NOMBRE DEL PROCESO: Auditoria al Proceso de Infraestructura Tecnológica

INFORME DEFINITIVO: 18 de agosto de 2017

1. INTRODUCCIÓN

La Oficina de Control Interno, en ejercicio de las facultades legales otorgadas por la Ley 87 de 1993, modificada por la Ley 1474 de 2011, el Decreto 2145 de 1999 y sus modificaciones; Los Decretos 019, 2482 y 2641 de 2012, el Decreto 943 de 2014, Decreto 648 de 2017 y las Circulares Normativas establecidas por la Entidad, el estatuto de Auditoría Interna y la guía de auditoría para entidades públicas emitida por el DAFP en su versión No 2, tiene como función realizar la evaluación independiente y objetiva al Sistema de Control Interno, a los procesos, procedimientos, actividades y actuaciones de la administración, con el fin de determinar la efectividad del Control Interno, el cumplimiento de la gestión institucional y los objetivos de la Entidad, produciendo recomendaciones para asesorar al Representante Legal y al Comité de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva, en busca del mejoramiento continuo del Sistema de Control Interno.

En cumplimiento al Programa General de Auditorías aprobado en el mes de enero de 2017, por el Comité Asesor de Junta Directiva de Auditoria, la Oficina de Control Interno suscribió el contrato 016-2017, con la firma Deloitte & Touche Ltda., para realizar la Auditoria al Proceso de Infraestructura Tecnológica, el cual incluyó, la evaluación de controles generales de TI, controles automáticos y gestión de cambios en la compañía. Este informe tiene como propósito resumir el trabajo efectuado y las conclusiones obtenidas, además de efectuar las recomendaciones necesarias en pro del mejoramiento continuo del proceso, lo cual redundará en el cumplimiento de la Misión y los Objetivos Institucionales.

2. OBJETIVO DE LA AUDITORÍA

Evaluar sobre las plataformas Olympus, Cobra y Temis, una selección de controles generales de TI, gestión de cambios y controles automáticos con el fin de:

2.1. Evaluar las políticas y procedimientos de gestión tecnológica que permitan establecer controles en el uso y la administración de los sistemas de información en CISA.

2.2. Evaluar el diseño e implementación de los controles bajo alcance.

2.3. Revisar la implementación y efectividad operativa de los controles establecidos por CISA para los sistemas del alcance.

2.4. Identificar las oportunidades de mejoramiento para la gestión de riesgos de negocio originados en el uso de los recursos informáticos y la administración de controles de seguridad y operación para la plataforma tecnológica

2.5. Evaluar la efectividad del área de desarrollo, la metodología de desarrollo y el mantenimiento de las aplicaciones de la compañía.

3. ALCANCE

3.1. Controles generales de Tecnología:

Evaluar los procedimientos y los controles definidos por CISA, para las siguientes áreas de TI de las plataformas Olympus, Cobra y Temis:

- Seguridad de la información
- Control de acceso a las aplicaciones
- Centro de datos y operaciones de red

Para dichas áreas se cubrió el siguiente alcance:

a. Configuración de línea base de seguridad de las aplicaciones en base de datos y sistema operativo:
   I. Módulo de seguridad a nivel de la capa de aplicación, para controlar las políticas de contraseña
   II. Configuración de seguridad que soporta la ejecución de las aplicaciones Olympus, Temis y Cobra:
      - Servidor donde se almacenan las aplicaciones
      - Servidor donde se almacena la base de datos
      - Sistema operativo Windows del servidor de aplicaciones
      - Sistema operativo Windows del servidor de base de datos

b. Administración de usuarios
   I. Asignación de privilegios de acceso autorizados únicamente por el personal definido en los procedimientos de la entidad.
   II. Bloqueo de usuarios pertenecientes a funcionarios retirados de la compañía, según los procedimientos definidos por la entidad

c. Control de acceso y mantenimiento de dispositivos ambientales del centro de cómputo:

   I. Asignación de privilegios de acceso permanente al centro de cómputo de la entidad.

II. Controles ambientales implementados en el centro de cómputo.

d. Administración de las operaciones: procesos Batch y ejecución y almacenamiento de copias de respaldo:
   I. Ejecución de copias de respaldo acorde lo definido en las políticas de la entidad
   II. Envío a custodia externa de las copias de respaldo de la entidad
   III. Ejecución de pruebas de restauración para garantizar la disponibilidad de las copias de respaldo de la entidad.

e. Evaluación de aspectos normativos de tecnología relacionados con plan de continuidad de negocio y seguridad de la información.
   I. Definición del plan de continuidad del negocio de CISA
   II. Diagnóstico sobre el estado de implementación de ISO27001.

3.2. Gestion de cambios

Evaluar los procedimientos y los controles definidos por CISA para:

a. Control de cambios en aplicación y bases de datos para las plataformas Olympus, Cobra y Temis.
b. Segregación de funciones para los ambientes de desarrollo, producción y pruebas durante el proceso de control de cambios de las aplicaciones.
c. Aplicación de procedimientos, metodología formal y controles para el desarrollo y mantenimiento de aplicaciones que son comercializadas por CISA.
d. Métricas para la evaluación de la efectividad del área de desarrollo, incluyendo existencia y resultados de indicadores de gestión y medición sobre los procesos de desarrollo y soporte para las aplicaciones que comercializa CISA.

3.3. Controles automáticos:

Evaluar una selección de 25 controles automáticos relevantes sobre las aplicaciones Olympus, Cobra y Temis relacionados con:

I. Verificación de perfiles de usuarios en las aplicaciones que tienen acceso a las siguientes actividades:
   a. Creación de cargos administrativos, cargue de avalúos, creación y liquidación de inmuebles de CISA.
   b. Modificar porcentajes de compra y capital de las obligaciones previa a la conciliación.
   c. Actualizar saldos en Cobra.
   d. Modificar la asignación del portafolio de obligaciones

e. Actualizar información de los clientes en Cobra
f. Gestionar y convocar miembros del comité
g. Ingresar información a los procesos de Temis
h. Modificar porcentajes de propiedad de los inmuebles de CISA
i. Crear las obligaciones en Cobra

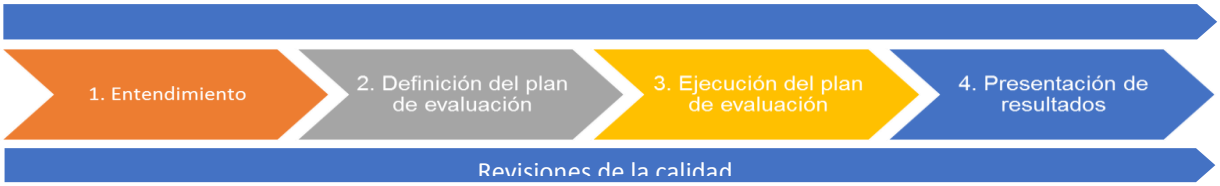
II. Verificar los valores ingresados en la oferta de Cobra y que esta no sea aceptada cuando se encuentre por debajo del valor de la negociación.
III. Verificar la interfaz entre Olympus y Concisa encargada de transmitir información de cuotas administrativas y sus pagos.
IV. Verificar que solo usuarios convocados a comité puedan registrar su decisión en Cobra y al finalizar se fije la vigencia de los acuerdos.
V. Verificar que el sistema Cobra no permita grabar obligaciones si la información definida por el previamente por área financiera no coincide.
VI. Verificar que Olympus calcule el valor parcial y total de los inmuebles.
VII. Verificar que Olympus calcule la viabilidad de las ofertas.
VIII. Verificar que el sistema realice el cálculo del valor propio del inmueble.
IX. Verificar la interfaz entre las aplicaciones Olympus y Temis para registrar los procesos jurídicos de los inmuebles de CISA.
X. Verificar que los conceptos jurídicos cargados por los abogados en Temis se vean reflejados en la aplicación Cobra.
XI. Verificar la interfaz de Cobra que refleja los pagos realizados por usuarios en portales bancarios.

3.4. Limitaciones en el alcance

Durante la evaluación de controles automáticos para identificar los usuarios con acceso a transacciones críticas en las aplicaciones Cobra, Temis y Olympus se solicitó al área de TI un reporte de usuarios vs perfiles y un reporte de perfiles vs menús y permisos (transacciones). Sin embargó, no fue posible obtener el listado de perfiles vs menús asociado a los nombres de los menús de las aplicaciones, por lo que se realizó una consulta por base de datos y se seleccionaron las transacciones que tuvieran un nombre similar al de cada aplicación. Teniendo en cuenta lo anterior, es posible que esta asociación no sea acertada, por lo que no fue posible obtener con total seguridad los usuarios con acceso a ciertos menús solicitados.

4. DESARROLLO DE LA AUDITORÍA

El proceso de auditoria se llevó a cabo en cuatro fases, de la siguiente manera:



4.1. Entendimiento

Se llevó a cabo un entendimiento general de los procesos del negocio, la infraestructura tecnológica de CISA para identificar, entre otros:

- Los procedimientos, responsabilidades y estructura organizacional del área de tecnología de la Compañía.
- Controles generales de tecnología en las aplicaciones y las plataformas tecnológicas donde operan.
- Principales módulos que conforman las aplicaciones y procesos que soportan.
- Procedimientos de gestión de usuarios, gestión de configuración y gestión de incidentes.
- Esquema de seguridad de las aplicaciones y sus plataformas tecnológicas.
- Identificación de controles automáticos claves de las aplicaciones que soportan los procesos de negocio

4.2. Definición del plan de evaluación

De acuerdo con el entendimiento obtenido en la fase anterior y las expectativas de la Compañía, se diseñaron los planes de revisión para la infraestructura tecnológica de CISA.

Las pruebas definidas para la evaluación de los controles generales de tecnología para la infraestructura tecnológica y desarrollo y mantenimiento de aplicaciones de CISA se realizaron con base en nuestra metodología, el enfoque COBIT 5 y bases de datos de buenas prácticas de seguridad.

La selección de controles de operación de las aplicaciones se realizó en conjunto con la compañía una vez identificados en la fase anterior los controles claves que soportan los procesos de negocio de CISA.

4.3. Ejecución del plan de evaluación

Con base en el plan de evaluación previamente definido establecimos los programas de trabajo detallados en donde se definió:

- Ejecutar las pruebas detalladas.

- Documentar los resultados.

La ejecución del plan incluyó la realización de pruebas de diseño e implementación, documentación y análisis de los resultados; dependiendo de la actividad de control a probar en cada caso, se utilizaron procedimientos de revisión que a nuestro juicio fuera el más efectivo, como revisión directa de los sistemas, muestreos, pruebas sobre datos, evaluación y verificación de documentación entre otros.

Durante el desarrollo de la auditoria en CISA se identificaron las siguientes situaciones, las cuales fueron subsanadas durante la etapa de ejecución.

4.3.1. Diseño del procedimiento de gestión de cambios

Durante la revisión al diseño de los controles implementados en la vigencia 2016, para la gestión de cambios en las aplicaciones de CISA y de la Circular 093 - Anexo 8, Instructivo para la Gestión de Cambios, se observó que el procedimiento en noviembre de 2016 actualizó lo siguiente:

Los cambios críticos son aprobados por el Comité Asesor de Cambios, anteriormente, eran aprobados por el Comité de Emergencia que estaba conformado únicamente por el Gerente de Tecnología y Sistemas de Información.

4.3.2. Inconsistencia en la ejecución de copias de respaldo

Para una muestra de cinco semanas del 2016, se solicitaron evidencias que permitieran verificar que las tareas de copias de respaldo se ejecutaron de forma exitosa y de acuerdo con los procedimientos establecidos en la Circular 093. Para la semana 16, la cual iba del lunes 18 al domingo 24 de abril, no se obtuvo la evidencia correspondiente, al log de la herramienta Dataprotector, con la cual se ejecutan las copias de respaldo en la actualidad.

En validación con la DBA, nos informó que debido a que la entidad se encontraba en proceso de actualización del servidor de versión Windows 2003 a Windows 2012, por lo que no se conservó el *log* del Dataprotector.

Teniendo en cuenta que no fue posible obtener la evidencia de la herramienta, se observó el soporte de envío de cintas, de acuerdo al control establecido por CISA para le externalización de cintas.

4.3.3. Valoración del software que vende CISA

Conocimos que se está llevando a cabo un proceso de mejora y actualización del área de desarrollo con el fin de optimizar las actividades del área y aumentar la rentabilidad de venta de aplicaciones que desarrolla CISA.

En la actualidad se está llevando a cabo un proyecto para evaluar los costos de los desarrollos, mantenimientos y soportes para cada cliente, teniendo en cuenta los requerimientos especiales, tipos de contratos y personal disponible para la realización de estas tareas. Este proyecto incluye la valoración de las aplicaciones con el fin de reactivar la venta de las mismas.

4.4. Presentación de resultados

Preparar e informar a las personas designadas por CISA y a las áreas que se considere necesario, acerca de los hallazgos que significan riesgos para la compañía, así como las recomendaciones que permitan definir y ejecutar planes de mejora necesarios para mitigar y administrar los riesgos identificados.

Realizamos las siguientes actividades:

- Validar los hallazgos y recomendaciones con las áreas responsables.
- Solicitar al área de tecnología, los responsables de definir e implementar los planes de acción y el cronograma de implementación, con el fin de facilitar el seguimiento que realizará la entidad.
- Presentar un informe con los hallazgos y las oportunidades de mejora.

5. HALLAZGOS DE AUDITORÍA

Como resultado de la evaluación sobre plataformas Olympus, Cobra y Temis, para la selección de controles generales de TI, gestión de cambios y controles automáticos, se identificaron los siguientes hallazgos:

5.1. Evaluación de controles generales de tecnología

5.1.1. Ausencia de DRP

Durante la revisión, se identificó que actualmente CISA no cuenta con un Plan de Recuperación de Desastres (DRP), ni se han establecido medidas formales para mitigar el impacto de un evento de desastre mayor, que pudiera afectar la disponibilidad de la tecnología asociada a los procesos críticos de negocio de la entidad.

5.1.2. Inconsistencias en la externalización de copias de respaldo

Para validar la efectividad del control de externalización de medios que tiene CISA, se generó una muestra de cinco semanas del 2016 y se solicitaron las evidencias para verificar que las copias de respaldo que toma la entidad, son enviadas a custodia externa oportunamente. Sin embargo, se evidenció lo siguiente:

a. El backup de la semana 51, la cual iba del lunes 19 al domingo 25 de diciembre de 2016, se envió a custodia externa hasta el 17 de enero de 2017, puesto que el funcionario encargado del proceso se encontraba en periodo de vacaciones.
b. Para el backup de la semana 30, la cual iba del lunes 25 al domingo 31 de julio de 2016, obtuvimos una remesa con fecha errada y que no tenía la relación de cintas. Posteriormente, evidenciamos en la herramienta del proveedor la relación de cintas enviadas, por lo que pudimos concluir que la cinta fue enviada según la frecuencia establecida, pero se presentó un error en el diligenciamiento del formato interno que ha establecido el área de TI

La *circular normativa 093 Politica y procedimiento de infraestructura tecnológica* establece en el numeral *5.10 Políticas de generación y restauración de backup* que la información almacenada en las copias de seguridad realizadas debe estar disponible a las personas autorizadas para ello en el momento en que se necesite y de acuerdo con los niveles de servicio establecidos.

5.1.3. Falta de evidencia para la restauración de copias de respaldo

Durante la evaluación a los controles de restauración de copias de respaldo, se generó una muestra de dos meses para los cuales se solicitaron las evidencias de las pruebas de restauración para las aplicaciones Cobra, Temis y Olympus. Como resultado identificamos que para la restauración de Cobra del mes de febrero de 2016 no se cuenta con evidencia que permita verificar que el proceso se llevó a cabo de manera exitosa, en razón a que los pantallazos del motor de base de datos no muestran el resultado final de la restauración realizada. Para los demás casos si se obtuvieron dichas evidencias.

La *circular normativa 093 Politica y procedimiento de infraestructura tecnológica* establece en el numeral *5.10 Políticas de generación y restauración de backup* que cita: (…) *“el proceso de infraestructura tecnológica deberá cumplir con el plan de restauración de copias de seguridad para asegurar la confiabilidad en caso de emergencia y el no deterioro de los dispositivos y los medios de almacenamiento”.*

5.1.4. Controles ambientales del centro de cómputo

Se realizó una visita al centro de cómputo principal de CISA, identificando las siguientes inconsistencias en los controles ambientales:

- No se realiza mantenimiento al techo falso del centro de cómputo.
- No existe un sistema de extinción automático de incendios
- El material del techo falso no es ignifugo
- No se realizan arqueos de medios magnéticos.

La *circular normativa 093 Politica y procedimiento de infraestructura tecnológica* establece en el numeral *5.2.1. Áreas seguras* que teniendo en cuenta que el centro de cómputo resguarda información operativa de CISA, es necesario que dicho lugar conserve un nivel de seguridad física y ambiental adecuado.

Adicionalmente, en el numeral *5.2.4 Mantenimiento preventivo y correctivo* establece que *"todos los equipos necesarios para el adecuado funcionamiento tanto del centro de cómputo como de los centros de cableado deberán estar amparados con contratos de mantenimiento preventivo y correctivo."*

"Dicha programación anual de mantenimiento debe realizarse sobre los equipos de cómputo, los controles ambientales y de protección contra fuego, detección de humedad, plantas eléctricas, UPS, entre otros".

5.2. Evaluación del proceso de desarrollo y mantenimiento de aplicaciones

5.2.1. Control de cambios en aplicación

Durante la evaluación del control de cambios en aplicación, se generó una muestra aleatoria de 15 fechas de objetos modificados entre enero y diciembre de 2016 mediante la tabla sysobjects (desarrollos) para las aplicaciones Olympus, Temis y Cobra para verificar que el proceso de gestión de cambios se llevó a cabo de acuerdo con lo establecido en la Circular 093.

Como resultado de esta evaluación se identificó:

a. Para 4 casos, no obtuvimos ningún soporte del cambio. Según lo informado por el jefe de operaciones tecnológicas, no es posible identificar si la modificación registrada en la tabla sysobjects corresponde a un proceso de cambio en la aplicación o al procesamiento normal de la misma. **Ver Anexo 1.**

b. Para 6 casos no se obtuvieron soportes de pruebas de calidad.

c. De acuerdo con lo informado, por criterio técnico del encargado de la jefatura de desarrollo estos cambios no requerían pruebas de calidad, sin embargo, en el procedimento no se encuentra estabelecida excepciones: Radicados: 239064, 223452, 208569, 186994, 210108, 187225.

d. Para 3 casos no fueron entregados soportes de pruebas de calidad y pruebas unitarias (desarrollo). Radicados: 232735, 183734, 232448.co

La circular normativa 093 establece en el numeral 6.7 *"Procedimiento para la gestión de requisitos de software"* en la actividad 10 establece que se deben realizar pruebas de calidad y no se definen excepciones a las solicitudes realizadas.

5.2.2. Control de cambios directos en base de datos

Durante la evaluación del control de cambios directamente sobre los datos (en las bases de datos) se identificó que no se contemplan validaciones por parte del usuario solicitante o del líder del proceso que se ve impactado por el cambio. Así mismo, no se deja evidencia en Zeus de la revisión realizada por la Oficial de Seguridad, donde se verifica que se hayan modificado solo los datos solicitados y no información adicional.

También se identificó que actualmente, CISA no cuenta con un registro del sistema que permita identificar los cambios directos realizados sobre los datos para sus aplicaciones Olympus, Temis y Cobra. Lo anterior no permite que la compañía puede realizar trazabilidad sobre los cambios efectuados con el fin de garantizar que todos han sido aprobados adecuadamente.

Adicionalmente, verificamos que este proceso se realiza de manera recurrente en CISA, identificando más de 150 modificaciones para 2016 por errores operativos de las áreas de soporte o comercial.

La *circular normativa 093 Politica y procedimiento de infraestructura tecnológica* establece en el numeral 6.1 Procedimiento para solicitar modificación o adición de información en bases de datos que el usuario responsable debe analizar y validar la solicitud de cambio.

5.3. Evaluación a los controles automáticos de Cobra, Olympus y Temis

5.3.1. Usuarios no autorizados con acceso a transacciones críticas en Cobra

Durante nuestra revisión, obtuvimos el archivo de conformación de perfiles generado desde la base de datos, en donde para una muestra de controles automáticos del sistema, se identificaron los perfiles con permisos para ejecutar actividades críticas de

Cobra. Esta identificación de perfiles se realizó comparando los nombres de los menús con los nombres de los menús en la base de datos, ya que los nombres no son iguales en todos los casos. Posteriormente, se obtuvo el listado de usuarios de la aplicación, para identificar que personal tenía asignado dichas actividades (menús). Como resultado de la revisión se identificó*:

a. Siete usuarios quienes previa conciliación, pueden modificar los porcentajes de compra y capital de las aplicaciones, de los cuales:
   - Tres usuarios no se encuentran autorizados.
   - No se obtuvo respuesta de validación para tres usuarios.
   - Un usuario se encuentra autorizado. **Ver Anexo: 2**

b. Ocho usuarios con acceso a actualizar saldos en la aplicación, de los cuales:
   - Cuatro usuarios no se encuentran autorizados
   - No se obtuvo respuesta de validación para cuatro usuarios.**Ver Anexo: 3**

c. Cinco usuarios con acceso a modificar la asignación del portafolio de obligaciones, sin embargo, no se obtuvo validación de si estos usuarios se encontraban autorizados. **Ver Anexo: 4**

d. Se identificaron 198 usuarios con acceso a actualizar información de los clientes, de los cuales:
   - Usuarios no autorizados: 27
   - Usuarios autorizados: 53
   - No pertenecen al proceso: 2
   - No pertenece a la sucursal: 1
   - No trabaja en CISA: 1
   - No obtuvimos validación de 114 usuarios. **Ver Anexo: 5**

e. Se identificaron 153 usuarios que pueden gestionar y convocar miembros del comité, de los cuales:
   - Usuarios no autorizados: 34
   - Usuarios autorizados: 22
   - No pertenecen al proceso: 2
   - No pertenece a la sucursal: 1
   - No trabaja en CISA: 1
   - No obtuvimos validación de 93 usuarios **Ver Anexo: 6**

f. Se identificaron dos usuarios con perfil de administrador que pueden crear obligaciones en cobra, sin embargo, no se obtuvo la validación de si estos eran usuarios autorizados. Los usuarios son: Diana Judith Guzman y Sandro Jorge Bernal que se encuentran a cargo de Edgar Guzman.

(*) Las personas con las que se validaron los usuarios se encuentran relacionadas en cada uno de los anexos.

La *circular normativa 093 Politica y procedimiento de infraestructura tecnológica* establece en el numeral *5.1.2.1 Politica de control de acceso* que durante el proceso de autorización de cuentas y permisos a los sistemas de información de CISA se debe validar que el usuario requiera permisos acorde al desarrollo de sus funciones.

Adicionalmente, establece que se realice una revisión periódica de los permisos de acceso de las cuentas de los funcionarios a las diferentes aplicaciones o cuando se reporte alguna novedad o movimiento en alguno de los procesos de CISA con el apoyo del Proceso de Gestion del Talento Humano.

5.3.2. Usuarios no autorizados con acceso a transacciones críticas en Temis -

Durante nuestra revisión, obtuvimos el archivo de conformación de perfiles generado desde la base de datos, en donde para una muestra de controles automáticos del sistema, se identificaron los perfiles con permisos para ejecutar actividades críticas de Temis. Esta identificación de perfiles se realizó comparando los nombres de los menús con los nombres de los menús en la base de datos, ya que los nombres no son iguales en todos los casos. Posteriormente, se obtuvo el listado de usuarios de la aplicación, para identificar que personal tenía asignado dichas actividades (menús). Como resultado de la revisión se identificó*:

a. Se identificaron 27 usuarios con acceso a realizar modificaciones a los procesos radicados en Temis, de los cuales:
   - Usuarios no autorizados: 7
   - Usuarios autorizados: 13
   - Usuarios retirados: 1
   - No se obtuvo la validación de 6 usuarios **Ver Anexo: 7**

b. Se identificaron 6 usuarios con acceso a ingresar información a los procesos de Temis, de los cuales:
   - Usuarios autorizados: 4
   - No se obtuvo la validación de un usuario
   - Usuarios retirados: 1 **Ver Anexo: 8**

(*) Las personas con las que se validaron los usuarios se encuentran relacionadas en cada uno de los anexos.

La *circular normativa 093 Política y procedimiento de infraestructura tecnológica* establece en el numeral *5.1.2.1 Política de control de acceso* que durante el proceso de autorización de cuentas y permisos a los sistemas de información de CISA se debe validar que el usuario requiera permisos acordes al desarrollo de sus funciones.

Adicionalmente, establece que se realice una revisión periódica de los permisos de acceso de las cuentas de los funcionarios a las diferentes aplicaciones o cuando se reporte alguna novedad o movimiento en alguno de los procesos de CISA con el apoyo del Proceso de Gestion del Talento Humano.

5.3.3. Usuarios no autorizados con acceso a transacciones críticas en Olympus

Durante nuestra revisión, obtuvimos el archivo de conformación de perfiles generado desde la base de datos, en donde para una muestra de controles automáticos del sistema, se identificaron los perfiles con permisos para ejecutar actividades críticas de Olympus. Esta identificación de perfiles se realizó comparando los nombres de los menús con los nombres de los menús en la base de datos, ya que los nombres no son iguales en todos los casos. Posteriormente, se obtuvo el listado de usuarios de la aplicación, para identificar que personal tenía asignado dichas actividades (menús). Como resultado de la revisión se identificó*:

a. Se identificaron dos usuarios que pueden crear nuevos inmuebles en Olympus, sin embargo, no obtuvimos respuesta a la validación con el fin de identificar si estos se encontraban autorizados para esta tarea:

Nombre	Perfil	Jefe
Luz Angela Lopez	Administrador	Nubia Correa
Maria Fernanda Cáceres	Administrador	Nubia Correa

b. Se identificaron dos usuarios que pueden crear porcentajes de propiedad de los inmuebles de CISA, sin embargo, no obtuvimos respuesta a la validación con el fin de identificar si estos se encontraban autorizados para esta tarea:

Nombre	Perfil	Jefe
Luz Angela Lopez	Administrador	Nubia Correa
Maria Fernanda Cáceres	Administrador	Nubia Correa

c. Se identificaron 21 usuarios con acceso a crear cargos administrativos a los inmuebles de CISA, de los cuales:
   - Usuarios no autorizados: 3
   - Usuarios autorizados: 7
   - No se obtuvo la validación de 11 usuarios **Ver anexo 9**.

d. Se identificaron 22 con acceso a cargar avalúos de los inmuebles de CISA, de los cuales:
   - Usuarios no autorizados: 3
   - Usuarios autorizados: 7
   - Sin respuesta: 12 – **Ver Anexo 10**

e. Se identificaron 22 usuarios con acceso a liquidar inmuebles de CISA, de los cuales:
   - Usuarios no autorizados: 3
   - Usuarios autorizados: 7
   - Sin respuesta: 12 **Ver Anexo 11**

(*) Las personas con las que se validaron los usuarios se encuentran relacionadas en cada uno de los anexos.

La *circular normativa 093 Política y procedimiento de infraestructura tecnológica* establece en el numeral *5.1.2.1 Política de control de acceso* que durante el proceso de autorización de cuentas y permisos a los sistemas de información de CISA se debe validar que el usuario requiera permisos acordes al desarrollo de sus funciones.

Adicionalmente, establece que se realice una revisión periódica de los permisos de acceso de las cuentas de los funcionarios a las diferentes aplicaciones o cuando se reporte alguna novedad o movimiento en alguno de los procesos de CISA con el apoyo del Proceso de Gestion del Talento Humano.

6. OBSERVACIONES

6.1. Autorización en las solicitudes de creación de usuarios

Durante la evaluación al proceso de creación de usuarios, se generó una muestra de dos usuarios creados en 2016 en Temis, Olympus y Cobra para verificar que el proceso de aprovisionamiento de usuarios se realizó de acuerdo con lo establecido en la Circular 093. Como resultado se identificó una inconsistencia en el proceso de creación de la funcionaria Olga Orellano ya que se evidenció que la aprobación del jefe inmediato fue realizada por la misma usuaria que requería el acceso.

Si bien, se contaba con autorizaciones adicionales de acuerdo con el procedimiento, lo anterior, permite identificar que hubo un incumplimiento a las políticas de la entidad las cuales indican que las solicitudes de asignación de privilegios deben ser aprobadas por el jefe inmediato del usuario que requiere el acceso. Adicionalmente, esta situación genera un conflicto de segregación de funciones, ya que no es adecuado que sea el mismo usuario solicitante quien realice la autorización de su acceso.

6.2. Falta de trazabilidad en el control de acceso al centro de cómputo

Se observó que para el control de acceso físico del centro de cómputo se cuenta con dos puertas, en donde la primera puerta tiene un sistema de alerta para el ingreso de funcionarios autorizados por medio de código.

Adicionalmente, se observó que el sistema de control de acceso biométrico al centro de cómputo principal de CISA (puerta dos), no permite identificar que funcionarios tienen privilegios de acceso a este, Este sistema fue implementado hace varios años y no cuenta con una interfaz que permita realizar la administración de estos usuarios, por lo que no es posible saber que usuarios han sido creados, ni tener un registro automático de sus ingresos por medio del dispositivo biométrico.

6.3. Controles generales de tecnología

6.3.1. Inconsistencias de seguridad en la configuración de las bases de datos

Durante nuestra revisión, observamos que CISA no ha definido estándares de seguridad detallados donde se establezca la configuración que deben tener las bases de datos que soportan la operación de la entidad.

Adicionalmente, se realizó una evaluación a la configuración de seguridad de las instancias de la base de datos “Local”, que contiene la información de las aplicaciones Olympus, Temis, “CISAUNO” y Cobra contra las buenas prácticas de seguridad establecidas por el proveedor de SQL y se identificó lo siguiente:

Todos los procedimientos almacenados, vistas y triggers, se encuentran sin cifrar. Ante una eventual intrusión a la base de datos, esta información estaría totalmente visible. De acuerdo con lo informado no es posible hacerlo por estructura de la base de datos.

6.3.2. Inconsistencias de seguridad en los sistemas operativos de los servidores de aplicación y base de datos

Durante nuestra revisión, observamos que CISA no cuenta con estándares de seguridad detallados donde se establezca la configuración que deben tener los sistemas operativos de los servidores que soportan las aplicaciones de la compañía.

Adicionalmente, se realizó una evaluación a la configuración del sistema operativo del servidor de aplicaciones Prometeo, en el que se encuentran las aplicaciones del alcance (Olympus, Cobra y Temis) y al sistema operativo del servidor de base de datos MDBServer, donde se encuentran las instancias que local y cisauno contra las buenas prácticas del fabricante Microsoft, observando que:

a. La cuenta “Invitado” se encuentra activa en Prometeo.
b. Las cuentas “Administrador” no han sido renombradas
c. El grupo “Todos” que cuenta con acceso a las carpetas compartidas del servidor, no requiere dichos permisos de acceso.

d. Las políticas de auditoria están deshabilitadas:

Evento	Valor actual Success	Valor actual Failure	Valor recomendado
Audit Account Logon	Not Defined	Not Defined	Success, Failure
Audit Account Manage	Not Defined	Not Defined	Success, Failure
Audit Logon Events	Not defined	Not Defined	Failure
Audit Object Access	Not Defined	Not Defined	Failure
Audit Policy Change	Not Defined	Not Defined	Success, Failure
Audit Privilege Use	Not Defined	Not Defined	Failure
Audit Process Tracking	Not Defined	Not Defined	None
Audit Prometeotem Events	Not Defined	Not Defined	Success, Failure

6.3.3. Ausencia de fecha de creación de usuarios en aplicaciones

Durante nuestra revisión, se observó que las aplicaciones Olympus, Temis y Cobra, no cuentan con mecanismos que permitan identificar la fecha de creación de los usuarios en estas aplicaciones. Lo anterior no permite que la gestión de usuarios y trazabilidad de los mismos se realice de manera eficiente y adecuada.

6.4. Diagnóstico sobre la implementación ISO27001

Como parte del diagnóstico de la implementación de la norma ISO27001 en CISA se observó:

a. Se validaron los documentos de la entidad en los que están definidos los riesgos, amenazas y vulnerabilidades, identificando que la metodología de asociación de riesgos a cada uno de los activos de información está contemplando riesgos de seguridad generales para CISA pero no a partir de un análisis de riesgos sobre los activos de información de la entidad. Lo ideal es que se definan los impactos, amenazas, vulnerabilidades, riesgos y planes de tratamiento para cada activo de información, de manera tal que se dé cubrimiento y respuesta al universo de parejas amenaza- vulnerabilidad que puede afectar cada activo. Adicionalmente se evidenció que la definición de riesgos y planes de tratamiento, no cubren la totalidad de activos de información.
b. No se han definido indicadores que permitan revisar si las clausulas relacionadas con temas de seguridad de la información que se incluyen en los contratos de trabajo, se están cumpliendo por parte de los funcionarios.
c. Se han realizado cuatro auditorías externas contratadas con externos, sin embargo, CISA aún no se ha presentado a una auditoria para certificación.

d. No se han implementado los controles de la norma relacionados con la continuidad de los activos de información y su cambio de requisitos en caso de presentarse una situación de desastre.
e. Se ha definido un comité de seguridad de la información que es la máxima autoridad del SGSI, sin embargo, no hay evidencia formal de las actividades que debe llevar a cabo este comité dentro del ciclo PHVA, de acuerdo con lo definido en el anexo 22 del manual 13.

CISA no tiene como objetivo a corto plazo certificarse en la norma técnica ISO27001 pese a llevar más de 16 meses en la implementación de la misma y más de 4 años desde que se dio la iniciativa como resultado de la consultoría que recomendó la implementación de la norma.

De otra parte no se ha realizado un análisis costo-beneficio que permita determinar el costo de las auditorías realizadas frente a beneficio obtenido con las actividades relacionadas a la implementación de la norma.

6.5. Evaluación del proceso de desarrollo y mantenimiento de aplicaciones

6.5.1. Diseño de los procedimientos de gestión de cambios

a. Se identificó que actualmente no se deja una evidencia formal (actas o similar) de las reuniones realizadas semanalmente por parte del Comité Asesor de Cambios (CAB) donde se plasmen las situaciones comentadas, decisiones tomadas y que permita verificar que los cambios que fueron tratados y que efectivamente asistieron las personas requeridas, por lo anterior se sugiere crear un documento en donde se aplique lo mencionado.
b. Se observó que no se contaba con evidencia formal de la tipificación de los cambios, donde se pudiera identificar los criterios formalmente definidos para determinar cuando los cambios eran críticos o programados y el análisis realizado por el área de TI determinar lo anterior, sin embargo, evidenciamos que esta catalogación se encuentra alineada a la afectación en la operación de la entidad.
c. De acuerdo con lo indicado en la Circular 093 para algunos casos se requiere la validación de los casos de pruebas asociados al cambio por parte del usuario solicitante. Lo anterior implica que no para todos los casos solicitan pruebas de usuario antes de la puesta en producción de los cambios, de acuerdo a lo anterior se sugiere realizar una mejora en la Circular 093 con el fin de definir aquellos casos en donde aplique la validación de los cambios por los usuarios funcionales.

6.5.2. Fábrica de software

De acuerdo con la revisión realizada a la fábrica de software de CISA, se identificarón las siguientes debilidades:

a. No se generan estadísticas y reportes formales para medir la efectividad del área de desarrollo. Lo anterior implica que no se tienen datos formales que permitan medir si las horas estimadas para un requerimiento son las horas reales incurridas.

b. No se encuentran documentados formalmente los perfiles y opciones que se han definido en las aplicaciones vendidas por CISA.

c. No se cuenta con documentación formal de la arquitectura, casos de uso, funcionalidades, clases, entre otros que tiene cada aplicación para cada cliente. Debido a esta ausencia formal de documentación en ocasiones los ingenieros deben invertir mucho tiempo para identificar cuál debe ser la funcionalidad a modificar cuando un cliente realiza un requerimiento.

d. Como parte de la entrega del software no se realiza la entrega de manuales de usuario o similar

6.5.3. Aplicación de la metodología Scrum para el área de desarrollo

De acuerdo con lo informado, desde 2017 el área de desarrollo ha adoptado la metodología SCRUM para el mantenimiento y soporte de las aplicaciones que CISA ha comercializado, en nuestra revisión se identificó que el área cuenta con 13 recursos, entre los cuales se rota la ejecución de tareas de arquitectura, desarrollo y pruebas de los diferentes requerimientos; en la actualidad la metodología no se está aplicando teniendo en cuenta las tareas pendientes de cada proyecto/cliente (product backlog) sino que se tiene un listado de proyectos de desarrollo pendientes que son asignadas al personal.

Lo anterior ha permitido que el área genere entregas agiles de los desarrollos cada tres semanas, pero no entregas basadas en iteraciones por proyecto ejecutadas en un periodo de tiempo definido (Sprint) que es lo que sugiere la metodología.

Adicionalmente, la reunión definida en la metodología (Scrum team meeting) para evaluar las entregas críticas, problemas presentados o similar, se realiza cada semana y no diariamente como está definida metodológicamente.

De otra parte frente a la documentación de la metodología de desarrollo implementada por el área de desarrollo es importante que se cuente con documentación formal donde se indique

los pasos, tareas y evidencias de cada una de las etapas que se siguen de la metodología acogida para poder realizar una trazabilidad adecuada del cumplimiento de la misma y seguimiento de los objetivos definidos.

6.6. Evaluación a los controles automáticos de Cobra, Olympus y Temis

6.6.1. Asignación y conformación de perfiles en las aplicaciones

Durante nuestra revisión, evidenciamos que actualmente en las aplicaciones Cobra, Olympus y Temis no es posible obtener información desde el sistema de las transacciones o menús que confirman cada perfil definido, debido a:

a. No es posible identificar en el listado generado desde IMC, a que menús tiene acceso cada uno de los perfiles, ya que la descripción de las opciones en el listado, no es igual, a la descripción de los menús en los sistemas. Durante nuestra revisión no fue posible obtener reportes generados desde las aplicaciones de los menús y/o permisos que conforman cada perfil.
b. Identificamos que la asignación de permisos se da a través de perfiles, sin embargo, estos perfiles se han ido personalizando para cada usuario de acuerdo con sus necesidades. Por lo anterior, aunque un funcionario cuente con un perfil determinado, puede tener acceso a otros menús que no hacen parte de dicho perfil. Esto genera un problema operativo para la administración de usuarios e inconvenientes en la trazabilidad de los mismos.

6.6.2. Cargue de pagos de usuarios en Cobra

Durante nuestra revisión, identificamos que actualmente el proceso de cargue de pagos de usuarios en la aplicación Cobra se realiza mediante una interfaz manual. Para realizar este proceso, se descarga un reporte de los portales bancarios, el cual viene en formato de texto claro, sin ningún tipo de cifrado, y se guarda en una carpeta compartida del área* para ser modificado antes de ser cargado a Cobra. Según lo informado para ser cargado en Cobra se requiere modificar la estructura del archivo.

Actualmente no se cuentan con controles adicionales que permitan asegurar que la información que se carga en Cobra, no presenta modificaciones no autorizadas y corresponda a la que fue descargada de los portales bancarios.

(*) La ruta donde se está almacenando el reporte es la siguiente: Vice_Financiera_y_Administrativa/G_Contable_y_Operativa/Tesoreria/CI1D1_RECAUDOS/REC BANCOLOMBIA/RIN/ENVIADOS A OPERACIONES.

7. RECOMENDACIONES

7.1. Ausencia de un plan DRP

Diseñar, implementar, probar y difundir un DRP el cual se ajuste y responda a las necesidades y objetivos de CISA considerando previamente la selección de procesos críticos por parte de la entidad mediante la ejecución de análisis de impacto al negocio para posteriormente identificar las plataformas y requerimientos tecnológicos asociados a dichos procesos.

Se recomienda que el DRP contemple al menos los siguientes aspectos:

a. Gobierno: roles y responsabilidades definidas para la administración del DRP involucrando a la alta gerencia.
b. Asociación de las plataformas y requerimientos tecnológicos acorde con la definición de los procesos críticos para continuidad del negocio de CISA de acuerdo con unos criterios estratégicos y con evaluación de su impacto en la operación en caso de no estar disponibles.
c. Análisis de riesgos de tecnología.
d. Asociación con los resultados de los Análisis de impacto al negocio, donde se identifique para la tecnología relacionada con cada proceso crítico lo siguiente: tiempo objetivo de recuperación (RTO) y punto objetivo de recuperación (RPO).
e. Definición de estrategia de tecnología: acorde con los resultados del análisis de riesgo y análisis de impacto al negocio la organización debe seleccionar e implementar una estrategia de tecnología que permita dar cubrimiento a los aspectos identificados.
f. Definición del plan de recuperación de desastres (DRP) donde se indiquen las acciones antes, durante y después de un evento de desastre o crisis para puesta en marcha de la estrategia de DRP definida.
g. Plan de pruebas: donde se definan pruebas y simulacros controlados de situaciones de desastre para probar la eficiencia del sistema
h. Plan de capacitación y sensibilización del DRP para los empleados y actores involucrados.
i. Mejoramiento y mantenimiento del DRP.

Nota: Para la implementación de un DRP se recomienda llevar a cabo un proceso para el diseño, implementación y pruebas de un plan de continuidad de negocio de manera tal que la entidad determine sus procesos críticos y el impacto en caso de que estos no se encuentren disponibles. Se sugiere considerar estos aspectos para la definición de un DRP con el fin de que este alineado a las necesidades y objetivos del negocio.

7.2. Inconsistencia en la ejecución de copias de respaldo

a. Implementar mecanismos que permitan asegurar que las copias de respaldo se ejecuten con la periodicidad definida en el documento Protección de datos y backups CISA. Este documento no se encuentra formalizado en el sistema integral, por lo que adicionalmente se recomienda su formalización.

b. Teniendo en cuenta que en la actualidad la CISA no cuenta con un plan formal de continuidad de negocio, ni DRP, se recomienda prestar especial atención al proceso de ejecución de copias de respaldo de los sistemas de la compañía, puesto que en la actualidad las copias de respaldo son un activo crítico en caso de una llegar a presentarse una situación de desastre o contingencia.

7.3. Autorización en las solicitudes de creación de usuarios

a. Definir medidas que permitan asegurar que las políticas de la entidad relacionadas con la autorización de solicitudes de creación de usuarios se cumplan sin excepción. No se deberían realizar creaciones de usuario, si no son autorizadas por el personal establecido en la *Circular 093 - Política y procedimiento de infraestructura tecnológica, numeral 5.1.3.*
b. Definir medidas que permitan asegurar que el diligenciamiento de la información en Zeus, relacionada con el jefe inmediato de los funcionarios, sea la indicada por Gestión Humana en el momento que ingresan las personas a la compañía. En caso de no ser diligenciada en el momento del ingreso, el analista de infraestructura debe consultar ante cualquier inconsistencia esta información con Gestión Humana.

7.4. Inconsistencias de seguridad en la configuración de las bases de datos

a. Se sugiere definir un estándar de seguridad para la configuración de las bases de datos que se encuentre alineado a los mejores estándares y donde se contemplen los siguientes aspectos como mínimo:
    - Uso de cuentas por defecto del sistema
    - Uso de cuentas invitado del sistema
    - Controles para la administración del catálogo de tablas
    - Permisos sobre las tablas del sistema
    - Conexiones remotas a la base de datos
    - Eventos de auditoria registrados
    - Métodos de autenticación a la base de datos
    - Asignación de roles críticos
    - Métodos de auditoria

7.5. Inconsistencias de seguridad en los sistemas operativos de los servidores de aplicación y base de datos

a. Documentar y formalizar estándares de seguridad para los sistemas operativos de CISA en los cuales se incluyan todos los parámetros de configuración, indicando los valores óptimos para cada uno dependiendo de los requerimientos de la entidad.
b. Inhabilitar la cuenta invitado en el servidor de aplicaciones Prometo.
c. Evaluar la viabilidad técnica de renombrar la cuenta administrador tanto el servidor Prometeo como en “MDBServer”
d. Evaluar la viabilidad técnica de remover los privilegios de acceso a carpetas compartidas al grupo “Todos” tanto en el servidor “Prometeo” como en “MDBServer”
e. Evaluar la viabilidad de habilitar las políticas de auditoria tanto en el servidor “Prometeo” como en “MDBServer” de acuerdo con los valores recomendados.
f. Los aspectos anteriores deben ser analizados según los requerimientos de negocio y en caso de no implementar alguna de las recomendaciones se recomienda emitir un documento formal con el análisis y su resultado que sea aprobado por la gerencia.

7.6. Ausencia de fecha de creación de usuarios en aplicaciones

Evaluar la viabilidad técnica de implementar un registro que almacene la fecha de creación de los usuarios en las aplicaciones, Olympus, Temis y Cobra, con el fin de poder llevar a cabo la gestión de usuarios y la trazabilidad de su creación, modificación o retiro de acuerdo con las políticas de CISA.

7.7. Controles ambientales del centro de computo

a. Establecer mantenimientos al techo falso, con el fin de verificar periódicamente el estado del mismo. Se debe almacenar la evidencia de los mantenimientos que se realicen.
b. Evaluar la viabilidad de implementar un sistema de extinción automática de incendios dentro del centro de cómputo teniendo en cuenta la criticidad de la información que allí se almacena y que en este momento no hay definido un plan de continuidad y DRP que permita la operación en contingencia del centro de cómputo en caso de una situación de desastre.
c. Evaluar la viabilidad de cambiar el techo del centro de cómputo con material ignífugo.
d. Definir controles para la ejecución de arqueos de medios magnéticos de forma periódica, manteniendo evidencias del resultado de la actividad.
e. Definir un cronograma formal de mantenimientos al centro de cómputo y hacer seguimiento al cumplimiento del mismo.

7.8. Diagnóstico sobre la implementación ISO27001|

a. Evaluar la viabilidad de realizar un análisis de riesgo sobre los activos de información definidos por CISA, contemplando por cada activo su impacto, vulnerabilidades y amenazas, controles asociados, riesgo inherente y residual, con el fin de establecer planes de tratamiento por cada activo adecuado en el marco de la norma ISO27001.
b. Diseñar e implementar indicadores que permitan evaluar el cumplimiento de las cláusulas de seguridad de la información incluidas en los contratos de trabajo de CISA. Definir un plan de acción para la implementación de los controles de la norma ISO27001 relacionados con la gestión de proveedores y la gestión de dispositivos móvil. Dejar evidencia de las actividades y responsabilidades que son ejecutadas por el comité de seguridad de la información, dentro del ciclo PHVA, según lo establecido en el anexo 22 del manual 13.
c. Evaluar la viabilidad de iniciar una auditoría de certificación de la norma ISO/IEC 27001:2013, teniendo en cuenta el esfuerzo y tiempo dedicado a la implementación de la misma en el proceso de infraestructura tecnológica. Es necesario asegurar para este proceso, que la Alta Dirección apruebe la documentación y las actividades que se llevan a cabo para la implementación de la norma.

7.9. Diseño de los procedimientos de gestión de cambios

a. Establecer criterios formales para la tipificación de los cambios con el fin de realizar la debida gestión a través de la herramienta ZEUS de acuerdo con las necesidades del negocio. Así mismo, se sugiere que dicha evaluación y determinación del tipo de cambio se realice en conjunto con personal del área de TI y se deje evidencia de ello.

b. Considerar la posibilidad de implementar un acta con el fin de llevar un registro formal de la asistencia y toma de decisiones del Comité Asesor de Cambios (CAB).

c. Considerar la ejecución de pruebas por parte de los usuarios solicitantes para todos los cambios con el fin de que se verifique la adecuada modificación, que esta cumpla con lo requerido por el usuario y que no afecte otras funcionalidades de la aplicación, antes de su puesta a producción.

7.10. Control de cambios en aplicación

a. Considerar incluir en los procedimientos de control de cambios las excepciones relacionadas con la ejecución de pruebas de desarrollo y calidad de los radicados.

b. Implementar mecanismos que permitan identificar directamente en las aplicaciones Cobra, Olympus y Temis, todos los cambios que se realicen a estas aplicaciones, con el fin de poder realizar una adecuada trazabilidad y control de todas las modificaciones a las cuales son sometidas las aplicaciones.
c. Realizar una evaluación y revisión detallada de las fechas y objetos modificados para los cuales no se cuenta con soportes, con el fin de verificar que dichas modificaciones correspondieron a solicitudes autorizadas y/o actividades autorizadas de mantenimiento o similar.

7.11. Control de cambios directos en base de datos

a. Evaluar la viabilidad técnica, de incluir dentro del flujo de Zeus, evidencia de la validación realizada por la Oficial de Seguridad sobre los cambios realizados a los datos, con el fin de mitigar que se realicen cambios no autorizados a las bases de datos.
b. Evaluar la viabilidad de contar con un registro que permita identificar los cambios directos realizados sobre los datos para las aplicaciones Olympus, Temis y Cobra.
c. Es importante tener en cuenta que la modificación directa de datos es un proceso que genera el riesgo de modificación no autorizada o errónea de información clave del negocio, por lo que debería usarse lo más mínimo como excepciones claramente definidas.

7.12. Fábrica de software

a. Definir métricas para la fábrica de software con el fin de evaluar su efectividad.
b. Tener documentación formal de los perfiles y sus transacciones para cada proyecto de software.
c. Dejar documentación técnica de cada aplicación personalizada con el fin de dejar un mapa de ruta cuando se requieran ajustes y/o requerimientos sobre el software.
d. Considerar la viabilidad de documentar entregables para los clientes que adquieran los productos de la compañía donde se incluya la guía de uso.
e. Burn down chart: gráfica o estadísticas de los requisitos del backlog del proyecto pendiente al comienzo de cada sprint. Esto permite ver el progreso de cada proyecto.

7.13. Evaluación a los controles automáticos de Cobra, Olympus y Temis - Asignación y conformación de perfiles en las aplicaciones

a. Evaluar la viabilidad de implementar en Cobra, Olympus y Temis un reporte que liste los menús y permisos que tiene definido cada perfil. Es necesario que para

dicho reporte se realicé una homologación de los nombres de los menús de las aplicaciones versus el nombre dado a nivel de código para garantizar coherencia.

b. Para los casos en los que los perfiles no sean estándar y se hayan personalizado, se sugiere evaluar en conjunto con las áreas usuarias, la viabilidad de modificar los perfiles, con el fin de asegurar que cada perfil tenga asociadas funciones específicas para cada función y no presenten conflictos de segregación de funciones. Se recomienda definir perfiles estándar para cada aplicación según las funciones de cada proceso y que las transacciones o accesos de estos perfiles no se modifiquen. En caso de que sea necesario por alguna excepción que un usuario requiere algún menú adicional, este cambio sea aprobado formalmente por el líder del área y la oficial de seguridad y que quede debidamente documentada esta excepción para su posterior gestión.
c. Una vez realizadas las tareas anteriores, se recomienda realizar una revisión de perfiles con los jefes de área, enviando por cada funcionario los menús y permisos asociados para que los jefes verifiquen que sus empleados cuentan con acceso únicamente a los menús que requieren por sus funciones y eliminar cualquier posible conflicto de segregación de funciones.

7.14. Cargue de pagos de usuarios en Cobra

a. Evaluar la posibilidad de implementar mecanismos de cifrado al archivo que es descargado de los portales bancarios para evitar modificaciones no autorizadas. Si no es viable, definir e implementar controles de revisión posteriores al cargue del archivo en Cobra, de forma que otra persona verifique la integridad de la información con respecto a la de los portales bancarios.
b. Revisar los usuarios que cuentan con acceso a la ruta donde es guardado el archivo de pagos y asegurar que solamente correspondan a usuarios autorizados, que requieran tener acceso a esta información para el desarrollo de sus funciones.

7.15. Usuarios no autorizados con acceso a transacciones críticas en Cobra – Temis – Olympus

a. Eliminar los permisos de los usuarios no autorizados que tienen acceso a las actividades mencionadas y eliminar aquellos usuarios que corresponden a personal retirado de la compañía.
b. Revisar los usuarios para los cuales no se obtuvo validación, con el fin de verificar si deben contar con acceso a las actividades mencionadas, de acuerdo con las funciones que desempeñan en la compañía.
c. Se sugiere que cuando se presenten reingresos o cambios de área, se ejecute el proceso de gestión de usuarios, verificando que se eliminen los permisos anteriores

y se creen los nuevos, no únicamente que se reactive el usuario y se sumen nuevos permisos.

d. El dueño del proceso, debe realizar revisiones periódicas de los usuarios con acceso a Cobra, con el fin de asegurar que solamente tengan acceso a estas actividades, personal que lo requiera para el desempeño de sus funciones.

7.16. Plan de Mejoramiento

Suscribir Plan de Mejoramiento que incluya los temas que ameritan adoptar acciones correctivas, dentro de los siguientes diez (10) días hábiles siguientes a la fecha de recibo del informe definitivo de acuerdo con el Anexo *"Plan de Mejoramiento por Procesos."* De la circular normativa 017.

8. CONCLUSIÓN DE AUDITORÍA

De la evaluación realizada al Proceso de Infraestructura Tecnológica, se puede concluir que el proceso en general está realizando sus actividades de manera controlada de acuerdo con lo establecido en la Circular Normativa 093, no obstante presenta hallazgos y oportunidades de mejora relacionadas con la evidencia de los controles, trazabilidad sobre la gestión de usuarios y cambios y definiciones de estándares de seguridad sobre sus plataformas, como se describe en los numerales 5 y 6 del presente informe.

Así mismo, se identificaron dos temas relevantes que generan riesgos significativos que deben ser evaluados por la entidad para su análisis e implementación de acciones de mejora. El primer punto corresponde a la ausencia de un plan formal DRP (acompañado además de un plan de continuidad), en donde se definan claramente las acciones tendientes a recuperar y volver a operación normal en caso de un evento de desastre que genere la no disponibilidad de la tecnología de la compañía. Esta situación genera un riesgo de no disponibilidad de la información y soporte tecnológico para soportar los procesos y operación de CISA y que la información contable y financiera no pueda ser recuperada cuando se presente una pérdida de datos.

También concluimos que la gestión para la asignación y conformación de perfiles en las aplicaciones, evidenciamos que actualmente en las aplicaciones Cobra, Olympus y Temis que no es posible obtener reportes generados desde las aplicaciones de los menús y/o permisos que conforman cada perfil; adicional se observó que la asignación de permisos se da a través de perfiles, sin embargo, existen perfiles personalizados para cada usuario de acuerdo a sus necesidades. Esto genera un riesgo de usuarios con privilegios más allá de los necesarios para realizar las actividades asignadas y/o concentración inadecuada de privilegios por no modificación de los perfiles en los sistemas de información. De acuerdo a lo

anterior, se sugiere abordar un proyecto de evaluación y segregación de funciones en donde se contemplen los accesos en los sistemas por los usuarios teniendo en cuenta los requerimientos basados en sus funciones dentro de los diferentes procesos en la entidad, con el fin de mejorar la administración de usuarios y evitar inconvenientes en la trazabilidad y asignación de responsabilidades de los mismos.

Es importante resaltar la cordialidad, disponibilidad y atención prestada por los servidores públicos del proceso auditado, mostrando un alto grado de responsabilidad frente a la cultura del control.

9. MESA DE TRABAJO

Se realizó mesa de trabajo con la participación del Responsable del proceso, Doctor Sergio moreno y el ingeniero Omar Ardila, de acuerdo con lo indicado en el Acta de mesa de trabajo adjunta al presente informe.

Aprobado por:	Elaborado por:	Fecha aprobación
ORIGINAL FIRMADO **ELKIN ORLANDO ANGEL MUÑOZ** Auditor Interno	ORIGINAL FIRMADO **LUISA FERNANDA DIAZ** Gerente Deloitte	18/08/2017