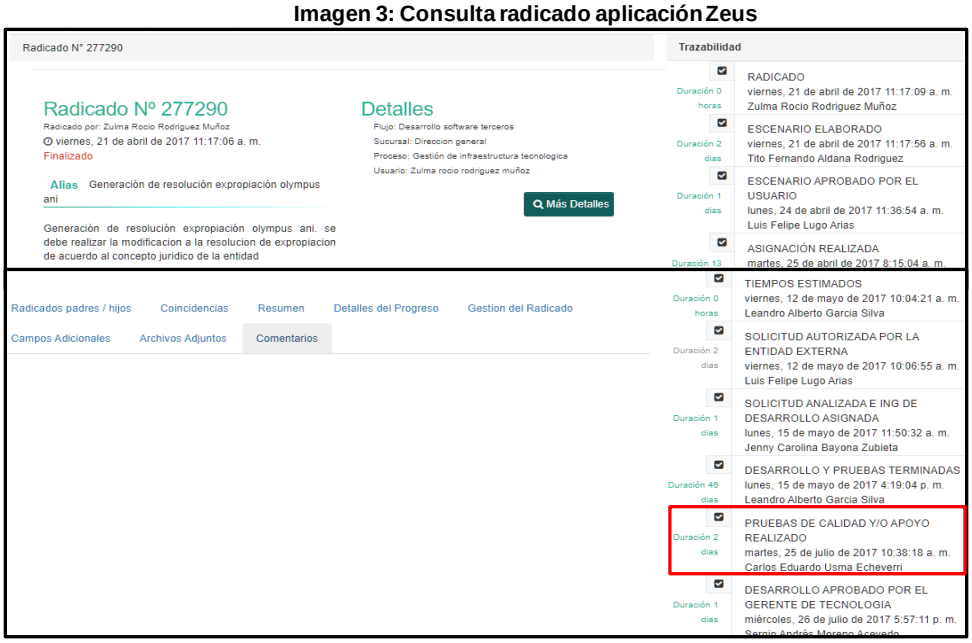
De acuerdo al análisis se concluye el cierre de la observación con la revisión de los estados para los flujos de "Soportes de aplicativos institucionales", "Gestión requisitos de software" y "Desarrollo software terceros", donde se incluyó el estado "Pendiente realizar pruebas de calidad y/o apoyo", como se muestra en la siguiente imagen:

Imagen 2: Consulta radicado aplicación Zeus



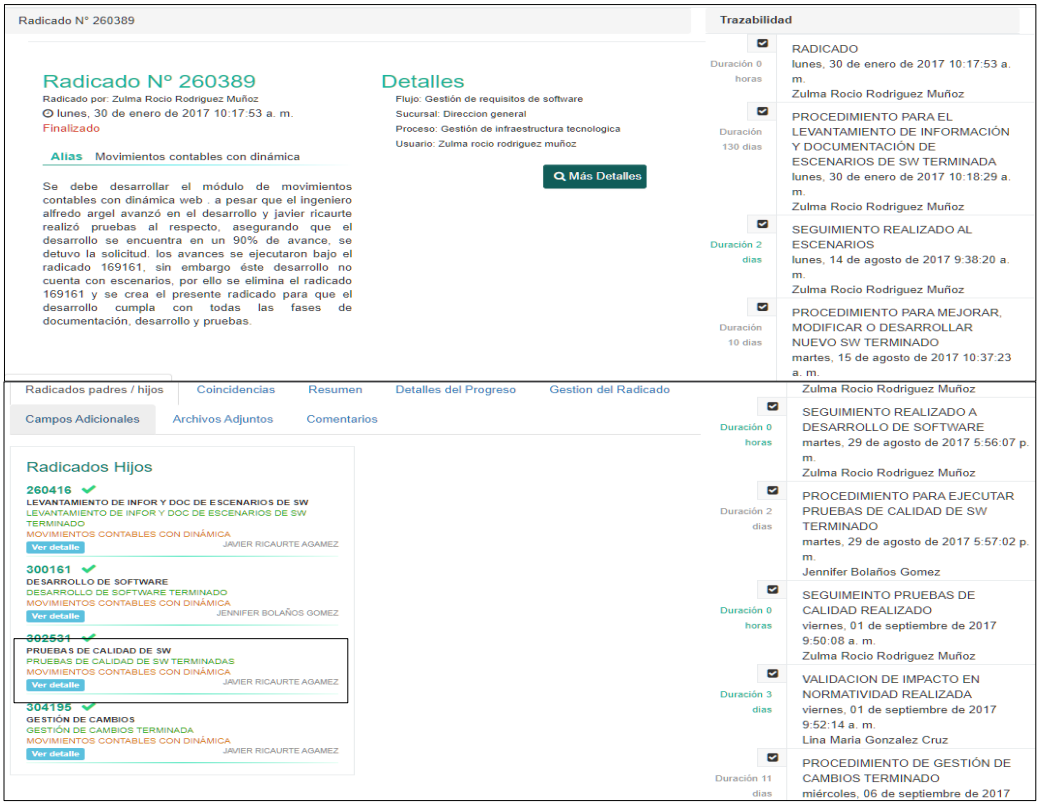
Fuente: \serverfile\Presidencia\AUDITORIA_INTERNA\2017\AuditoriadeTecnología –29 de enero de 2021

Imagen 3: Consulta radicado aplicación Zeus



Fuente: \serverfile\Presidencia\AUDITORIA_INTERNA\2017\AuditoriadeTecnología –29 de enero de 2021

Imagen 4: Consulta radicado aplicación Zeus



Fuente: \serverfile\Presidencia\AUDITORIA_INTERNA\2017\AuditoriadeTecnología –29 de enero de 2021

De acuerdo a la revisión realizada por el equipo auditor y a las pruebas que soportan el cumplimiento de esta acción de mejora, se concluye una vez analizada su eficacia, que se puede cerrar el presente hallazgo; 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 del hallazgo, puesto que al consultar los estados del flujo "Soporte aplicativos a Terceros" encontramos que se encuentra definido el estado "Pendiente realizar pruebas de calidad y/o apoyo", como vemos a continuación en la imagen 5:

Imagen 5: Estados de Flujo

No.	ESTADOS FLUJO DE SOPORTE APLICATIVOS TERCEROS
1	RADICADO
2	PENDIENTE VALIDACIÓN GERENCIA DE TECNOLOGIA Y SISTEMAS DE INFORMACIÓN
3	PENDIENTE EJECUTAR SOPORTE CONFORME A LA SOLICITUD
4	PENDIENTE REALIZAR PRUEBAS DE CALIDAD Y/O APOYO
5	PENDIENTE PASO A PRUEBAS
6	PENDIENTE DESPLIEGUE AMBIENTE PREPRODUCCIÓN
7	PENDIENTE REALIZAR PRUEBAS CLIENTE - AMBIENTE DE PREPRODUCCIÓN
8	PENDIENTE PASO A PRODUCCION
9	PENDIENTE ACEPTACIÓN USUARIO EXTERNO

Fuente: Información TI – Estados Flujo – Aplicación Zeus –23 de marzo de 2021

OBSERVACIÓN 5.2.2 Control de Cambios directos en la base de datos: De acuerdo a la revisión a los flujos de los procesos de Tecnología en donde se evidencia que para el flujo "Solicitud modificación o adición información en BD" se incluyó el estado "Pendiente Revisión Oficial de Seguridad de la información", como se detalla en el siguiente cuadro, por lo tanto, se cierra la observación; sin embargo, en el análisis a las solicitudes efectuadas utilizando este flujo en el subnumeral 4.4.1. de este informe 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 identificación de un hallazgo.

Imagen 6: Estados de Flujo

No.	ESTADOS FLUJO SOLICITUD MODIFICACIÓN O ADICIÓN INFORMACIÓN EN BD
1	RADICADO
2	PENDIETE VALIDACION LIDER DEL APLICATIVO
3	PENDIENTE VALIDAR POR EL GERENTE DEL AREA
4	PENDIENTE REVISIÓN ANALISTA CONTABLE
5	**PENDIENTE APROBACION CONTABLE**
6	PENDIENTE APROBACIÓN DIRECTOR DE TECNOLOGIA
7	PENDIENTE REVISIÓN JEFE OPERACIONES TECNOLÓGICAS
8	**PENDIENTE VALIDACIÓN OFICIAL DE SEGURIDAD DE LA INFORMACIÓN**
9	PENDIENTE EJECUCION EN PRODUCCION
10	PENDIENTE VALIDAR SOLICITUD

Fuente: Información TI - Estados Flujo – Aplicación Zeus –23 de marzo de 2021

OBSERVACIÓN 6.5.1 Diseño de los procedimientos de gestión de cambios: El equipo auditor revisó únicamente 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", ver imagen 7:

Imagen 7: Estados Flujo

No.	ESTADOS FLUJO GESTIÓN DE CAMBIOS
1	RADICADO
2	PENDIENTE REVISIÓN ARQUITECTURA DE SOFTWARE
3	PENDIENTE REVISIÓN OFICIAL DE SEGURIDAD DE LA INFORMACIÓN
4	PENDIENTE REVISIÓN JEFATURA DE MEJORAMIENTO CONTINUO
5	PENDIENTE REVISIÓN GERENCIA DE TI
6	**PENDIENTE REVISAR CRITERIOS DE OPERACIONES TECNOLÓGICAS Y PROGRAMAR REUNIÓN CAB**
7	PENDIENTE PROGRAMAR REUNIÓN DE CAMBIOS CRÍTICOS
8	PENDIENTE HABILITAR SUPERUSUARIO
9	PENDIENTE AJUSTAR RFC NO SE ESTA REALIZANDO
10	PENDIENTE IMPLEMENTAR EL CAMBIO
11	PENDIENTE DESHACER EL CAMBIO Y DETERMINAR CAUSA DE ERROR
12	PENDIENTE CONFIRMAR LA PUESTA EN PRODUCCIÓN

Fuente: Información TI – Estados Flujo – Aplicación Zeus –23 de marzo de 2021

Al realizar una revisión en una muestra de 30 solicitudes como se desarrolló en el subnumeral "4.4.1. Ciclo de vida de desarrollo de software" se observa que no se cuenta con dicha evidencia ni digital ni física, por lo tanto, esta observación se mantiene abierta.

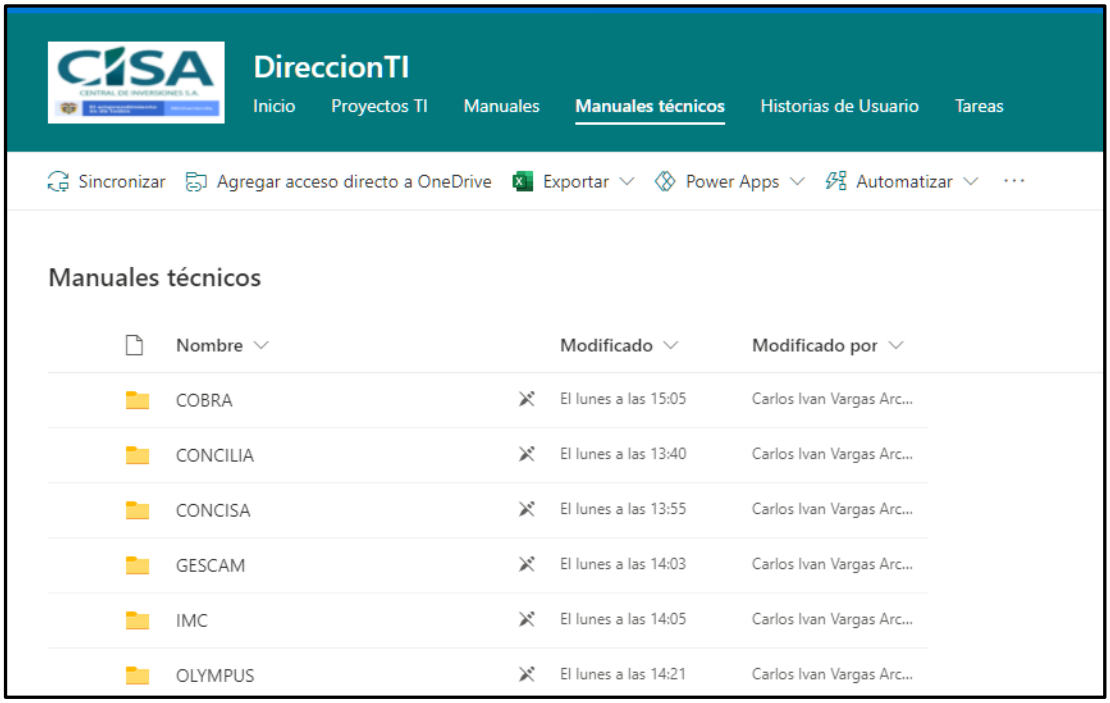
OBSERVACIÓN 6.5.2 Fábrica de Software: La Dirección de Tecnología realizó la adquisición de dos herramientas para realizar la gestión de las actividades de la fábrica de software, llamadas Celoxis y DevOps desde agosto de 2020, las cuales se encuentran en implementación, por esta razón al momento de 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 observación se

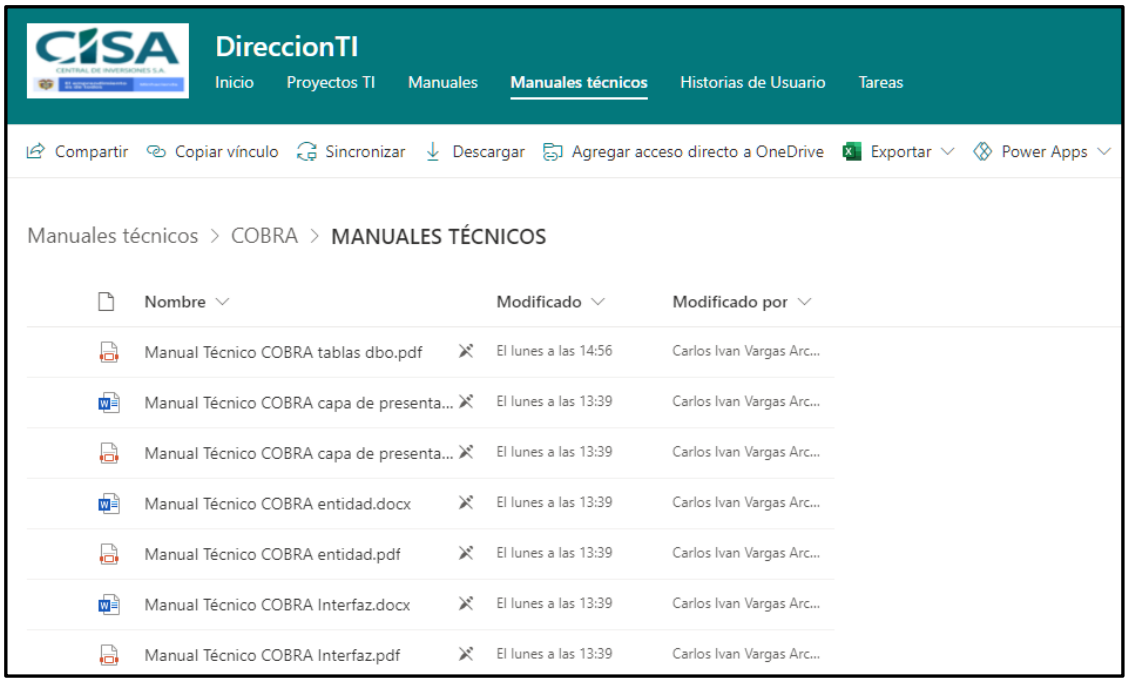
mantiene abierta de acuerdo a los desarrollado en el subnumeral “4.4.6. Identificación de costos de la fábrica de software”.

En cuanto a los manuales de usuario de los aplicativos COBRA, TEMIS y OLYMPUS éstos se encuentran desactualizados en el SIG respecto a los que se encuentran en el SharePoint de la Dirección de Tecnología, por lo tanto, esta observación sobre esta acción sigue abierta.

Respecto a los manuales técnicos estos se encuentran actualizados y almacenados en el repositorio del SharePoint de la Dirección de Tecnología https://centraldeinversionessa.sharepoint.com/sites/DireccionTI/Proyectos%20TI/Forms/AllItems.aspx, para la consulta del personal de la fábrica de software como se muestra a continuación, por esta razón esta acción se cierra:

Imagen 8: Manuales Técnicos





Fuente: SharePoint – Consulta Manuales Técnicos – 4 de mayo de 2021

OBSERVACIÓN 6.5.3 Aplicación de la metodología SCRUM para el área de desarrollo: Se cierra la observación al revisar la actualización de la Circular Normativa 093 "Política y procedimiento de gestión tecnológica" versión 62 de 30 de diciembre de 2020 subnumeral "5.9. Políticas de desarrollo" y Circular Normativa 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.

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 observa que la Gerencia de Tecnología es responsable de 6 acciones de mejora propuestas en el "Plan de Mejoramiento CGR - TI", las cuales se encuentran relacionados con la actualización

de los manuales: técnicos, de usuario y código fuente, como se muestra en el siguiente cuadro:

HALLAZGO	DESCRIPCION DE HALLAZGO	ACCION DE MEJORA	ACTIVIDADES / DESCRIPCIÓN	ACTIVIDADES / UNIDAD DE MEDIDA
H15Feb14	Aplicativos En los aplicativos desarrollados por CISA, conforme con lo establecido en la Circular 093, se debe incluir además del código fuente del aplicativo, la documentación correspondiente al manual técnico y al manual de usuario. Sin embargo, se observa que para los aplicativos COBRA, GESCAM, CONCISA, NUEVOSIGEP no se cuenta con la mencionada documentación (H15-feb14)	Elaboración y/o actualización de manuales técnicos y de usuario para los aplicativos CONCISA, SIGEP, GESCAM, TEMIS, COBRA, OLYMPUS, SIGA, ZEUS	Elaborar manuales técnicos y de usuario para la aplicación COBRA	Manuales Documentados
			Elaborar manuales técnicos y de usuario para las aplicaciones SIGEP y GESCAM	Manuales Documentados
			Elaborar manuales técnicos y de usuario para las aplicaciones ZEUS y SIGA	Manuales Documentados
			Elaborar manual técnico y de usuario para la aplicación OLYMPUS	Manuales Documentados
			Actualizar los manuales técnicos y de usuario para las aplicaciones	Manuales Documentados

HALLAZGO	DESCRIPCION DE HALLAZGO	ACCION DE MEJORA	ACTIVIDADES / DESCRIPCIÓN	ACTIVIDADES / UNIDAD DE MEDIDA
			CONCISA, TEMIS e IMC	
			Actualizar el repositorio documental con los manuales actualizados y divulgar a los usuarios de CISA y Terceros las nuevas versiones para su uso.	Registro de divulgación de manuales de usuarios actualizados a líderes de aplicación y usuarios de los sistemas

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, se adjunta un ejemplo para el manual de la aplicación Olympus – Manual de Convenios:

Imagen 9: Banco de Documentos

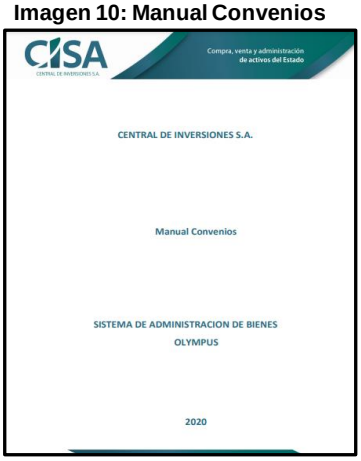
Documentos Encontrados

Total de Registros **34** - Pagina **1** de **2** - Mostrando 30 registros, del **1** al **30**

Consultar	Nombre	Titulo	Fecha_Actualizac
Consultar	Circular Normativa 097 de 2021	Manual de Judicialización	15/04/2021
Consultar	Manual 012 de 2021	Políticas y Procedimientos de Planeación Estratégica	14/04/2021
Consultar	Manual 022 de 2021	Manual de Continuidad del Negocio	25/03/2021
Consultar	Manual 021 de 2021	Reglamento Interno de Cobro de Cartera Coactiva	23/03/2021
Consultar	Manual 018 de 2021	Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST)	16/03/2021
Consultar	Circular Normativa 055 de 2021	Manual de Presupuesto	04/01/2021
Consultar	Circular Normativa 044 de 2020	Manual de Contratación	30/12/2020
Consultar	Circular Normativa 110 de 2020	Manual de Políticas de Provisiones por Contingencias Judiciales	30/12/2020
Consultar	Manual 011 de 2020	Código de Buen Gobierno	30/12/2020
Consultar	Manuales de Usuario Aplicativos 001 de 2020	Manual de Usuario Aplicativo Temis	30/12/2020
Consultar	Manuales de Usuario Aplicativos 002 de 2020	Manual de Usuario Aplicativo SIGA WEB	30/12/2020
Consultar	Manuales de Usuario Aplicativos 003 de 2020	Manual de Usuario Aplicativo ZEUS WEB	30/12/2020
Consultar	Manuales de Usuario Aplicativos 004 de 2020	Manual de Usuario aplicativo GESCAM	30/12/2020
Consultar	Manuales de Usuario Aplicativos 005 de 2020	Manual de Usuario Aplicativo SIGEP – Ejecución Presupuestal	30/12/2020
Consultar	Manuales de Usuario Aplicativos 006 de 2020	Manual de Usuario Aplicativo SIGEP – Parámetros	30/12/2020
Consultar	Manuales de Usuario Aplicativos 007 de 2020	Manual de Usuario Aplicativo SIGEP – Reportes y opciones	30/12/2020
Consultar	Manuales de Usuario Aplicativos 008 de 2020	Manual de Usuario Aplicativo CONCISA	30/12/2020
Consultar	Manuales de Usuario Aplicativos 009 de 2020	Manual de Usuario Aplicativo OLYMPUS – Consultas y reportes	30/12/2020
Consultar	Manuales de Usuario Aplicativos 010 de 2020	Manual de Usuario Aplicativo OLYMPUS – Contratación	30/12/2020
Consultar	Manuales de Usuario Aplicativos 011 de 2020	Manual de Usuario Aplicativo OLYMPUS – Convenios	30/12/2020
Consultar	Manuales de Usuario Aplicativos 012 de 2020	Manual de Usuario Aplicativo OLYMPUS – Pagos y reembolsos	30/12/2020

Fuente: Banco de Documentos – Sistema Integrado de Gestión –23 de marzo de 2021

Imagen 10: Manual Convenios


CENTRAL DE INVERSIONES S.A.

Manual Convenios

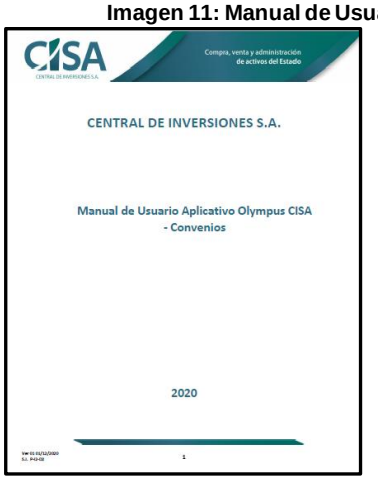
SISTEMA DE ADMINISTRACION DE BIENES
OLYMPUS

2020

Versión	Fecha	Cambio	Elaborado Por	Aprobación		
				Nombre y Cargo	Fecha	Firma
1.0	15/10/2019	Creación de Documento	Adriana Gómez	Sergio Moreno Acevedo	15/10/2019	
2.0	30/12/2020	Se modificó teniendo en cuenta la actualización de la nueva imagen corporativa.	Nicolás Bonilla	Deibis Jacob Jiménez Salcedo	30/12/2020	

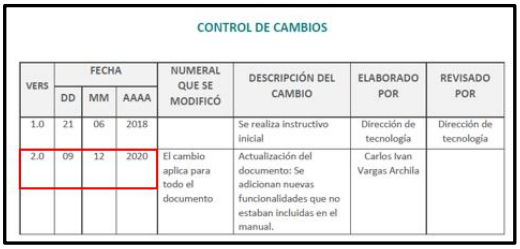
Fuente: Consulta Banco de Documentos –23 de marzo de 2021

Imagen 11: Manual de Usuarios Aplicativo Olympus CISA


CENTRAL DE INVERSIONES S.A.

Manual de Usuario Aplicativo Olympus CISA
- Convenios

2020


CONTROL DE CAMBIOS

VERS	FECHA			NUMERAL QUE SE MODIFICÓ	DESCRIPCIÓN DEL CAMBIO	ELABORADO POR	REVISADO POR
	DD	MM	AAAA				
1.0	21	06	2018		Se realiza instructivo inicial	Dirección de tecnología	Dirección de tecnología
2.0	09	12	2020	El cambio aplica para todo el documento	Actualización del documento: Se adicionan nuevas funcionalidades que no estaban incluidas en el manual.	Carlos Ivan Vargas Archila	

Fuente: Share Point Dirección TI –23 de marzo de 2021

En el ejemplo 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.

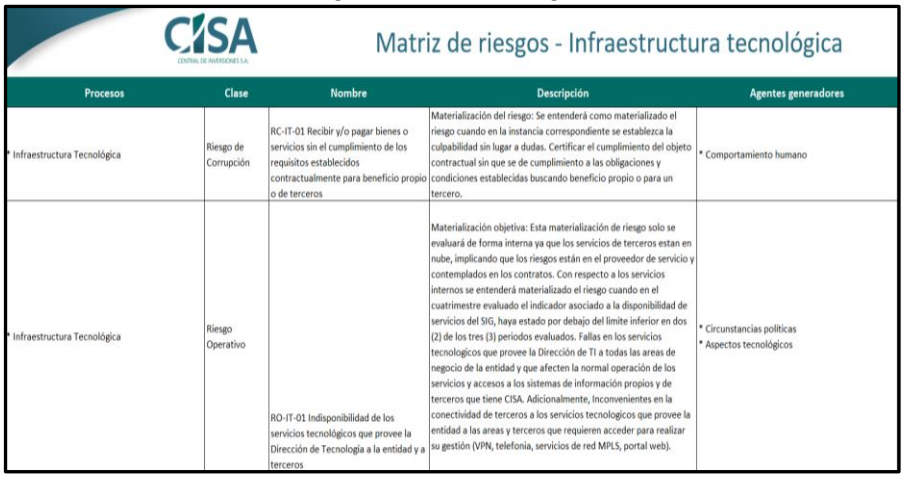
Realizada la verificación al plan de mejoramiento suscrito entre CISA y la Contraloría General de la República aplicable a la vigencia 2020, se observa que no se ha dado cumplimiento a la acción de mejora con respecto a la actualización de los manuales de usuario, la actualización del repositorio documental y la divulgación de la nueva versión a los usuarios de CISA y a Terceros.

4.2. EVALUACIÓN DE RIESGOS

CISA cuenta con la CN107 "*Política de Administración de Riesgos en Central de Inversiones S.A*" Versión 22 del 18 de diciembre de 2020, en la cual se definen los riesgos estratégicos, operativos, de corrupción, de seguridad digital y continuidad del negocio.

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. Al revisar el "Mapa de Riesgos – Infraestructura Tecnológica" se observa que se tienen definidos los riesgos de: Corrupción y Operativo, tal como se muestra en la siguiente imagen:

Imagen 12: Matriz de riesgos



CISA — 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 politicas * Aspectos tecnológicos

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

Se evidencia que respecto al subnumeral 4.3.2 “Valoración y Tratamiento de los riesgos” contenido en el numeral 4.3 “Evaluación de Riesgos”, falta la definición de eventos de riesgos de acuerdo a la caracterización del subproceso de “Construcción de software”; 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, evidenciado en el correo electrónico generado por el Director de Tecnología el 15 de abril del 2021 y los anexos, entre los que se encuentran la siguiente comunicación entre la analista de riesgos del área de la Jefatura de Procesos y Productividad y el área de Gestión Tecnológica:

Imagen 13: Correo análisis de riesgos

Laura Alejandra Lopez
RE: RIESGOS PROCESO DE DESARROLLO DE SOFTWARE

Hola Zulma, buenas tardes:

Preliminarmente mis comentarios y ajustes en azul.

Saludos cordiales,

CISA — Laura Alejandra López
Analista de Riesgos

De: Zulma Rocio Rodriguez Muñoz
Enviado el: miércoles, 7 de abril de 2021 6:50 p. m.
Para: Laura Alejandra Lopez
Asunto: RV: RIESGOS PROCESO DE DESARROLLO DE SOFTWARE

Laura,

Te comparto versión **preliminar** de las fichas, para tu VoBo previo a la revisión final por parte del equipo de tecnología.

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

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.

4.3. EVALUACIÓN DE INDICADORES

El proceso de Gestión Tecnológica es responsable de la medición y reporte de indicadores en el Plan Estratégico de CISA y en la herramienta ISOLUCION para la gestión del SIG como soporte de sus actividades, los cuales presentan el siguiente comportamiento:

4.3.1. Indicador Atención de las solicitudes de soporte de aplicativos institucionales y de terceros: Para la vigencia enero – diciembre 2020, la Gerencia de Tecnología realizó la medición y reporte con el siguiente resultado:

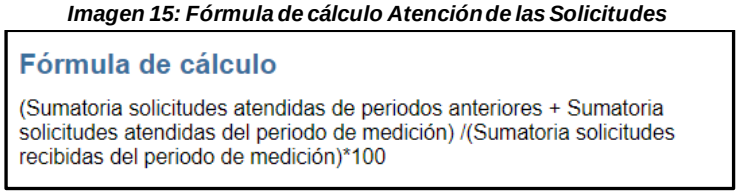
Imagen 14: Indicador Atención de las Solicitudes

Fuente: Aplicación Isolucion –11 de marzo de 2021

De acuerdo con el informe revisado en Isolucion se evidencia que el indicador cumplió la meta del 90% de las solicitudes de soporte de aplicativos institucionales y de terceros solo en el mes de julio no se cumple la meta con un 67% de medición, esto debido a la priorización de la implementación del proyecto Procesamiento de Cartera y el de subasta electrónica.

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.

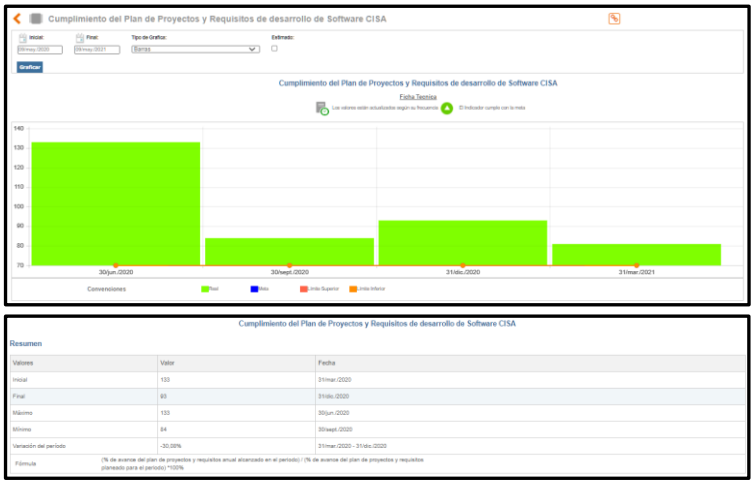
Imagen 15: Fórmula de cálculo Atención de las Solicitudes



Fuente: Aplicación Isolucion –11 de marzo de 2021

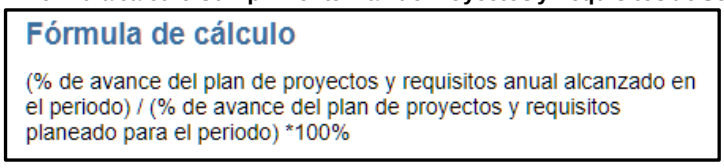
4.3.2. Cumplimiento del Plan de Proyectos y Requisitos de desarrollo de Software CISA: Para la vigencia enero – diciembre 2020, la Gerencia de Tecnología realizó la medición y reporte con el siguiente resultado:

Imagen 16: Indicador Cumplimiento Plan de Proyectos y Requisitos de Software



Fuente: Aplicación Isolucion –11 de marzo de 2021

Imagen 17: Fórmula cálculo Cumplimiento Plan de Proyectos y Requisitos de Software



Fuente: Aplicación Isolucion –11 de marzo de 2021

Se observa 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 temas 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.

4.4. DESARROLLO DE SOFTWARE Y CONTROL DE CAMBIOS

4.4.1. Ciclo de Vida de Desarrollo del Software

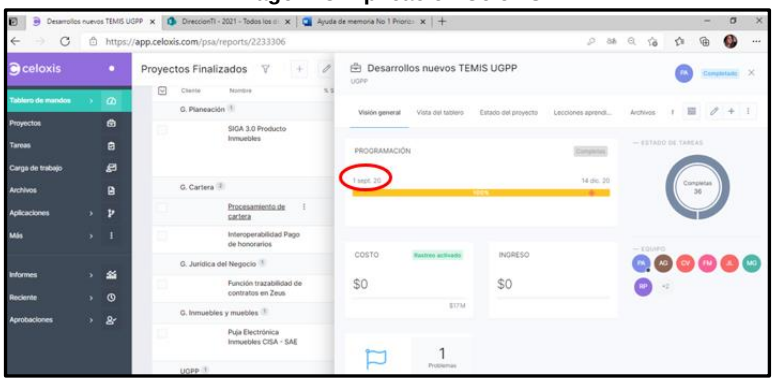
La Dirección de Tecnología de CISA, tiene definido en la Circular Normativa N°127 "*Políticas y Procedimientos para la Gestión de Proyectos de Tecnología"* Versión 16 del 1 de diciembre de 2020, los lineamientos que se aplican en el desarrollo de software, el cual involucra elementos de metodologías 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.

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 https://centraldeinversionessa.sharepoint.com/sites/DireccionTI/Proyectos%20TI/Forms/AllItems.aspx. Se muestra a continuación el recorrido de esta fase:

Imagen 18: Aplicación Celoxis



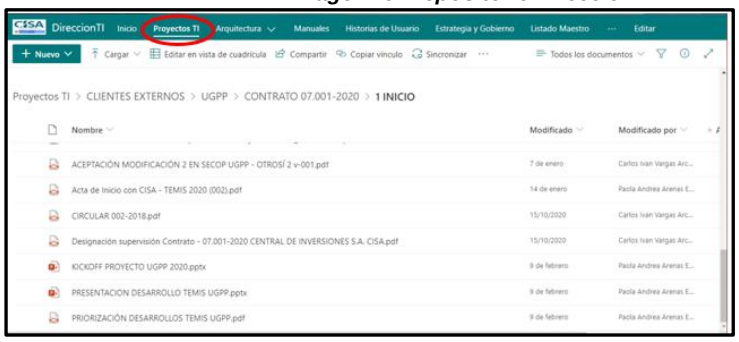
Fuente: Registro Proyecto – Reunión 11 de marzo de 2021

Imagen 19: Salidas de la fase de inicio

SALIDAS DE LA FASE DE INICIO			
	REGISTRO	METODOLOGÍA ÁGIL INTEGRADA	
		PROYECTO INTERNO	PROYECTO EXTERNO
1	Presentación necesidad de proyecto ante el comité de arquitectura.	R	R
2	Viabilidad proyecto Comité de arquitectura	R	NA
3	Matriz de priorización de proyectos o acta de priorización con cliente.	R	OP
4	Contrato (Si aplica)	NA	R
5	Oferta comercial	NA	R
6	Nombrar al Scrum Owner o Gerente del proyecto	R	R
7	Presentación de inicio del proyecto (Kick Off) - Acta de inicio	R	R
8	Registro del proyecto en el portafolio de proyectos correspondiente y repositorio SharePoint del proyecto creado	R	R
R= Requerido NA= No Aplica			

Fuente: Fase de Inicio – Circular 127 – Reunión 11 de marzo de 2021

Imagen 20: Repositorio Dirección TI



Fuente: Repositorio Documental – Sharepoint – Reunión 11 de marzo de 2021

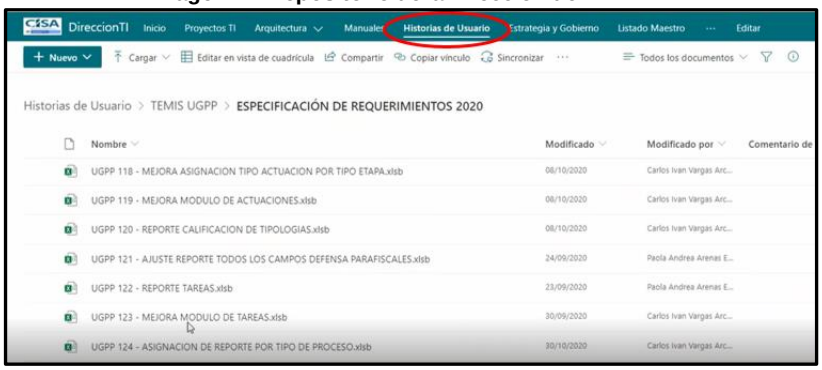
b. Fase Planificación Proyectos: En donde se puede encontrar toda la planeación y especificación de los requerimientos como son arquitectura, historia de usuarios, escenarios, prototipos, criterios de aceptación, estimación de los esfuerzos, Sprint Backlog – Sprint Goal o cronograma y matriz de riesgos:

Imagen 21: Salidas de la fase de Planificación

SALIDAS DE LA FASE DE PLANIFICACIÓN			
	REGISTRO	METODOLOGÍA ÁGIL INTEGRADA	
		PROYECTO INTERNO	PROYECTO EXTERNO
1	Plan del proyecto y Backlog priorizado del producto/ proyecto -	R	R
2	**Planificación de Arquitectura del Proyecto**	R	R
3	Especificaciones de requerimientos: Historias de usuario, escenarios, prototipos, criterios de aceptación.	R	R
4	Listado Maestro de Escenarios por producto	R	R
5	Estimaciones de esfuerzo: tfs, sprint, o documento formal cliente externo.	R	R
6	Planificación de los Sprint del proyecto - Sprint Backlog – Sprint Goal - o cronograma.	R	R
8	Matriz de riesgos por tipo de proyecto de TI	R	R
R= Requerido NA= No Aplica OP=Opcional			

Fuente: Fase Planificación Proyectos – CN 127 – Reunión 11 de marzo de 2021

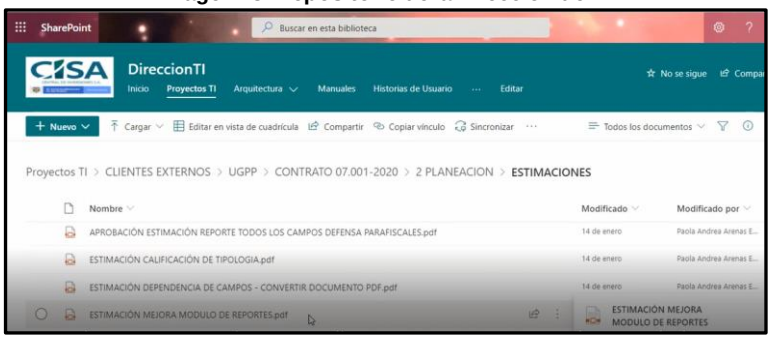
Imagen 22: Repositorio de la Dirección de TI



Fuente: Repositorio Documental – Historia de Usuarios – Reunión 11 de marzo de 2021

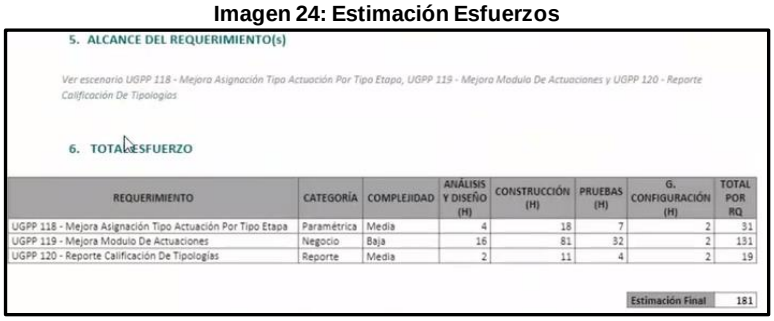
Como se muestra en la imagen 22, CISA define las historias de usuario, el Backlog y las estimaciones para cada requerimiento, en el caso de los terceros las estimaciones se realizan formalmente a través de correo electrónico y se deja constancia en el Sharepoint, en el documento "Estimación de requerimientos", donde se especifica el alcance y los acuerdos del total de esfuerzos entregados al cliente para la aprobación del uso de horas, tal como se muestra en las siguientes imágenes:

Imagen 23: Repositorio de la Dirección de TI



Fuente: Repositorio Documental – Estimaciones – Reunión 11 de marzo de 2021

Imagen 24: Estimación Esfuerzos



5. ALCANCE DEL REQUERIMIENTO(s)

Ver escenario UGPP 118 - Mejora Asignación Tipo Actuación Por Tipo Etapa, UGPP 119 - Mejora Modulo De Actuaciones y UGPP 120 - Reporte Calificación De Tipologías

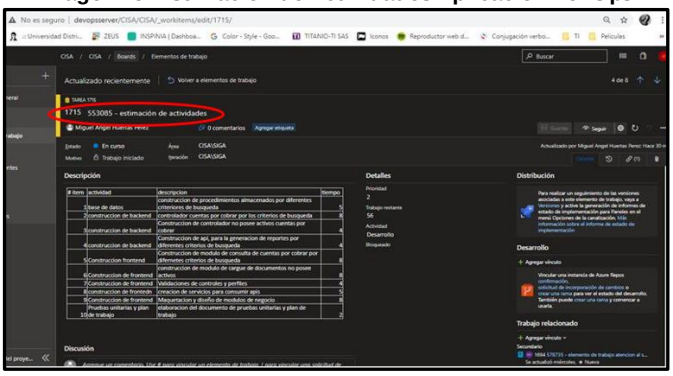
6. TOTAL ESFUERZO

REQUERIMIENTO	CATEGORÍA	COMPLEJIDAD	ANÁLISIS Y DISEÑO (H)	CONSTRUCCIÓN (H)	PRUEBAS (H)	G. CONFIGURACIÓN (H)	TOTAL POR RQ
UGPP 118 - Mejora Asignación Tipo Actuación Por Tipo Etapa	Paramétrica	Media	4	18	7	2	31
UGPP 119 - Mejora Modulo De Actuaciones	Negocio	Baja	16	81	32	2	131
UGPP 120 - Reporte Calificación De Tipologías	Reporte	Media	2	11	4	2	19
						Estimación Final	181

Fuente: Documento Proyectos de TI – Estimación de Requerimientos – Reunión 11 de marzo de 2021

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 CN127, 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.

Imagen 25: Estimación de Actividades Aplicación DevOps



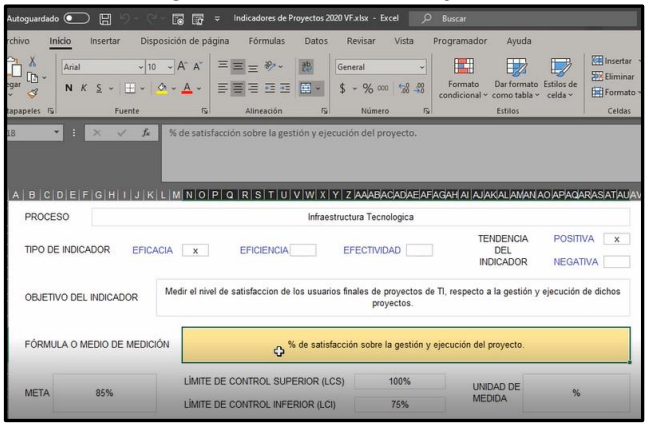
Fuente: Aplicación Devops – Reunión 11 de marzo de 2021

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:

a) Porcentaje de cumplimiento del cronograma (desviación).
b) Porcentaje de ejecución presupuestal.
c) 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”.

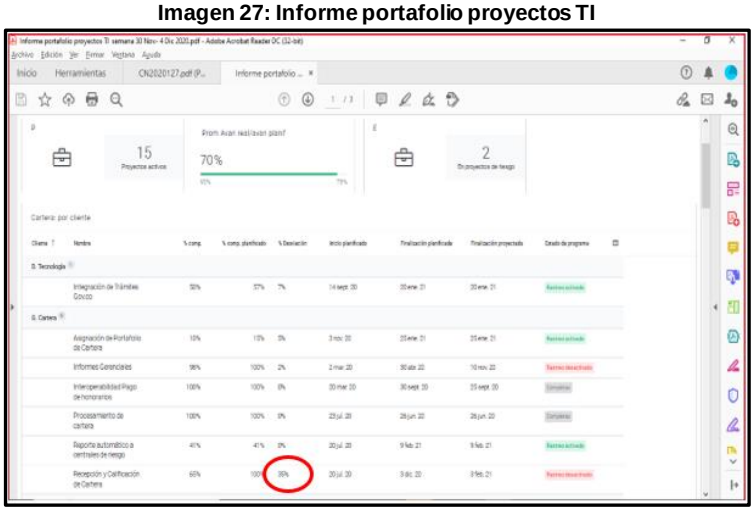
Imagen 26: Indicadores de Proyectos



Fuente: Documento TI – Reunión 11 de marzo de 2021

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 tomar. Ver imagen 27.

Imagen 27: Informe portafolio proyectos TI



Fuente: Informe Portafolio del Proyecto – Repositorio – Reunión 11 de marzo de 2021

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.

Imagen 28: Salidas de la fase de Ejecución/Implementación

		PROYECTO INTERNO	PROYECTO EXTERNO
1	Comunicaciones con el cliente (Si aplica)	R	R
2	Actas de Reunión internas	OP	R
3	Actas de Reunión externas (Si aplica)	NA	R
4	Entregables del proyecto	R	R
5	Actas de aceptación de los entregables / proyecto y Aceptación en Zeus de los requerimientos que hacen parte del proyecto (cliente interno)	R	R
6	Product Increment - Integración al producto de los ítems completados en el sprint	R	R
7	Tablero Kanban -Dayly Standup	R	R
8	Actualización del Sprint Backlog	R	R
R= Requerido NA= No Aplica OP=Opcional			

Fuente: Ejecución/Implementación – Circular 127 – Reunión 11 de marzo de 2021

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.

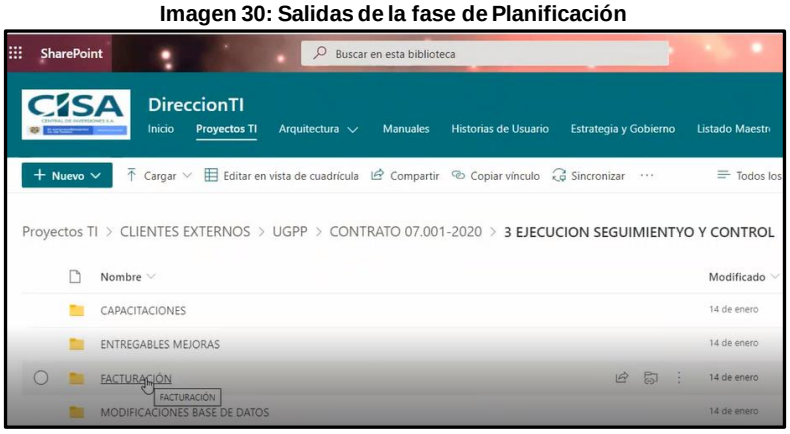
Imagen 29: Salidas de la fase de Seguimiento y Control

SALIDAS DE LA FASE DE SEGUIMIENTO Y CONTROL			
	REGISTRO	METODOLOGÍA ÁGIL INTEGRADA	
		PROYECTO INTERNO	PROYECTO EXTERNO
1	Informes de Gestión del Proyecto: Informe de supervisión y/o ANS.	NA	R
2	Seguimiento en el Comité de Proyectos usando la Herramienta de gestión de proyectos de tI.	R	R
3	Actas de Reunión internas (Si aplica) – Comités proyecto	OP	OP
4	Actas de Reunión externas (Si aplica) – Comités proyecto	NA	R
5	Registro de Control de cambios en la herramienta de gestión de proyectos	R	R
6	Registro de Lecciones aprendidas como resultado reunión retrospectiva	R	R
7	Tablero Kanban - Daily Stand up - Registros de seguimiento al cronograma – meta del sprint	R	R
8	Actualización del Product Backlog del proyecto	R	R
9	Métricas del proyecto	R	R
R= Requerido NA= No Aplica OP=Opcional			

Fuente: Seguimiento y Control – Circular 127 – Reunión 11 de marzo de 2021

La documentación de esta fase se encuentra 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.

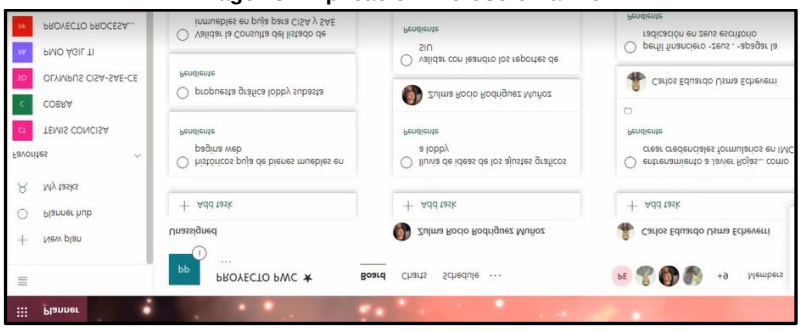
Imagen 30: Salidas de la fase de Planificación



Fuente: Ejecución Seguimiento y Control – Repositorio Documental– 11 de marzo de 2021

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

Imagen 31: Aplicación Microsoft Planner



Fuente: Ejecución Seguimiento y Control – Daily – Reunión 11 de marzo de 2021

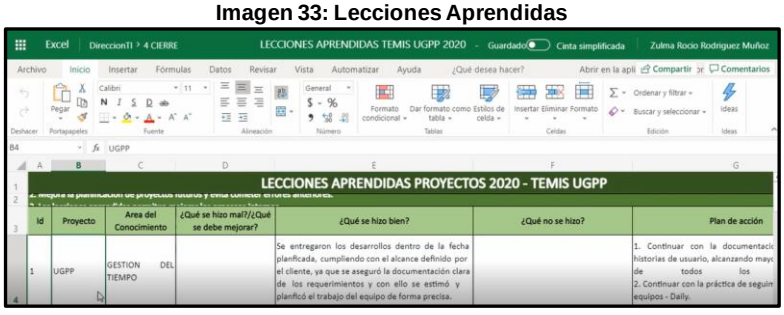
e. Fase de Cierre: En esta etapa se genera el informe del cierre del proyecto, la encuesta de satisfacción del cliente, el registro final de lecciones aprendidas que se registra en la aplicación Celoxis, aceptación del usuario y manuales de usuario.

Imagen 32: Salidas de la fase de Cierre

SALIDAS DE LA FASE DE CIERRE DEL PROYECTO			
REGISTRO		METODOLOGÍA ÁGIL INTEGRADA	
		PROYECTO INTERNO	PROYECTO EXTERNO
1	Informe de Cierre del proyecto. (Si aplica)	OP	R
3	Paz y Salvo contractual (Si aplica) / Acta de liquidación	NA	R
4	Encuesta de Satisfacción cliente– post proyecto- Encuesta de Satisfacción servicio de Software	R	R
5	Registro final de lecciones aprendidas	R	R
6	Activos de proceso del proyecto almacenados en el repositorio	R	R
7	Consolidado Aceptación del producto / proyecto - Zeus	OP	R
8	Manuales de usuario	R	R
R= Requerido NA= No Aplica OP=Opcional			

Fuente: Seguimiento y Control – Circular 127 – 11 de marzo de 2021

Imagen 33: Lecciones Aprendidas



Fuente: Registro de Lecciones Aprendidas – Repositorio – 11 de marzo de 2021

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 correo electrónico en cumplimiento del Memorando Circular 59 versión 2 del 8 de octubre de 2020.

Todos los desarrollos se gestionan con solicitudes ingresadas en el aplicativo Zeus que van asociadas a una orden de trabajo, se evidencia en éste aplicativo los estados del flujo "Gestión requisitos mejorado" y los archivos de cada una de las fases, a continuación, se muestran los archivos adjuntos, los estados definidos para el flujo y la estimación de tiempos que se realizaba en el aplicativo TFS:

Imagen 34: Archivos Adjuntos Aplicativo Zeus

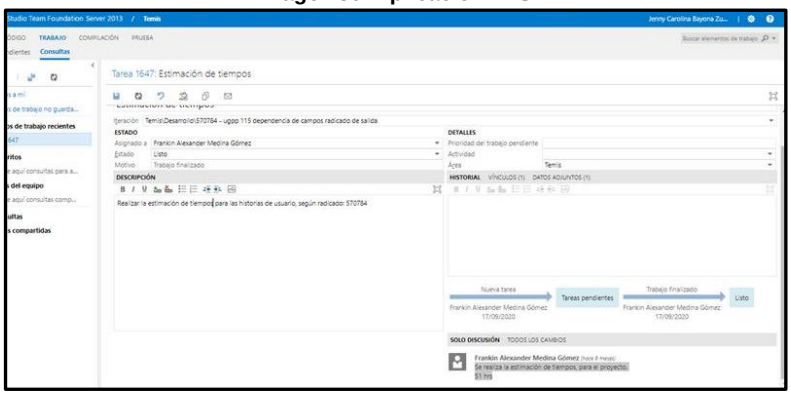
Fuente: Documentación Adjunta – Aplicativo Zeus– 11 Reunión de marzo de 2021

Imagen 35: Estados del Flujo

No.	FLUJO GESTIÓN REQUISITOS MEJORADO
1	RADICADO
2	PENDIENTE VALIDACIÓN OFICINA DE PROYECTOS
3	PRESENTAR SOLICITUD ANTE EL COMITÉ DE ARQUITECTURA
4	PRIORIZAR Y ASIGNAR AL INGENIERO DE REQUERIMIENTOS
5	PENDIENTE CONSTRUIR HISTORIAS DE USUARIO
6	SOCIALIZAR Y APROBAR EL DOCUMENTO POR PARTE DEL USUARIO
7	ACTUALIZAR REPOSITORIO
8	PLANIFICAR LA ARQUITECTURA Y DISEÑO DE LA SOLUCIÓN
9	PENDIENTE ESTIMACIÓN DE TIEMPO
10	ACTUALIZAR CRONOGRAMAS - ASIGNAR INGENIERO Y SOCIALIZAR HISTORIA DE USUARIO
11	EJECUCIÓN DE DESARROLLO
12	ENTREGAR DESARROLLO A PRUEBAS DE CALIDAD
13	PENDIENTE DESPLIEGUE EN AMBIENTE DE PRUEBAS
14	PENDIENTE EJECUTAR PRUEBAS DE QA
15	PENDIENTE ACTUALIZAR MANUAL DE USUARIO
16	PENDIENTE PASO A PREPRODUCCIÓN
17	EJECUTAR PRUEBAS PREPRODUCCIÓN
18	REVISAR NORMATIVIDAD VS NUEVO DESARROLLO
19	EJECUTAR GESTIÓN DE CAMBIOS
20	SOCIALIZACIÓN Y ACEPTACIÓN DEL CAMBIO
21	ACTUALIZAR MANUALES DE USUARIO
22	PENDIENTE REVISAR MANUALES
23	PENDIENTE PASO A PRODUCCIÓN MANUALES
24	VALIDAR CUMPLIMIENTOS POLÍTICA DE SEGURIDAD

Fuente: Información Dirección TI – Estados Flujo Zeus – Reunión 11 de marzo de 2021

Imagen 36: Aplicación TFS



Fuente: Estimación de tiempos – TFS– Reunión 11 de marzo de 2021

Al realizar el recorrido del proceso en la sesión de trabajo con la Líder de la Oficina de Proyectos TI tomando un ejemplo del flujo "Gestión de requisitos mejorados" con el radicado 570784 "Temis UGPP", en la aplicación Zeus se evidenció: que los soportes de salida de cada una de las fases de la "Metodología de Desarrollo" 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 encontraban adjuntos; que el usuario que generó el radicado realizó las pruebas unitarias y al verificar el documento de las pruebas éste se encontró sin información.

Imagen 37: Documento pruebas unitarias sin información

Fuente: Información Dirección TI – Reunión 11 de marzo de 2021

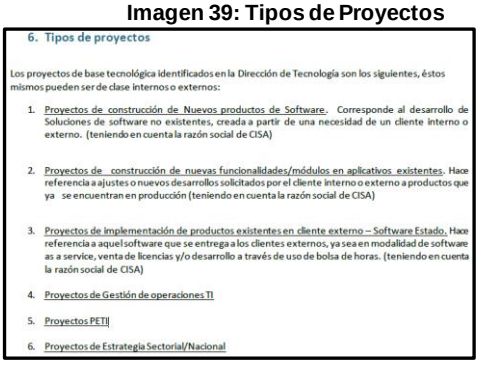
Imagen 38: Trazabilidad actividades del radicado

Fuente: Consulta aplicativo Zeus – Reunión 11 de marzo de 2021

De acuerdo a lo anterior, 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) ver. 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 CN127 versión 16 en el numeral "6. Tipos de proyectos", tal como se muestra la imagen 39, se tomó una muestra de 30 solicitudes del flujo "Gestión requisitos mejorado" para la vigencia de 2020 y se revisaron los soportes en la herramienta Zeus, encontrando las siguientes situaciones:

Imagen 39: Tipos de Proyectos



6. Tipos de proyectos

Los proyectos de base tecnológica identificados en la Dirección de Tecnología son los siguientes, éstos mismos pueden ser de clase internos o externos:

1. Proyectos de construcción de Nuevos productos de Software. Corresponde al desarrollo de Soluciones de software no existentes, creada a partir de una necesidad de un cliente interno o externo. (teniendo en cuenta la razón social de CISA)
2. Proyectos de construcción de nuevas funcionalidades/módulos en aplicativos existentes. Hace referencia a ajustes o nuevos desarrollos solicitados por el cliente interno o externo a productos que ya se encuentran en producción (teniendo en cuenta la razón social de CISA)
3. Proyectos de implementación de productos existentes en cliente externo – Software Estado. Hace referencia a aquel software que se entrega a los clientes externos, ya sea en modalidad de software as a service, venta de licencias y/o desarrollo a través de uso de bolsa de horas. (teniendo en cuenta la razón social de CISA)
4. Proyectos de Gestión de operaciones TI
5. Proyectos PETI
6. Proyectos de Estrategia Sectorial/Nacional

Fuente: CN127 – Reunión 11 de marzo de 2021

- 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 CN127 "Políticas y Procedimientos para la Gestión de Proyectos de Tecnología", lo cual no se evidenció el cumplimiento del "Ciclo de vida del software" por parte del equipo auditor.

Al validar con la Dirección de Tecnología se evidencia 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.

Al realizar la validación 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 CN127 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

CISA tiene definido en la Circular Normativa 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.

De acuerdo a la información suministrada por la Dirección Tecnológica se evidencian los siguientes estados para el flujo de "Gestión de cambios":

Imagen 40: Estados de Flujo

No.	ESTADOS FLUJO GESTIÓN DE CAMBIOS
1	RADICADO
2	PENDIENTE REVISIÓN ARQUITECTURA DE SOFTWARE
3	PENDIENTE REVISIÓN OFICIAL DE SEGURIDAD DE LA INFORMACIÓN
4	PENDIENTE REVISIÓN JEFATURA DE MEJORAMIENTO CONTINUO
5	PENDIENTE REVISIÓN GERENCIA DE TI
6	PENDIENTE REVISAR CRITERIOS DE OPERACIONES TECNOLÓGICAS Y PROGRAMAR REUNIÓN CAB
7	PENDIENTE PROGRAMAR REUNIÓN DE CAMBIOS CRÍTICOS
8	PENDIENTE HABILITAR SUPERUSUARIO
9	PENDIENTE AJUSTAR RFC NO SE ESTA REALIZANDO
10	PENDIENTE IMPLEMENTAR EL CAMBIO
11	PENDIENTE DESHACER EL CAMBIO Y DETERMINAR CAUSA DE ERROR
12	PENDIENTE CONFIRMAR LA PUESTA EN PRODUCCIÓN

Fuente: Información Dirección TI – Estados Flujo Zeus – Reunión 11 de marzo de 2021

Durante la etapa de ejecución de la auditoría para la vigencia de 2020 de los 299 radicados de Gestión de Cambios se determinó una muestra de 30 solicitudes en cumplimiento al Anexo 7 de la CN093, 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:

- Las solicitudes no cuentan con una 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 093 versión 63 del 30 de diciembre

de 2020 numeral "6. Descripción de actividades" y en el subnumeral "2.2 Responsables" se menciona que el CAB está conformado por el Director de Tecnología y Sistemas de Información, el Oficial de Seguridad de la Información, Jefe de Procesos y Productividad y el Jefe de Operaciones Tecnológicas o sus delegados respectivos, además se observa la existencia de invitados al comité, como los Líderes de los Aplicativos o sus delegados, usuarios, encargados de desarrollo, consultores técnicos, expertos según el tipo del cambio solicitado, siendo este el escenario para la toma de decisiones sobre los cambios requeridos en Tecnología.

- 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 octubre de 2019, subnumeral "4.2.2 Formato de Cambios", sin embargo, la Dirección de TI, indica que para este documento se utiliza "Plan de trabajo", el cual no contiene la información inicial de la solicitud.

- CISA define los cambios por la prioridad "Critica" y "Programada" de acuerdo al Anexo 7 de la CN093 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 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 la gestión de cambios.

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

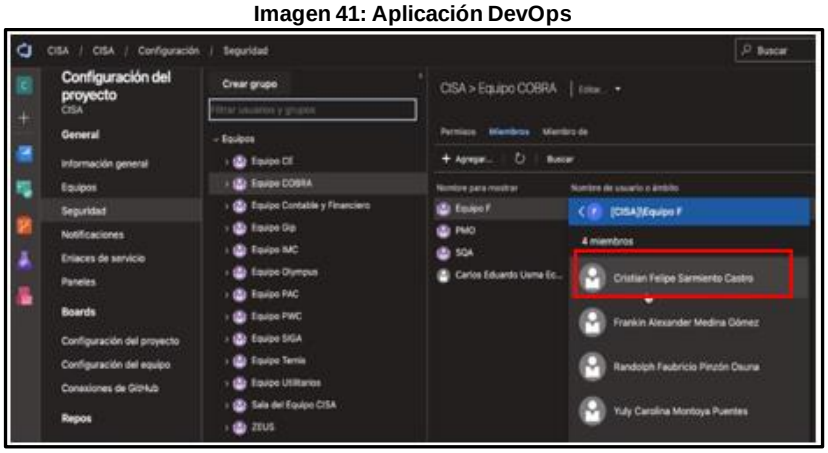
versiones, dicha herramienta apoya a los desarrolladores a crear, probar, implementar y supervisar las aplicaciones de la entidad.

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.

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. A continuación, se muestra la imagen de la herramienta con las células asignadas a los equipos de trabajo:

Imagen 41: Aplicación DevOps



Fuente: Reunión 29 de marzo de 2021

Actualmente, DevOps se encuentra en implementación, no se tiene en este momento el módulo de Continuous Integration (Integración Continua), Continuous Release

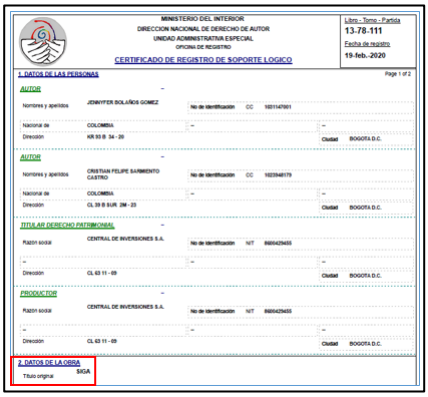
(Paso a Producción automático), el Pull request (validación del código), estas actividades se realizan de forma manual, es decir el versionamiento no es automático. Se sugiere implementar estos módulos de la herramienta DevOps con el fin de optimizar el proceso de control de versiones del software.

4.4.4. Derechos de Autor ante DNDA

La Dirección de Tecnología tiene definido el procedimiento para el Registro de software desarrollado en CISA, el cual se encuentra documentado en la CN093 "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, a continuación, se muestra un "Certificado de Registro de Soporte Lógico":

Imagen 42: Certificado del DNDA



MINISTERIO DEL INTERIOR
DIRECCION NACIONAL DE DERECHO DE AUTOR
UNIDAD ADMINISTRATIVA ESPECIAL
OFICINA DE REGISTRO

Libro - Tomo - Partida
13-78-111
Fecha de registro
19-feb.-2020

CERTIFICADO DE REGISTRO DE SOPORTE LOGICO

1. DATOS DE LAS PERSONAS

Page 1 of 2

AUTOR
Nombres y apellidos: JENNYFER BOLAÑOS GOMEZ — No de identificación: CC 1031147001
Nacional de: COLOMBIA
Dirección: KR 93 B 34 - 20 — Ciudad: BOGOTA D.C.

AUTOR
Nombres y apellidos: CRISTIAN FELIPE SARMIENTO CASTRO — No de identificación: CC 1023949179
Nacional de: COLOMBIA
Dirección: CL 39 B SUR 2M - 23 — Ciudad: BOGOTA D.C.

TITULAR DERECHO PATRIMONIAL
Razón social: CENTRAL DE INVERSIONES S.A. — No de identificación: NIT 8600425455
Dirección: CL 63 11 - 09 — Ciudad: BOGOTA D.C.

PRODUCTOR
Razón social: CENTRAL DE INVERSIONES S.A. — No de identificación: NIT 8600425455
Dirección: CL 63 11 - 09 — Ciudad: BOGOTA D.C.

2. DATOS DE LA OBRA
Título original: SIGA

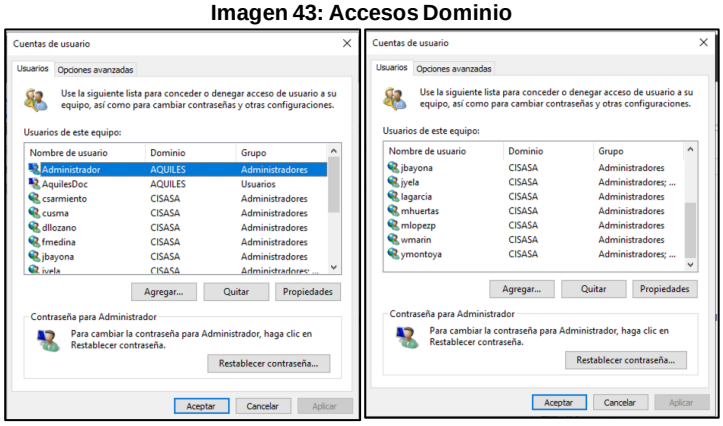
Fuente: Dirección de Tecnología – 4 de marzo de 2021

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, a continuación, se muestra un ejemplo de la consulta realizada al servidor Aquiles de desarrollo:

Imagen 43: Accesos Dominio



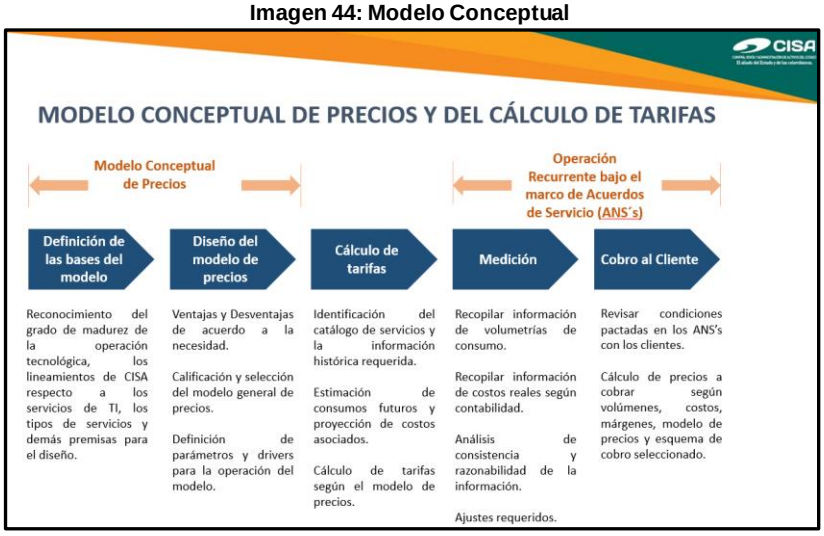
Fuente: Información Dirección TI del 25 de marzo de 2021

Se evidencia 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, como se muestra a continuación:

Imagen 44: Modelo Conceptual



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

El modelo 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.

Imagen 45: Costos Administrativos

Costos TI/mes X puesto de Trabajo estándar					
Equipo de Cómputo	$ 75.235	$ 75.235	$ 75.235	$ 75.235	$ 75.235
Licencia Office	$ 105.400	$ 105.400	$ 105.400	$ 105.400	$ 105.400
Licencia Antivirus	$ 13.334	$ 13.334	$ 13.334	$ 13.334	$ 13.334
Extensión Telefónica	$ 50.400	$ 50.400	$ 50.400	$ 50.400	$ 50.400
Internet	$ 6.000	$ 6.000	$ 6.000	$ 6.000	$ 6.000
Promedio Adtvo Planta(263)					
Costo Adtvo X persona	$ 380.000	$ 380.000	$ 380.000	$ 380.000	$ 380.000
Acueducto, energia, parqueaderos, arriendos, telefonía fija, cafetería, papelería, vigilancia, aseo, alojamiento y manutención, etc.					
Licencias especializadas					
Vstudio	$ 293.333		$ 293.333	$ 293.333	
EA	$ 233.333			$ 233.333	
Project		$ 74.667			
Snagit	$ 11.500		$ 11.500	$ 11.500	$ 11.500
Costo Mes (160 horas)	$ 1.168.536	$ 705.036	$ 935.202	$ 1.168.536	$ 641.869
Costo Hora	$ 7.303	$ 4.406	$ 5.845	$ 7.303	$ 4.012
ROL	**Arquitecto**	**Analista Negocio**	**Desarrollo**	**QA**	**UX**

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

De acuerdo a los reportes suministrados por el área contable se observa que en la estructura de gastos para el 2020 se tienen $592 millones, en donde se encuentran gastos en: servicio de nube, nómina y puesto de trabajo, en 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 46: 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, incurriendo en una eventual subjetividad de los porcentajes asignados a cada proyecto afectando la rentabilidad real y que son reportados al área financiera, tal como se observa en la siguiente imagen:

Imagen 47: 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

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.

Actualmente 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, actualmente la rentabilidad de los proyectos se calcula basados en estimaciones de los tiempos dedicados a cada proyecto.

Es importante mencionar que la entidad contrató una consultoría que finalizó en agosto de 2019 para establecer la metodología de medición de cargas de trabajo de la Dirección de Tecnología y Sistemas de Información donde se planteaban entre otros objetivos específicos los siguientes:

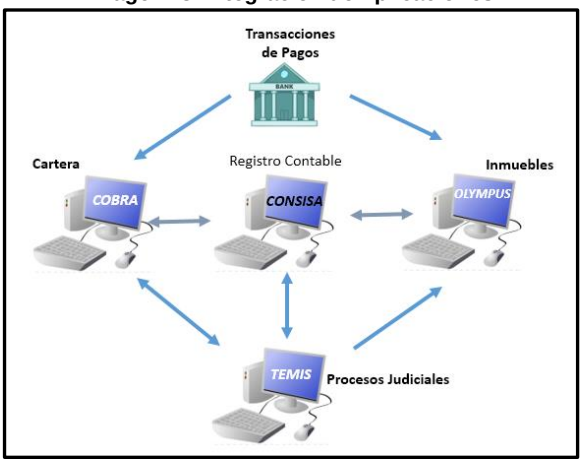
- Establecer el método para determinar las necesidades de recursos humanos para la Dirección de Tecnología (operaciones tecnológicas y desarrollo de software).
- Suministrar la herramienta para la medición de cargas de trabajo de la Dirección de Tecnología (operaciones tecnológicas y desarrollo de software), es decir, para cada uno de los tipos de cargo.

Como resultado de esta consultoría principalmente se estableció la necesidad de nuevos recursos o roles y mantener el modelo organizacional de la Dirección Tecnológica y entre los entregables se deja la herramienta (Excel) para la medición de cargas de trabajo que se aplicó durante la consultoría, la cual podría utilizarse en caso de requerirse este nuevo análisis por parte de la misma Dirección Tecnológica o el área de Gestión Humana. No obstante a la fecha de este informe se notificó al equipo auditor que no se ha usado la citada herramienta.

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 48: 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 como los siguientes para minimizar afectaciones a la integridad, confidencialidad y confiabilidad de la información:

- Identificador único en Cobra para el contrato y las obligaciones.
- Identificador único para los inmuebles en Olympus.
- Controles de acceso para la modificación de contratos, creación de inmuebles, cargue masivo de obligaciones y restricción de campos.
- Validación de reglas y/o políticas como:
  - ✓ Validación del vencimiento del avalúo para generar uno nuevo.
  - ✓ Si el avalúo se encuentra vencido no se publica en la página web.
  - ✓ Cambio de estado de avalúo cuando esta vencido de "Comercial" a no "Comercializable".

- Controles informativos y/o alertas, como:
  - ✓ Si el usuario cambio un avalúo el sistema genera si la información es correcta y por medio del mensaje: “Confirme si la información digitada es correcta?”.
  - ✓ Cuando llega una oferta nueva para un inmueble se emite una alerta al Coordinador.
  - ✓ Cuando se elimina una Gestión de un contacto el sistema muestra: “Esta seguro que desea eliminar la Gestión del contacto?”.
- Controles de acceso basados en perfiles y roles que se encuentran alineados con la CN093 “Política y Procedimiento de Gestión Tecnológica”, Versión 62 del 30 de diciembre de 2020, numeral “5. Políticas de Operación”, subnumeral “5.1.2.1 Política de Control de Acceso”.

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 CN093 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.

Al validar las modificaciones a la base de datos se evidencia el posible riesgo de falta de integridad de la información, tal como se muestra a continuación en las siguientes solicitudes: el radicado 555255 “Eliminación de Obligaciones repetidas en Procesos Temis” y el radicado 569681 “Eliminación homologado duplicado Banco Agrario”, donde se duplica la información en la base de datos.

Imagen 49: Consulta Modificación BD

Fuente: Aplicativo Zeus – Reunión 23 de abril de 2021

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

Imagen 50: 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 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 sistema 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.

Al revisar otros flujos se encontraron cuatro (4) solicitudes en el flujo de "Soporte a aplicativos institucionales" y una solicitud del flujo de "Soporte aplicativos a Terceros", donde se observan errores de registros duplicados lo que muestra que la aplicación no posee controles que valide correctamente la información ingresada, a continuación, se relacionan las solicitudes identificadas:

Imagen 51: Consulta Estados Modificación BD

RADICADO	ALIAS	Flujo
540314	LEGALIZACIONES DUPLICADAS	Soporte aplicaitvos institucionales
541341	ERROR LEGALIZACIONES DUPLICADAS EN EL SIGEP DAR 135	Soporte aplicaitvos institucionales
543249	OBLIGACION DUPLICADA C.C. 101479238	Soporte aplicaitvos institucionales
563421	ERROR ARCHIVOS DUPLICADOS SIN ESTAR DUPLICADOS	Soporte aplicaitvos institucionales
606868	FALLA DUPLICIDAD ABOGADO RAMIREZ OSORIO JORGE HERNANDO	Soporte aplicaitvos institucionales
542878	DUPLICIDAD INFORMACIÓN PROYECTO MAGDALENA DOS	Soporte aplicativos a Terceros

Fuente: Aplicativo Zeus – Reunión 11 de marzo de 2021

Se consultó en Zeus, los estados del flujo "Solicitud modificación o adición información en BD", encontrando los siguientes estados:

Imagen 52: Consulta Estados Modificación BD

No.	ESTADO
1	RADICADO
2	PENDIETE VALIDACION LIDER DEL APLICATIVO
3	PENDIENTE VALIDAR POR EL GERENTE DEL AREA
4	PENDIENTE REVISIÓN ANALISTA CONTABLE
5	**PENDIENTE APROBACION CONTABLE**
6	PENDIENTE APROBACIÓN DIRECTOR DE TECNOLOGIA
7	PENDIENTE REVISIÓN JEFE OPERACIONES TECNOLÓGICAS
8	**PENDIENTE VALIDACIÓN OFICIAL DE SEGURIDAD DE LA INFORMACIÓN**
9	PENDIENTE EJECUCION EN PRODUCCION
10	PENDIENTE VALIDAR SOLICITUD

Fuente: Aplicativo Zeus – Reunión 11 de marzo de 2021

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 Circular normativa 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)".* Teniendo en cuenta el volumen de estas solicitudes pueden considerarse como una actividad rutinaria que genera carga operativa en el proceso de Gestión Tecnológica.

4.7.7.2 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 se observa en la siguiente imagen:

Imagen 53: Consulta Estados Modificación BD

	A	B	C	D	E	F	G
	IdInmueble	CedulaCatastral	chip	MatMatricula	MatChip	ValorAvaluoCatastral	FechaAvaluoCatastral
	14289	01010001087801		01N-291264		1154833	2300-01-01 00:00:00
	16064	01-04-0117-0001-000		280-43348		77787500	2219-04-15 00:00:00
	3570	010001960163801		232-0026708		8275000	5005-12-31 00:00:00
	17277	01-02-0551-0016-000				4900	3012-02-03 00:00:00

Fuente: Tomada de BD suministrada por Jefatura de Operaciones TI - 4 de mayo de 2021

En 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.

5. HALLAZGOS

5.1. Metodología de desarrollo

En revisión realizada a 30 solicitudes del flujo "Gestión Requisitos Mejorado" atendidas por la Dirección de Tecnología de CISA, se identificó 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 CN127 "Políticas y Procedimientos para la Gestión de Proyectos de Tecnología", lo cual no evidencia el cumplimiento del "Ciclo de vida del software" por parte del equipo auditor.

Adicionalmente se observa que existen solicitudes del flujo "Gestión Requisitos Mejorado" que no corresponde a Proyectos, es decir, que no cumplen el requisito que define la CN127 en el numeral "3. Definiciones", que sean más de 180 horas en su desarrollo, dato que no se muestra en la documentación o herramienta Zeus, lo cual no conlleva a la implementación de toda la metodología del Desarrollo de Software.

5.2. Solicitud de Modificación o adición de información a las bases de datos

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 del flujo de Zeus llamado "Modificación o adición información en BD", las cuales son ejecutadas por el área de Tecnología, a través de acciones directamente sobre la base de datos. Al revisar las solicitudes de este fujo 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, una cifra considerable de cambios directo a las bases de datos de la entidad.

Al verificar 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:

APLICACIÓN	SITUACIONES IDENTIFICADAS
COBRA **206 solicitudes**	• 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
OLYMPUS SAE **125 solicitudes**	Las 125 solicitudes son 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.
OLYMPUS **93 solicitudes**	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).
TEMIS **123 solicitudes**	Se identificaron 123 solicitudes 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.
CONCISA **12 solicitudes**	Las 12 solicitudes 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.

Si bien este tipo de modificaciones cuentan con niveles de aprobación como los de la oficial de seguridad, jefe del área solicitante, usuario líder de la aplicación y por el área financiera que evalúa el impacto contable, hace 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, tal como se menciona en la CN093 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)"*. Lo anterior conlleva a que se debe identificar un riesgo que permita mitigar el impacto de la posible pérdida de integridad de la información, estableciendo controles efectivos.

5.3. Integridad de la información en las BD

Evaluadas 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 falta de controles de cargue o de reglas de negocio que no estén adecuadamente definidas o configuradas en las aplicaciones, por lo tanto es importante que se identifique la causa raíz de cada una de las situaciones.

6. OBSERVACIONES

6.1. Gestión de riesgos

Se observa que en la "Matriz de Riesgos – Infraestructura Tecnológica" falta la definición de eventos de riesgos de acuerdo a la caracterización del subproceso de "Construcción de software" 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 se contemple este aspecto de la rotación de personal y así minimizar los impactos generados.

6.2. Evaluación de indicadores

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 dentro del 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.

En el cálculo del indicador "Cumplimiento Plan de Proyectos y Requisitos de Software" se observa que se está midiendo en el mismo indicador dos temas 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.

6.3. Actualización de manuales de usuario

Al realizar la verificación de los manuales de usuario de las aplicaciones que se encuentran 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.

6.4. Documentación de lecciones aprendidas

Se observó que en la metodología "Gestión de Proyectos de Tecnología", si bien, se registran las Lecciones Aprendidas, no se cuenta con la consolidación de dichas lecciones junto con los planes de acción que permitan no incurrir en errores presentados en el pasado.

6.5. Gestión de cambios

Respecto a la aplicación de las actividades definidas para la gestión de cambios se identificaron las siguientes observaciones:

a. En revisión de una muestra de 30 solicitudes de "Gestión del cambio" no se observa una 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" Versión 21 del 20 de octubre de 2020, de la CN093 versión 62.

b. 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".

c. CISA define los cambios por la prioridad "Critica" y "Programada" de acuerdo al Anexo 7 de la CN093 en el numeral 5 subnumeral "5.1 Solicitudes de Gestión de Cambios"; sin embargo, no se encuentra alineada a lo que sugiere el documento "G.SIS.01 Guía del dominio de Sistemas de Información" del MINTIC versión 1.1 octubre de 2019, en el numeral "4.2 Procedimiento de cambios", donde se menciona que las solicitudes de cambios deben ser clasificadas como estándar, normal y emergencia.

6.6. Derechos de Autor ante DNDA

CISA cuenta con los "Certificados de Registros de Soporte Lógico" de sus aplicaciones ante la Dirección Nacional de Derechos de Autor, no obstante, la Dirección Tecnológica no tiene claridad sobre los criterios a tener en cuenta para presentar la solicitud de actualización ante la DNDA de estos Certificados para mantener vigente la protección de derechos de autor, reconocimiento de derechos morales y patrimoniales de la entidad.

6.7. Modelo de costos de desarrollo

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, incurriendo en una eventual subjetividad de los porcentajes asignados a cada proyecto y que son reportados al área financiera.

7. RECOMENDACIONES[1]

7.1. Metodología de desarrollo

Al validar los hallazgos presentados en el tema "Ciclo de vida de Proyectos ", se sugiere analizar la posibilidad de adquirir una herramienta robusta para la gestión de

[1] Se incluye este texto como última recomendación en el informe definitivo

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.

7.2. Solicitud de Modificación a las BD

Efectuar un análisis junto con los dueño de los procesos a 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.

7.3. Integridad de la información en las BD

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.

7.4. Gestión de riesgos

Si bien, la Dirección de Tecnología se encuentra en el proceso de construcción, aprobación y divulgación de los riesgos del área de Tecnología, se sugiere 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.

7.5. Evaluación de indicadores

Se recomienda revisar la estructura de los indicadores de "Atención de las solicitudes de soporte de aplicativos institucionales y de terceros" 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.

7.6. Actualización de manuales de usuario

En cuanto a 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.

7.7. Documentación de lecciones aprendidas

Se sugiere que se implemente una bitácora o herramienta de consolidación que permita identificar las acciones de mejora a partir de estas 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.

7.8. Gestión de cambios

Con 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. Incluir en el procedimiento de "Gestión de Cambios" el Formato de Requerimiento de Cambios, que incluyan los datos básicos de la solicitud formal, tal 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"

c. Definir por lo menos tres tipos de cambios: Cambio estándar; Cambio normal y Cambio de emergencia, con el fin establecer mayores criterios para el análisis de su clasificación, priorización y gestión de este tipo de requerimientos como lo sugiere la "G.SIS.01 Guía del dominio de Sistemas de Información" del MINTIC versión 1.1 octubre de 2019, en el numeral "4.2 Procedimiento de cambios".

d. Considerar la implementación de los siguientes indicadores operativos que puedan medir la eficacia de la gestión de cambios:
   - Porcentaje de cambios exitoso.
   - Porcentaje de Cambios con ejecución fallida.
   - Porcentaje de cambios rechazados por el CAB.
   - Porcentaje de cambios por aplicativo o servicio.
   - Porcentaje de cambios de: menores, mayores y de emergencia atendidos.

   Estos pueden soportar la identificación de incidentes, reducir el número de reprocesos y problemas asociados a los cambios. En la "G.SIS.01 Guía del dominio de Sistemas de Información" ver 1.1 de octubre de 2019 de MINTIC en el numeral "4. Ciclo de vida de los Sistemas de Información" se pueden observar estos indicadores.

7.9. Derechos de Autor ante DNDA

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 Dirección Nacional de Derechos de Autor, es decir, cuál es el criterio, (p. ej. porcentajes de cambio), 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.

7.10. Modelo de costos de desarrollo

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 de cada servicio para calcular la rentabilidad de cada uno y de la línea de servicio de Software Estado.

8. CONCLUSIÓN DE AUDITORÍA

Como resultado general de la evaluación al componente de Desarrollo de software y gestión de cambios se identificó que el proceso de Gestión Tecnológica de Central de Inversiones S.A., tiene enfoque principalmente en el desarrollo, soporte y mantenimiento de aplicaciones, considerando que estas son utilizadas para el soporte de los procesos del negocio y que tienen el servicio denominado "Software Estado" que consiste en prestar servicios de software a otras entidades del Estado por lo tanto cuentan con herramientas, metodología y procedimientos para la gestión del desarrollo de software, gestión de cambios, soporte y mantenimiento; sin embargo se presentan oportunidades de mejora relacionadas con la evidencia del cumplimiento metodológico del ciclo de vida del software y la identificación de los tiempos reales asignados cada uno de los desarrollos, mantenimiento o soporte de aplicaciones.

Si bien la entidad cuenta con esquemas de control sobre la información que se procesa en las aplicaciones, es importante que se minimice los cambios directos de datos a las bases de datos, con el propósito de mantener las características de la información como integridad, confiabilidad y confidencialidad.

9. MESA DE TRABAJO

En atención al "Procedimiento para Auditorías Internas de Gestión", una vez remitido el informe preliminar por el Auditor Interno, el líder del proceso auditado dispone de tres (3) días hábiles para convocar y realizar la mesa de trabajo, no obstante el Director de Tecnología responde por medio de correo electrónico el día 10 de junio de 2021, que no le es posible agendar la mesa de trabajo y envía sus comentarios al informe, los cuales son analizados y respondidos por el equipo auditor de Bellicorp el día 15 de junio de 2021, quedando las mismas conclusiones del informe preliminar.

10. ANEXOS

Aprobado por:	Elaborado por:	Fecha aprobación
Elkin Orlando Ángel Muñoz Auditor Interno	**Bellicorp SAS** **Auditor Externo** **Equipo Auditor**	(16/06/2021)