POR FAVOR AL CONTESTAR CITE EL No. DEL RADICADO
IPES - Correspondencia Administrativa- INTERNAS
Radicado: 00110-817- 005100
Fecha: 20/08/2021 - 05:50 PM
Remitente: CARMEN ELENA BERNAL ANDRADE
Destinatario: FATIMA VERONICA QUINTERO NUÑEZ
No.Folios: 3 Anexos: 67

MEMORANDO

110301

Bogotá DC.,

PARA: FÁTIMA VERÓNICA QUINTERO NÚÑEZ, Subdirección de Diseño y Análisis Estratégico

DE: CARMEN ELENA BERNAL ANDRADE, Asesora de Control Interno

ASUNTO: Informe Final de Auditoría

Respetada doctora:

En el marco del Sistema de Control Interno se ha de tener en cuenta lo establecido por la Ley 87 de 1993 en cuanto a quiénes son los responsables de la implementación de un sistema de control interno en las entidades del Estado:

> *"**ARTÍCULO 6º. Responsabilidad del control interno.** El establecimiento y desarrollo del Sistema de Control Interno en los organismos y entidades públicas, será responsabilidad del representante legal o máximo directivo correspondiente. No obstante, la aplicación de los métodos y procedimientos al igual que la calidad, eficiencia y eficacia del control interno, también será de responsabilidad de los jefes de cada una de las distintas dependencias de las entidades y organismos".* Subrayas fuera de texto.

Aunado a lo anterior, se contempla en el Manual Operativo del Decreto 1499 de 2017, que articula los Sistemas Integrados de Gestión y de Control Interno, específicamente en la séptima dimensión del MIPG, el Control Interno[1], contempla cinco componentes de la estructura del MECI: 1) Ambiente de Control, 2) Evaluación del Riesgo, 3) Actividades de Control, 4) Información y Comunicación, y 5) Actividades de Monitoreo[2].

En este sentido la Asesoría de Control Interno, entregó a la Administración del IPES los resultados de la Auditoría Interna Regular al proceso de apoyo: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS, a través de

[1] Tal como lo establece la Ley 87 de 1993, el Control Interno está integrado por el esquema de organización y el conjunto de planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y de los recursos, se lleven a cabo de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la alta dirección y en atención a las metas u objetivos previstos.
[2] Manual Operativo MIPG Departamento Administrativo de la Función Pública.

Calle 73 N° 11-66
PBX. (+57) 2976030
Línea Gratuita
018000124737
www.ipes.gov.co

la socialización de observaciones con los auditados el pasado 29-jul-2021 y la entrega de un informe preliminar para réplicas con radicado 00110-817-004826 del 10-ago-2021 y finalmente, así como una reunión de cierre de auditoría regular realizada el 19-ago-2021. Se remite el informe de cierre (detallado) de auditoría con el presente oficio.

Una vez radicado el Informe Final, en el Archivo Excel "PV01-FO-015 V2 PLAN DE MEJORAMIENTO AUDITORIAS INTERNAS" el cual se encuentra publicado en SIG MIPS, la Subdirección de Diseño y análisis Estratégico, junto con los responsables de los procesos auditados, deben suscribir un Plan de Mejoramiento relacionando la causa raíz de cada observación, las acciones de mejora que mitiguen la causa raíz, los tiempos, responsables y los resultados entregables, para lo cual tiene 8 días hábiles a partir de la fecha de radicación de este Informe Final. De manera posterior, se suscribirá en el aplicativo CHIE.

Con el fin de cumplir con el objetivo de la mejora continua de los procesos y conscientes de la importancia de formular acciones de mejora efectivas para la mitigación de riesgos del proceso, para cumplir con los términos establecidos, desde la Asesoría de Control Interno se propone la realización de 2 mesas de trabajo virtuales para acompañamiento, en las siguientes fechas:

Mesa 1:
Miércoles, 25 de agosto · 2:00 – 2:45pm
Información para unirse a Google Meet
Enlace a la videollamada: https://meet.google.com/ncz-fadv-xth
O marca el: (CO) +57 1 8956954 PIN: 924 624 907#
Más números de teléfono: https://tel.meet/ncz-fadv-xth?pin=1369553568117

Mesa 2:
Martes, 30 de agosto · 2:00 – 2:45pm
Información para unirse a Google Meet
Enlace a la videollamada: https://meet.google.com/ncz-fadv-xth
O marca el: (CO) +57 1 8956954 PIN: 924 624 907#
Más números de teléfono: https://tel.meet/ncz-fadv-xth?pin=1369553568117

Por lo que agradezco a la SDAE designar a los responsables de la formulación y seguimiento de acciones de mejora, quienes deberán aportar en la primera mesa de trabajo, un primer borrador para retroalimentación por parte del auditor responsable.

Una vez recibido el plan de mejoramiento, se emitirá el informe final (ejecutivo) con destino a la Dirección General.

Calle 73 N° 11-66
PBX. (+57) 2976030
Línea Gratuita
018000124737
www.ipes.gov.co

La Asesoría de Control Interno realizará seguimiento al cumplimiento del Plan de Mejoramiento con el fin de asegurar que hayan sido tomadas las acciones definidas por el auditado y corregidos los hallazgos u observaciones.

Cordialmente,

CARMEN ELENA BERNAL ANDRADE

Anexos: 66 Folios y 1 Carpeta Comprimida con ANEXOS.

Copia:
Doctor JUAN CARLOS REYES ROJAS, Asesor del Despacho del Director General
Doctor JAVIER MORA ANDRADE, Asesor del Despacho del Director General
Doctor OSCAR ALBERTO BARRAGÁN LEÓN, Asesor del Despacho del Director General

	NOMBRE, CARGO O CONTRATO	FIRMA	FECHA
Elaboró	Rafael Eduardo Ortiz Gómez Contratista CO1.PCCNTR.2275626	*Rafael Ortiz*	20-ago-2021
Aprobó	Carmen Elena Bernal Andrade - Asesora de Control Interno	*Carmen Bernal*	
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad, lo presentamos para firma de la ***Asesora de Control Interno*** del Instituto para la Economía Social IPES.			

Calle 73 N° 11-66
PBX. (+57) 2976030
Línea Gratuita 018000124737
www.ipes.gov.co

Tipo de Auditoría	Especial		Regular	X	
Fecha Auditoría	24 de mayo al 30 de julio de 2021				
Dependencia	Subdirección de Diseño y Análisis Estratégico				
Proceso	Gestión de Seguridad de la Información y Recursos Tecnológicos				

Contenido

1. CONTEXTO Y JUSTIFICACIÓN 2
2. OBJETIVO GENERAL 5
2.1. OBJETIVOS ESPECÍFICOS 5
3. ALCANCE 5
2.1 LIMITACIÓN AL ALCANCE 6
4. CONFORMACIÓN EQUIPO DE TRABAJO DE AUDITORÍA 6
5. FORTALEZAS 7
6. CONCLUSIONES 7
7. RESUMEN DE RESULTADOS DE LA AUDITORÍA 8
8. DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA 9
9. PLAN DE MEJORAMIENTO 65
10. ANEXOS 66

INFORME DE CIERRE AUDITORÍA REGULAR
SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO
PROCESO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS

1. CONTEXTO Y JUSTIFICACIÓN

Dentro de las competencias de la Asesoría de Control Interno enmarcadas en la Ley 87 de 1993 está evaluar la eficiencia, eficacia y economía de los controles, asesorando a la Dirección General en la:

a) Continuidad del Proceso Administrativo,
b) Revaluación de los planes establecidos
c) Introducción de los correctivos necesarios para el cumplimiento de las metas y objetivos previstos por la Entidad.

De acuerdo al Plan Anual de la vigencia 2021, la Asesoría de Control Interno programó trabajo a Auditoría Interna Regular, y definió en su Alcance respecto a los procesos y procedimientos que ejecuta la dependencia: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS.

Este trabajo se llevó a cabo entre el 24 de mayo y el 30 de julio del 2021.

Los sistemas de información objeto de la presente auditoría fueron:

- **HEMI (HERRAMIENTA MISIONAL):**

La Herramienta Misional – HeMi es la plataforma tecnológica de información con la cual el IPES soporta su proceso de apoyo misional, registrando y generando la información necesaria para atender y plantear estrategias en la atención integral de nuestros beneficiarios en concordancia con los planes de desarrollo y las políticas trazadas por el Gobierno Distrital.

HEMI ha sido desarrollado por personal del IPES desde el año 2008, está orientado al uso de la Subdirección de Emprendimiento, Servicios Empresariales y Comercialización (SECEC) y de la Subdirección de Gestión de Redes Sociales e Informalidad (SGRSI).

- **GOOBI ERP (SISTEMA ADMINISTRATIVO Y FINANCIERO):**

Es el Sistema Integrado de Información, GOOBI GRP (Gestión de Recursos Públicos). Este Integra todos los procesos y la planeación de recursos de la gestión pública como son:

- Planeación
- Control de Gastos
- Gestión de Ingresos
- Gestión de Contratos
- Gestión Financiera
- Gestión de Personal
- Control de Bienes

GOOBI GRP, es el sistema administrativo utilizado por el IPES para la gestión de los recursos públicos desde hace 15 años (desde el año 2006); esto a partir del momento en el que el Fondo de Ventas Populares en Bogotá, por decreto de gobierno cambió su razón social a Instituto para la Economía Social IPES.

Es un software tercerizado, el cual pertenece al proveedor IT GOP SAS y se utiliza bajo licenciamiento en la entidad - IPES.

Nuevos desarrollos:

- ***Decreto 092 del 2021 (Elecciones de consejo vendedores (as) informales)***

El Instituto para la Economía Social – IPES, desarrolla las elecciones para los Consejos Locales de Vendedores (as) Informales, los cuales serán el máximo órgano representativo del gremio de cada localidad de Bogotá DC y estarán compuestos por los siete (7) integrantes más votados de la localidad representativa con voz y voto. Existirá un (1) consejo de vendedores informales. Su periodo será de 4 años, contados a partir de la instalación por parte del alcalde Local.

Con el propósito de garantizar la adecuada y efectiva participación de la mujer, cada Consejo Local debe estar compuesto como mínimo por cuatro (4) vendedoras informales.

El 31 de julio de 2020, el Instituto Distrital de Participación y Acción Comunal (IDPAC) lanza el Sistema de Votación Electrónica Ciudadana (VOTEC), una plataforma en la que las ciudadanas y los ciudadanos podrán votar de manera virtual con todas las garantías de transparencia a través de www.participacionbogota.gov.co

El alto nivel de participación de las y los bogotanos, el número de procesos electorales liderado por el IDPAC y la nueva realidad a causa de la COVID – 19, fueron las principales razones que motivaron a la creación de esta herramienta.

El IPES en colaboración con el IDPAC se ha conectado por medio de un *web service,* enviando la información de HEMI para autenticar cuáles candidatos y votantes están registrados en el aplicativo HEMI.

Las opciones que ofrece VOTEC son[1]:

- INSCRIPCIÓN: Los ciudadanos podrán inscribirse como electores o candidatos a los diversos procesos electorales.

- VERIFICAR INSCRIPCIÓN: Ingresando el tipo y número de documento, las personas que se inscribieron previamente como votantes, podrán validar su inscripción al proceso

[1] https://www.participacionbogota.gov.co/idpac-lanza-novedoso-sistema-de-votacion-electronica-ciudadana

democrático. El censo electoral nos ayudará a determinar el porcentaje de votación que tuvimos en la elección.

- POTENCIAL ELECTORAL: Aquí se encontrará el número de personas habilitadas para votar por localidad.

- VOTACIÓN: Los electores deberán ingresar su tipo y número de documento y la contraseña con la que se registraron previamente. (Si las personas olvidaron alguno de estos datos deberán seleccionar “Recuperar código de acceso” inmediatamente recibirán un correo electrónico con la información solicitada).
  Acto seguido se encontrará la lista de los aspirantes, después los electores deberán seleccionar el candidato de su preferencia y finalizar con el botón ‘Votar’.

- RESULTADOS: Aquí se almacenarán los resultados con los ganadores y la respectiva acta de escrutinio, la cual podrá ser descargada por los ciudadanos.

- ESTADÍSTICAS: Se entregarán las estadísticas de las elecciones por localidades, potencial electoral, porcentaje de participación, número de votantes, votos en blanco y cuantas mujeres y hombre votaron.

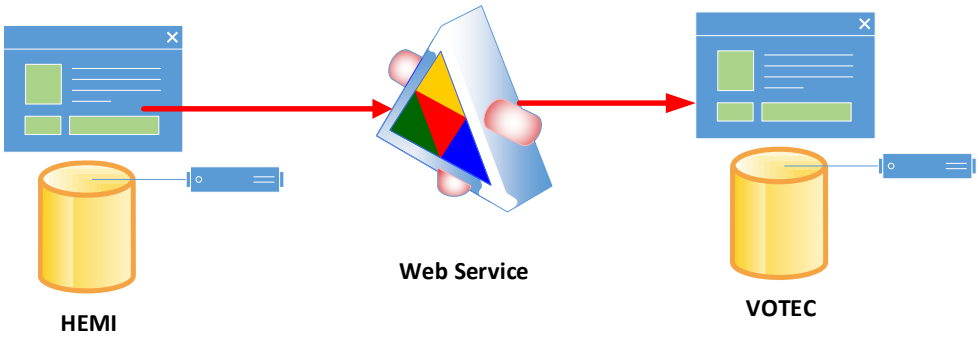


Diagrama I: Conexión de HEMI-VOTEC

La arquitectura de VOTEC es privada y pertenece a IDPAC, la arquitectura de HEMI es:

- ✓ Tipo de Aplicación: Web Enable
- ✓ Tecnología: ASP.NET
- ✓ IDE de Desarrollo: VS2019 Express
- ✓ Pantallas con tecnología AJAX
- ✓ Metodología N-Tier
- ✓ Capa de Presentación
- ✓ Capa de Lógica del Negocio (BLL)
- ✓ Capa de Acceso a Datos (DAL)
- ✓ Capa de Base de Datos (SQL)
- ✓ Bootstrap y Html5 (En proceso de implementación)

Figura 1. Arquitectura de HEMI

Diagrama II: PA08-DE-004 PLAN DE CONTINGENCIA DE TI

Aunque su desarrollo permite *web service* no se encuentra el *web service* ni el contrato *de web service* reflejado en su diagramación.

- ***Software digitalización de plazas de mercado - MARKETPLACE***

El objetivo de este proyecto es dar la posibilidad de que los locatarios de plazas puedan contar con un *e-commerce*, por lo tanto, el IPES se encuentra desarrollando una plataforma de *market place*.

La arquitectura el *frontend reactjs, backend nodejs,* base de datos en PostgreSQL, los servicios están publicados en *Firebase*, el repositorio está en un *Google storage*, el proveedor que desarrolla el software ofrece la infraestructura de desarrollo y pruebas.

En el momento es una solución totalmente independiente del proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos del IPES.

2. OBJETIVO GENERAL

Realizar una evaluación y entregar una opinión independiente sobre el adecuado diseño y ejecución de los controles establecidos para prevenir y mitigar los riesgos existentes en la ejecución de los procesos y procedimientos que se determinen en el alcance de la Auditoría Regular al proceso de apoyo: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS con enfoque de implementación de soluciones lógicas (Aplicaciones, arquitectura y su gestión).

2.1. OBJETIVOS ESPECÍFICOS

2.1.1. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS

- Establecer que los controles diseñados y aplicados son adecuados para la administración y gestión de los riesgos asociados a la planeación y gestión de los sistemas de información misionales HEMI y GOOBI en cuanto a la madurez en: su adquisición, desarrollo, mantenimiento, implementación, implantación y continuidad de la operación.

2.1.2. GESTIÓN CONTRACTUAL

- Determinar si la etapa Contractual, desde la ejecución y supervisión, en los procesos para la adquisición de bienes y servicios objeto de la muestra de auditoría, cumplieron los lineamientos vigentes del Manual de Contratación, Supervisión e Interventoría, si se ajustaron al Estatuto General de Contratación Pública, sus reglamentos y si se observaron los principios orientadores de la contratación administrativa.

3. ALCANCE

El Alcance se determinó como resultado de un análisis de:

- Procesos críticos de relevancia según tamaño del Impacto de Riesgo.
- Nivel de Criticidad (*procesos sin identificación de riegos, carencia de controles, alta rotación de personal, cambio de funciones, procedimientos, eventos recientes, SDQS, etc*.)
- Exposición a eventos externos e internos del Instituto.
- Criterio profesional de los auditores aprobado por la Asesoría de Control Interno.
- Disponibilidad de recurso humano, técnico, financiero, etc.

Por lo anterior, este trabajo incluyó la verificación del cumplimiento a los siguientes procesos y procedimientos ejecutados por GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLOGICOS en la vigencia 2020 hasta abril 2021:

a. *Gestión de Seguridad de la Información y Recursos Tecnológicos*

- PA08-DE-001 Plan Estratégico de Tecnologías de Información
- PA08-DE-002 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- PA08-DE-003 Plan de Seguridad y Privacidad de la Información
- PA08-DE-004 Plan de Contingencia de TI
- MS-013 Manual Seguridad de la Información
- MS-011 Manual del Usuario Herramienta Misional (HEMI)
- MS-010 Manual Técnico Herramienta Misional (HEMI)
- PR-123 Gestión de Incidentes de Seguridad
- PR-131 Monitoreo Acceso a los Medios de Procesamiento de Información
- PR-133 Otorgar Acceso a los Medios de Procesamiento de Información
- PR-136 Atención Mesa de Ayuda
- PR-033 Backup Generación y Recuperación
- IN-069 Gestión de Incidentes de Seguridad

b. *Gestión Contractual*

- MS-012 Manual de Contratación, Supervisión e Interventoría para cada vigencia - Contrato IT GOP

c. *Planeación Estratégica y Táctica*

- PR-042 Planeación Estratégica y Operativa

3.1. LIMITACIÓN AL ALCANCE

Respecto a los contratos adjudicados a IT GOP desde 2006, los informes de supervisión se encuentran dispersos soportados con la impresión de correos electrónicos, informes, requerimientos, reuniones, etc.; se detecta una información, pero las deficiencias en la conformación del archivo y su gestión documental dificultaron la labor de auditoría.

4. CONFORMACIÓN EQUIPO DE TRABAJO DE AUDITORÍA

Auditor(a) Responsable de la Auditoría – ARA

RAFAEL EDUARDO ORTÍZ GÓMEZ
Ingeniero de sistemas, Especializado en Telecomunicaciones, en Seguridad de la Información y Especialización Tecnológica en Gestión de Proyectos, certificado Auditor Interno ISO 27001, *Scrum Master*, *Product Owner*, COBIT 2019, Diplomado en Control Interno.

Para los hallazgos relacionados con el proceso de Gestión Contractual se contó con la participación del auditor:

PABLO MAURICIO SARMIENTO DELGADILLO
Abogado Magíster en Derecho Constitucional, Conciliador, Especialista en Contratación Estatal y en Defensa Jurídica, con 5 años de experiencia en contratación estatal y 2 años en Defensa Jurídica en el sector público.

5. FORTALEZAS

En el Alcance se incluyó los Procedimientos:

- PA08-DE-002 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- PA08-DE-003 Plan de Seguridad y Privacidad de la Información
- MS-013 Manual Seguridad de la Información
- PR-123 Gestión de Incidentes de Seguridad
- PR-133 Otorgar Acceso a los Medios de Procesamiento de Información
- IN-069 Gestión de Incidentes De Seguridad

En los que, al aplicar las pruebas de auditoría a la muestra seleccionada en cada procedimiento, no se identificaron observaciones o deficiencias; por lo tanto, la Asesoría de Control Interno concluye que la gestión es adecuada teniendo en cuenta que no se detectaron falencias ni incumplimiento notorio del procedimiento.

6. CONCLUSIONES

En los procesos y procedimientos evaluados se evidenciaron debilidades en la aplicación de los controles debido a que los lineamientos establecidos en las normas, los procedimientos, guías e instructivos no fueron ejecutados completa o adecuadamente, situación que pone en riesgo los intereses y recursos del IPES, a la vez que afecta el cumplimiento de los Objetivos Estratégicos y la Misión del Instituto.

Algunas de las principales causas de los resultados de auditoría pueden responder a:

1) Inadecuado diseño de controles, no cumplen con los 6 elementos: Responsable, periodicidad, propósito, procedimiento, desvío o manejo de excepciones y evidencia de la aplicación del control.
2) Software GOOBI no cumple con el objetivo misional.
3) Ausencia de planeación estratégica en los proyectos.
4) Falta aplicación de acciones de mitigación oportunas, lo que conllevó a la repetición de observaciones con alcance diferente.

5) Se proponen acciones de mejora con tiempos de hasta 1 vigencia, lo que resulta costoso e inefectivo.
6) Fallas y debilidades de control en la gestión del soporte informático respecto a la mesa de servicio, que no permite conocer el estado del servicio solicitado.
7) Falta de metodología para pruebas funcionales de las aplicaciones.
8) Desactualización de algunos procedimientos.
9) Falta de evidencias y/o registros de las pruebas antes de pasar a producción.
10) Debilidad en el levantamiento de requerimientos funcionales de los sistemas de información.
11) Ausencia de metodología para la gestión de proyectos.

Las siguientes fueron las situaciones identificadas en los procedimientos auditados de cada proceso:

a. **GESTIÓN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS**

- ***PR-042 Planeación Estratégica y Operativa***

1. Falta interoperabilidad de los sistemas de información.

- ***PR-131 Monitoreo Acceso a los Medios de Procesamiento de Información***

2. Deficiencias funcionales del software GOOBI.

- ***PR-136 Atención de Mesa de Ayuda***

3. Deficiencias en gestión de atención en mesa de ayuda.

- ***PR-033 Backup Generación y Recuperación***

4. Ausencia de métricas para validar la disponibilidad y la perdida de datos del servicio.
5. Desactualización del procedimiento de back up, generación y recuperación.
6. Deficiencias en el diseño de controles.

b. **GESTIÓN CONTRACTUAL**

- ***MS-012 Manual de Contratación, Supervisión e Interventoría***

7. Deficiencias en la aplicación de los principios de la contratación pública: eficacia

7. RESUMEN DE RESULTADOS DE LA AUDITORÍA

En la etapa de Planificación de la Auditoría se identificaron los procesos a auditar y se obtuvo como resultado el mapa de riesgos inherentes por cada proceso.

En la etapa de Desempeño del Trabajo se aplicaron las Pruebas de Validación de Efectividad Operativa –PVEO, con las que se obtuvo la valoración de los controles que permitieron valorar el riesgo residual de los riesgos inherentes que fueron analizados y evaluados (*Ver **ANEXO 1** - MAPAS DE RIESGOS*), y que permitieron la identificación de las Observaciones que se presentan a continuación.

En total se determinaron 7 Observaciones, de las cuales 1 tiene Posible Connotación Disciplinaria.

Proceso	Procedimiento	Total	%
PLANEACIÓN ESTRATÉGICA Y TÁCTICA	*PR-042 Planeación Estratégica y Operativa*	1	14%
	Total PROCESO 1	**1**	**14%**
GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS	*PR-131 Monitoreo Acceso a los Medios de Procesamiento de Información*	1	14%
	PR-136 Atención Mesa de Ayuda	1	14%
	PR-033 Backup Generación y Recuperación	2	28%
	Diseño de Controles	1	14%
	Total PROCESO 2	**5**	**0%**
GESTIÓN CONTRACTUAL	*MS-012 Manual de Contratación, Supervisión e Interventoría*	1	14%
	Total PROCESO 3	**1**	**14%**
	TOTAL GENERAL	**7**	**100%**

8. DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA

HALLAZGOS

Proceso: PLANEACIÓN ESTRATÉGICA & TÁCTICA
Procedimientos: PR-042 Planeación Estratégica y Operativa

Ver ***ANEXO 2*** **-** *MUESTRA PROCESO GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS* en archivo *ANEXOS* del Informe Final donde se describe la muestra analizada.

No.: 1
FALTA INTEROPERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN

Responsable de las acciones de mejora: SDAE

Se evidenció deficiencias para para fortalecer la interoperabilidad entre los sistemas de información e infraestructura tecnológica que faciliten el intercambio de información entre las entidades y los sectores del Distrito y los nuevos desarrollos tecnológicos se encuentran desarticulados de la gestión de GSIRT de la SDAE.

La interoperabilidad es uno de los inconvenientes más frecuentes dentro y fuera de las organizaciones tanto públicas como privadas. La arquitectura orientada a servicios (SOA) se viene desarrollando desde hace más de dos décadas, durante los años 80 aparecieron los modelos orientados a objetos, posteriormente en la década de los 90 aparecen modelos basados en componentes, actualmente los modelos orientados a servicios (*web service*). Dentro de sus características fundamentales se resalta el enfoque centrado en el negocio y en la neutralidad de proveedores.

Marco de Interoperabilidad – MINTIC
http://lenguaje.mintic.gov.co/marco-de-interoperabilidad

> ***"Definición del Marco de Interoperabilidad:***
> *Frente a las dificultades del ciudadano colombiano al realizar trámites con entidades del estado, asumiendo traslados innecesarios y gastos en tiempos y recursos, el Ministerio de las Tecnologías de la Información y las Comunicaciones identificó que las entidades estaban aisladas en la atención y en la debida gestión, razón que conlleva a plantear una solución para ofrecer servicios en línea que optimicen el proceso. Con este objetivo el Marco de Interoperabilidad para Gobierno Digital, nace como un conjunto de principios, políticas y recomendaciones que busca facilitar y optimizar el ejercicio de colaboración entre organizaciones para intercambiar información y conocimiento, en el marco de sus procesos de negocio, con el propósito de facilitar la entrega de servicios a ciudadanos, empresas y a otras entidades. Los motivos que supone para el Ministerio de las Tecnologías de la Información y las comunicaciones liderar esta iniciativa son:*
> - *Agilizar los trámites*
> - *Crear ventanillas únicas de consulta*
> - *Ofrecer un acceso a la información más fácil y menos dispendiosa*
> - *Facilitar la participación de los usuarios con apoyo de las TI*
> - *Consolidar un Estado transparente y coordinado*
> - *Promover la confianza del ciudadano en el uso de TI del Estado"*

Cuando se desarrolla el PA08-DE-001 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN y se analiza la situación actual de los sistemas de información del IPES, se indica:

> *"Este apartado comprende un entendimiento estratégico de la Entidad, así como un diagnóstico teniendo en cuenta los dominios del marco de referencia de arquitectura Empresarial (MAE). El Instituto para la Economía Social - IPES, elaboró un análisis a partir del cumplimiento de la Política de Gobierno Digital* ***teniendo en cuenta los dos componentes y los tres habilitadores transversales****; permitiendo así contar con una medición del nivel madurez tecnológico y una línea base para proyectar la visión de lo que se espera en materia de gestión de TI en el Instituto".* Negrilla fuera de texto.

Sin embargo, no se pudo evidenciar cuáles son los dominios y habilitadores que se adoptaron en el PETI 2020-2024, tampoco fue posible evidenciar cuál de los siguientes dominios se cumple:

- Dominio de planeación de la arquitectura
- Dominio de arquitectura misional
- Dominio de arquitectura de información
- Dominio de arquitectura de infraestructura Tecnológica
- Dominio de arquitectura de seguridad
- Dominio de uso y apropiación de la arquitectura
- Dominio de arquitectura de infraestructura TI

En el requerimiento de información para la auditoría, se solicitó a la SDAE el envío de la arquitectura de HEMI y GOOBI, pero en la respuesta del radicado 00110-817-003421 este ítem no fue suministrado, no obstante, en el PETI se enuncia la definición de la arquitectura implementada.

Se lee en el PA08-DE-001 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN, en el punto *7.2.3. Sistemas de Información* se puede visualizar la arquitectura de HEMI y la topología de red de HEMI y GOOBI, en donde se evidencia ausencia del cumplimiento del dominio del dominio *5.5. Interoperabilidad: "Utilizar los estándares que fortalezcan la plena interoperabilidad entre los sistemas de información e infraestructura tecnológica y que faciliten el intercambio de información entre las entidades y los sectores."* Faltando al cumplimiento de la normatividad.

La interoperabilidad en la era moderna abarca el intercambio de datos contenida en sistemas de información heterogéneos para cumplir un objetivo. La interoperabilidad le apunta a la optimización de los costos de producción como resultado de la eficiente utilización de los recursos tecnológicos y la reutilización viene siendo una forma de hacer más eficiente la actividad de las empresas públicas.

La Alta Consejería Distrital de TIC en octubre de 2020 ha identificado que el estado colombiano tenía ya definido un protocolo para la interoperabilidad, en año 2017 solo una entidad del distrito hacia uso de ello. La Alta Consejería Distrital de TIC pretende mejorar los procesos de intercambio de información entre las entidades del Distrito y otras entidades del País, se decide adoptar el marco de interoperabilidad del Gobierno Nacional en las entidades distritales.

Se evidenció que falta una definición de alcance hasta dónde desea llegar el IPES en términos de la administración y el desarrollo de sus *webs services* con otras organizaciones distritales, nacionales y/o privadas.

En el informe de Seguimiento al Sistema de Denuncias Quejas, Peticiones y Sugerencias - SDQS periodo junio 2020 – marzo 2021 con radicado 00110-817-002621, se identificó que se han realizado directrices para el cumplimiento de las circulares 07 de 2019, y la 032 y 053 de 2018 en donde la alta consejería de la Alcaldía Mayor de Bogotá establece la interoperabilidad entre diferentes sistemas de información para así poder gestionar la información de manera uniforme y asíncrona entre BOGOTÁ TE ESCUCHA y el los SQSD ingresados desde el IPES.

La Alta Consejería Distrital de TIC ha expedido la siguiente normatividad para que las entidades pertenecientes al distrito de Bogotá consuman el *web service:*

- Circulares 007 de 2019, de la Oficina alta consejería distrital de tecnologías de la información y las comunicaciones, "ha promovido el uso de la distribución *CMS Govimentum* basada en la plataforma de código abierto Drupal convocando a los *webmaster* distritales un escenario bajo la colaboración bajo las dinámicas de comunidad distrital especializada en la materia."
- Circular 032 de 2018, de la Oficina alta consejería distrital de tecnologías de la información y las comunicaciones, indica la actualización de los servicios web del sistema Distrital de quejas y soluciones (Bogotá te escucha) que actualmente consume el módulo govi_sdqs de la distribución distrital *CMS Govimentum.*
- Circular 053 de 2018, de la Oficina alta consejería distrital de tecnologías de la información y las comunicaciones, donde indican: "Lineamientos sobre el formulario electrónico para la recepción de solicitudes de acceso a información pública"

Las cuales solicitan la articulación para identificar y cruzar la información entre los sistemas de información de las entidades que hacen parte del distrito de Bogotá y su plataforma BOGOTÁ TE ESCUCHA - SDQS. En los aplicativos misionales HEMI y GOOBI no se evidencia en su arquitectura la interoperabilidad para comunicarse con otros sistemas de información.

Estas circulares dan cumplimiento a la resolución 3564 de 2015del MINISTRO DE TECNOLOGIASDE LA INFORMACION Y LAS COMUNICACIONES, donde la Ley N° 1341 de 2009 contempla dentro de sus principios orientadores, la masificación de Gobierno en Línea, exigiendo a las entidades públicas adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones en el desarrollo de Sus funciones con el fin de lograr la prestación de servicios eficientes a los ciudadanos.

Durante entrevista el 08-jul-2021 con el contratista encargado de la SESEC para el seguimiento y monitoreo al cumplimiento del decreto 092 del 2021, donde se define la línea base para la creación de los concejos de vendedores informales y se exige que las elecciones sean virtuales (artículo N° 14); las cuales llevarán a cabo en 19 localidades del distrito. En el primer trimestre de 2021 se desarrolló un *web service* que conecta HEMI con VOTEC (aplicativo que pertenece al Instituto Distrital de Participación y Acción Comunal - IDPAC). Para el desarrollo de este proyecto se realizaron mesas de trabajo lideradas por el IPES.

Al solicitar, en el marco de la auditoría, el contrato de servicios o contrato de *web service,* no se obtuvo evidencia de que existiera documentación y claridad de cómo se desarrolla el proyecto.

Falta de estructuras e implementación de la adopción hacia un modelo estandarizado de arquitectura y gobierno SOA que le permita al IPES alcanzar niveles de servicio a la comunidad y optimización de procesos.

En cuanto a los nuevos desarrollos en el IPES, la arquitectura documentada no refleja la interoperabilidad para dar cumplimiento a:

- Decreto 092 del 2021 (Elecciones de consejo vendedores informales).
- Software digitalización de plazas de mercado - MARKETPLACE (contrato N°1599650/2020).

Los cuales no se observan incluidos ni articulados con el PA08-DE-001 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN vigente, donde el proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, a cargo de la SDAE, no está participando en estos nuevos proyectos de solución tecnológica iniciados por las áreas misiones, lo cual denota una falta de alineación estratégica entre las dependencias, en cumplimiento de los Objetivos Estratégicos de TI que indican:

7.2.1.1. Objetivos Estratégicos de TI

El IPES comprende los siguientes objetivos estratégicos alineados en 3 componentes para lograr su misión:

Beneficiarios

- *Ofrecer mejores servicios a través de la herramienta misional.*
- *Fortalecer estrategias para obtener la calidad de los datos e integridad.*
- *Propender por mejoras tecnológicas en los procesos de caracterización.*

Procesos Internos

- *Analizar, diseñar, desarrollar nuevas funcionalidades en los sistemas de información.*
- *Implementar funcionalidades en desuso con el apoyo de los directivos.*
- *Actualizar procedimientos incorporando las herramientas tecnológicas de la entidad.*
- *Apoyar en la optimización de procesos misionales.*

Capacitación

- *Definir estrategias de apropiación de los sistemas de Información, que incluya socialización, sensibilización y capacitación.*
- *Fortalecer el uso de la tecnología.*

En las dos soluciones de software se encontraron las siguientes situaciones:

- ***Decreto 092 del 2021 (Elecciones de consejo vendedores informales)***

No se evidencia la correcta gestión de proyectos de parte de los lideres asignados por los responsables de los proyectos, se realizaron mesas de trabajo en las cuales se solicitó qué se requería, y ofrecieron una herramienta tecnológica que se llama VOTEC, donde no se observa cómo se asegura la continuidad del proyecto, tanto del factor humano como del tecnológico.

- ***Software digitalización de plazas de mercado - MARKETPLACE***

El objetivo de este proyecto es dar la posibilidad de que los locatarios de plazas puedan contar con un *e-commerce,* por lo tanto, el IPES se encuentra desarrollando una plataforma de MARKETPLACE.

Para el desarrollo de este proyecto, se trató de trabajar con servidores pertenecientes a la infraestructura del IPES, pero no se pudo usar por el repudio de que el proyecto se encontraba designado a una área ajena, se dio un acceso FTP para una única carpeta para realizar la gestión y aparte se presentó un incidente en la infraestructura en la prestación del servicio, y decidieron desde GSIRT eliminar el acceso al FTP, a pesar de que el proyecto consistía solo en la publicación de un directorio de los locatarios, se ha notado la ausencia de una gestión de proyectos (PMO).

Al respecto, se observa el incumplimiento del Documento Maestro de Arquitectura Empresarial (MAE) del MinTIC:

7.3.3. MAE.LI.AI.03 - Marco de interoperabilidad del Estado
7.3.10. MAE.LI.AI.10 - Apertura de datos

La ausencia de interoperabilidad en los sistemas de información en cualquier tipo de entidad dificultad la una comunicación eficiente, su no implementación podría generar información duplicada y reprocesos en la generación de valor en las partes interesadas.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR-058 NORMOGRAMA, presentó el siguiente Diseño de Control:

Control 3: PA08-DE-001 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN
7.5. MODELO DE PLANEACIÓN
7.5.1. Lineamientos y/o principios que rigen el Plan Estratégico de TIC
Plan de Desarrollo Distrital - PDD
Proyecto de Inversión
Proyecto de Inversión
Requerimientos externos para la definición y estructuración del PETI
7.5.2. Estructura de actividades estratégicas
Cumplimiento a la política gobierno digital
Fortalecimiento de la seguridad de la información
Fortalecimiento de la gestión misional mediante el uso de herramientas TI
Fortalecimiento de la gestión de las áreas administrativas y financieras mediante el uso de herramientas de TI
implementar tecnologías emergentes
Fortalecimiento tecnológico institucional

De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidad en la definición del responsable, la periodicidad, el propósito y el manejo de excepciones.

Valoración comentarios del Auditado

Los comentarios dejados por la SDAE fueron:

> *"La SDAE-PGSIRT no acoge la observación debido a que no es clara frente al texto "definición para fortalecer la plena interoperabilidad" debido a que los procesos de interoperabilidad, como bien se indica en la observación, se realizan entre dos o más partes, "entre las entidades y los sectores del Distrito", por lo que no se puede efectuar la misma desde un solo componente o sistema de información, se requiere la voluntad e intención entre las partes, es decir de otras entidades con sus aplicaciones y el IPES para lograr interoperar los sistemas. En ese contexto el Instituto para la Economía Social IPES, no puede realizar esfuerzos e inversiones de publicación o consumo de datos de una contraparte que no existe, o que no tiene la voluntad de interoperar o no cuenta con los recursos para dichas acciones.*
> *Por ejemplo: el IPES no puede invertir recursos en diferentes escenarios para interoperar con herramientas como SECOP II, SIVICOF o BOGDATA, entre otras, mientras las entidades propietarias de dichas herramientas no lo permitan y realicen las actividades relacionadas para consumir o exponer su información. En esta situación se configuraría un detrimento en el patrimonio, así como infringir algunos de los principios, planes y medidas de la función pública tal como la austeridad en el gasto; el realizar los mencionados esfuerzos conociendo que el proyecto carece de viabilidad dado que la otra entidad y el otro sistemas no lo permiten y no se encuentran preparados para realizar la interoperabilidad y en mayor proporción cuando se*

desconoce la forma de operar, adquirir o desarrollar las herramientas tecnológicas de las otras entidades que en muchas ocasiones se encuentran con la figura de tercerización y depende de una planeación y recursos en los cuales no podemos tomar parte.
Por lo anterior se concluye que las prácticas de interoperabilidad dependen de la demanda del servicio y no se puede obligar a otras entidades a invertir los recursos necesarios para implementarla a pesar de los lineamientos vigentes, los cuales hasta el momento no son de obligatorio cumplimiento para las entidades territoriales y solo conforman un marco de referencia en caso de requerirse."

Análisis ACI: Cuando se indica "*definición para fortalecer la plena interoperabilidad*", es precisamente identificar las necesidades actuales que tiene el IPES para seguir los lineamientos la Alta Consejería para las TIC del Distrito Capital, también estipular los contractos de *Web Service* con antelación para ser receptor y emisor solamente con las aplicaciones y/o entidades que lo requieran.

No se solicita conectar SECOP II o SIVICOF, como el auditado indica, no se requiere con estas plataformas, en este momento existen resoluciones de SDQS en donde las entidades pertenecientes al distrito de Bogotá DC se pueden conectar para optimizar el proceso de sus respuestas.

No se puede aceptar como evidencia las mesas de trabajo realizadas en este momento, debido a que la auditoria cubre las evidencias entre enero 2020 a abril 2021, a pesar de que ya se estén tomando acciones para el mejoramiento y optimización del intercambio de la información con otros sistemas de información. Estas actividades se deben reflejar en la formulación de una acción de mejora para efectuar el correspondiente seguimiento.

Los comentarios dejados por la SDAE fueron:

*"El apartado: "**Se lee en el PA08-DE-001 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN, en el punto 7.2.3. Sistemas de Información se puede visualizar la arquitectura de HEMI y la topología de red de HEMI y GOOBI, en donde se evidencia ausencia del cumplimiento del dominio del dominio 5.5. Interoperabilidad: "Utilizar los estándares que fortalezcan la plena interoperabilidad entre los sistemas de información e infraestructura tecnológica y que faciliten el intercambio de información entre las entidades y los sectores." Faltando al cumplimiento de la normatividad**."*
Tal como se expresó anteriormente no existe incumplimiento del dominio de interoperabilidad al ser un servicio por demanda y contener la arquitectura necesaria como se evidencia en la actual práctica en producción con VOTEC.
*La afirmación "**En el requerimiento de información para la auditoría, se solicitó a la SDAE el envío de la arquitectura de HEMI y GOOBI, pero en la respuesta del radicado 00110-817-003421 este ítem no fue suministrado**" no es cierta ya que a través de la comunicación 00110-817-003555-21, se brindó respuesta indicando claramente la arquitectura (Ver anexo, numeral 13, https://drive.google.com/drive/folders/1vyPXdh_780sV3s6Qjoo5A3XNvnUDoPr?usp=sharing)*
"13) Arquitectura de HEMI y GOOBI en tres capas u otra si se utilizan.
Hemi
La herramienta misional es desarrollada con una arquitectura N-tier de la siguiente manera.
Arquitectura aplicación web

- ✓ Tipo de Aplicación: Web Enable
- ✓ Tecnología: ASP.NET
- ✓ IDE de Desarrollo: VS2019 Express
- ✓ Pantallas con tecnología AJAX
- ✓ Metodología N-Tier
- ✓ Capa de Presentación
- ✓ Capa de Lógica del Negocio (BLL)
- ✓ Capa de Acceso a Datos (DAL)
- ✓ Capa de Base de Datos (SQL)
- ✓ Bootstrap y Html5 (En proceso de implementación)

Figura 1. Arquitectura de HEMI

● Capa de Presentación: Aplicación web con tecnología ASP.NET desplegada en un servidor de aplicaciones Microsoft Internet Information Services. Acá también se encuentra el componente web reporteador representado por Reporting Services.
● Capa de Lógica de Negocio: Conjunto de clases que permite especificar los métodos y servicios que accede la capa de presentación por cada módulo u objeto abstraído en el sistema.
● Capa de Acceso a Datos: Conjunto de clases que permiten el acceso a la base de datos para realizar las operaciones CRUD (Create, Read, Update, Delete) que el sistema requiere. Esta capa presta sus servicios a la capa de lógica de negocio.
● Base de Datos: Motor de base de datos Sql Server que gestiona el modelo de datos del sistema y el almacenamiento de la información correspondiente."
La anterior descripción corresponde estrictamente a lo enunciado, el diseño de arquitectura web con el que fue implementada la Herramienta Misional. Estas definiciones como es regla, responden a los lineamientos tecnológicos (plataformas, tecnologías y frameworks) en los que se soporta el sistema.
De acuerdo a la definición comúnmente aceptada; la interoperabilidad es la capacidad de dos o más sistemas o componentes para intercambiar información y usar la información que se ha intercambiado; y suponiendo que el requerimiento se refiere a señalar la interoperabilidad existente entre dos componentes, para eso utilizamos un diagrama de Arquitectura de Interoperabilidad. Cabe señalar que este requerimiento no ha sido recibido explícito y de manera formal.
Es importante resaltar que el servicio web que interactúa con VOTEC es un componente o aplicación más que permite compartir ciertos datos de la BD de HEMI, pero no es HEMI en sí, ni se refiere al sistema web HEMI; por lo que el diagrama de arquitectura aportado es suficiente y completo en cuanto a que se refiere al sistema HEMI (lo que fue requerido).
Para aportar al detalle de información relacionada de este informe, presentamos el diseño de la arquitectura de interoperabilidad que soporta la interacción entre los sistemas de VOTEC y el servicio Web HEMI para el proceso de elecciones.

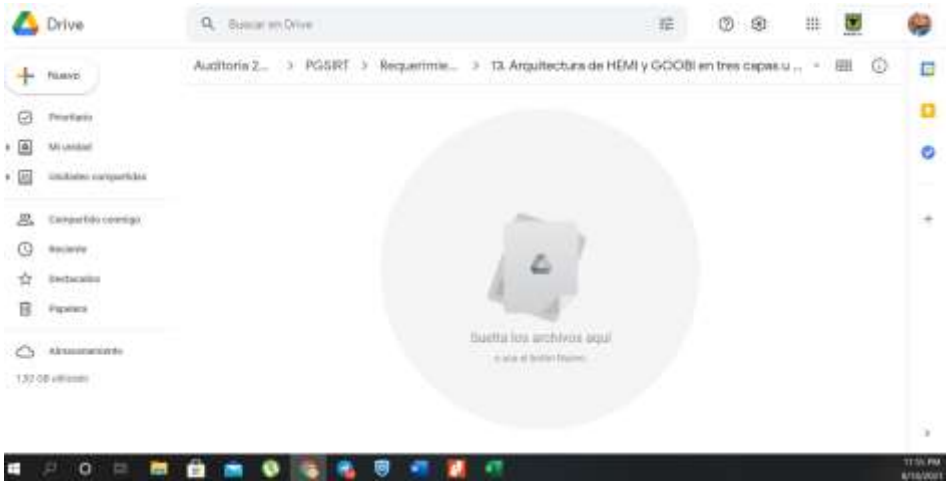
Adicionalmente, la documentación técnica de uso y de pruebas del Servicio Web enunciado se encuentra en: https://hemi.ipes.gov.co/services/swagger/index.html; recurso completo y suficiente para un par técnico, que indica los métodos de consumo expuestos, el esquema de uso y sus parámetros, y ofrece a su vez la interfaz de prueba en línea del servicio web. Fue precisamente mediante este mecanismo y buena práctica que se llevó a feliz término el proceso

de desarrollo, pruebas y puesta en marcha del servicio web en los tiempos estipulados junto con los ingenieros de IDPAC."

Análisis ACI: En la documentación se observa la arquitectura de HEMI de una forma bien explicada, pero en su diagrama y su descripción no se indica la posibilidad de realizar conexión de *web service.* En la mesa de trabajo con el desarrollador de HEMI, reconoció que si se puede desarrollar *web service* e indicó que se está trabajando en fortalecer la documentación.

VOTEC es la pruebade que los sistemas de información requieren interoperabilidad para optimizar los procesos y aumentar su precisión, el grupo de SDAE-PGSIRT, desarrolló un *web service,* pero al no tener documentado su consumo y al realizarse cambio de personal, obligaría tener que volver a programar esta función precisamente por la fuga de conocimiento.

La carpeta indicada sobre la documentación fue suministrada vacía como se muestra en la imagen:



La información suministrada en la respuesta del radicado no se puede aceptar debido a que en esta etapa no se pueden aceptar documentación no suministrada en la ejecución.

Respecto al comentario *"Cabe señalar que este requerimiento no ha sido recibido explícito y de manera formal",* se recuerda que de acuerdo a la Carta de Representación suscrita por los auditados se indicó por parte de la ACI en la reunión de apertura de auditoría:

"(…) Para poder llevar a cabo el trabajo, debe suscribirse la siguiente certificación donde se indica, que toda la información ha sido proporcionada a los auditores, ya sea solicitada directamente o no, y que la información dada a los auditores es verdadera y correcta de acuerdo a su conocimiento.

Los funcionarios y/o contratistas designados por cada Subdirección u Oficina suscriben la siguiente certificación:

Certificación de Representación

En cumplimiento del artículo 16 del Decreto 648 de 2017, mediante el cual se adicionó al Capítulo 4 del Título 21, Parte 2, Libro 2 del Decreto 1083 de 2015, el Artículo 2.2.21.4.8 Instrumentos para la Actividad de Auditoría Interna, y respecto a su literal " b) Carta de representación en la que se establezca la veracidad, calidad y oportunidad de la entrega de la información presentada a las Oficinas de Control Interno", que fue adoptada por el Instituto para la Economía Social – IPES mediante Resolución 050 de 2021, certificamos que:

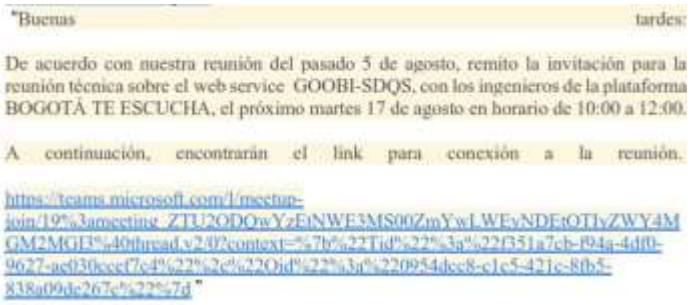
1. La información entregada para la realización del trabajo es verídica.

2. La información entregada cumple con los criterios de calidad.

3. La información es entregada oportunamente a la Asesoría de Control Interno, considerando los recursos disponibles para el desarrollo del trabajo al proceso PO - 013 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS de la dependencia SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO – SDAE."

Los comentarios dejados por la SDAE fueron:

*"La afirmación: **"Aunque su desarrollo permite web service no se encuentra el web service ni el contrato de web service reflejado en su diagramación."** Se desvirtúa, por lo que no se acoge la observación y se responde de manera formal mediante la anterior exposición y aclaración sobre las arquitecturas de los componentes mencionados y su carácter y fines independientes.*
*En cuanto a: **"...Las cuales solicitan la articulación para identificar y cruzar la información entre los sistemas de información de las entidades que hacen parte del distrito de Bogotá y su plataforma BOGOTÁ TE ESCUCHA - SDQS. En los aplicativos misionales HEMI y GOOBI no se evidencia en su arquitectura la interoperabilidad para comunicarse con otros sistemas de información."** respecto a los dos sistemas mencionados, no se acoge la observación porque:*
*1. **HEMI**: El objetivo funcional y misional de HeMi no tiene relación con los servicios funcionales prestados por Bogotá te Escucha.*
*2. **GOOBI**: Desde el ERP se realizó el desarrollo y pruebas de interoperabilidad con la plataforma BOGOTA TE ESCUCHA, sin embargo, están pendientes algunas reglas de negocio para iniciar su operación, por lo que se tienen programadas una serie de reuniones con los responsables desde alcaldía mayor:*


"Buenas tardes:

De acuerdo con nuestra reunión del pasado 5 de agosto, remito la invitación para la reunión técnica sobre el web service GOOBI-SDQS, con los ingenieros de la plataforma BOGOTÁ TE ESCUCHA, el próximo martes 17 de agosto en horario de 10:00 a 12:00.

A continuación, encontrarán el link para conexión a la reunión.

https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZTU2ODOwYzEtNWE3MS00ZmYwLWEyNDEtOTIyZWY4MGM2MGI3%40thread.v2/0?context=%7b%22Tid%22%3a%22f351a7cb-f94a-4df0-9627-ae030ccef7c4%22%2c%22Oid%22%3a%220954dcc8-c1c5-421c-8fb5-838a09de267c%22%7d"

*Respecto a la afirmación: "**Al solicitar, en el marco de la auditoría, el contrato de servicios o contrato de web service, no se obtuvo evidencia de que existiera documentación y claridad de cómo se desarrolla el proyecto.**" No es claro el ámbito al que se refiere la afirmación; sin embargo, no se acoge la observación de acuerdo a:*
*1. En el entendido de que se está refiriendo al **contrato técnico** de especificación del servicio web, como se mencionó anteriormente, la documentación técnica de uso y de pruebas del Servicio Web enunciado se encuentra en: https://hemi.ipes.gov.co/services/swagger/index.html; recurso completo y suficiente para un par técnico, que indica los métodos de consumo expuestos, el esquema de uso y sus parámetros, y ofrece a su vez la interfaz de prueba en línea del servicio web. Fue precisamente mediante este mecanismo y buena práctica que se llevó a feliz término el proceso de desarrollo,*

pruebas y puesta en marcha del servicio web en los tiempos estipulados junto con los ingenieros de IDPAC por lo que sí existió documentación relacionada y claridad respecto al desarrollo e implementación del proyecto.

2. Si el ámbito es del orden administrativo, es la SGRSI la encargada de ejercer las actividades administrativas y de gestión en lo relacionado con establecer los términos y condiciones de la interoperabilidad entre los dos componentes o entidades y en la coordinación e interacción administrativa y de equipos entre las dos partes.

*Sobre el enunciado: "**Falta de estructuras e implementación de la adopción hacia un modelo estandarizado de arquitectura y gobierno SOA que le permita al IPES alcanzar niveles de servicio a la comunidad y optimización de procesos.**", no se acoge la observación y hay que decir que no existe referencia ni lineamiento obligatorio en la materia que exija a la Entidad cumplir ciertas implementaciones en este sentido. Si bien lo expuesto en el enunciado está inmerso dentro las guías del MinTIC en lo relacionado con la adopción de una Arquitectura Empresarial y la Implementación de Servicios Digitales esto hace parte de un marco de referencia susceptible de ser usado en el momento en que se decidan adoptar e implementar. Actualmente el IPES no está incumpliendo la implementación de ninguna regulación en este sentido ni de ningún plazo relacionado con la materia en lo referente a entidades territoriales.*

En lo referente a: "En cuanto a los nuevos desarrollos en el IPES, la arquitectura documentada no refleja la interoperabilidad para dar cumplimiento a:

- ***Decreto 092 del 2021 (Elecciones de consejo vendedores informales).***
- ***Software digitalización de plazas de mercado - MARKETPLACE (contrato N°1599650/2020).***

Los cuales no se observan incluidos ni articulados con el PA08-DE-001 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN vigente, donde el proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, a cargo de la SDAE, no está participando en estos nuevos proyectos de solución tecnológica iniciados por las áreas misiones, lo cual denota una falta de alineación estratégica entre las dependencias, en cumplimiento de los Objetivos Estratégicos de TI que indican.".

No se acoge la observación, y anteriormente ya se especificó de manera completa que la arquitectura evidenciada fue la de la Herramienta Misional HEMI, tal cual como fue solicitado. La especificación del servicio web para integración con VOTEC en su diseño de arquitectura no había sido solicitado. Sin embargo, ya anteriormente se especificó la arquitectura del servicio, para claridad se adjunta de nuevo:

Respecto de la no inclusión de estas integraciones en el PETI, no se acoge la observación y se aclara que este documento es un mecanismo de planeación macro para la entidad en cuanto a lo relacionado con TI. Los detalles de implementación no deben especificarse allí y no necesariamente todo lo realizado debe estar planeado en el PETI. Es por esto que el PETI se debe actualizar anualmente contemplando las constantes necesidades y demandas de TI; como es el caso de la integración con VOTEC que responde a una necesidad puntual en un momento determinado y que no surgió como resultado de una planeación macro o mayor en el tiempo. Es así que no encontrar en el PETI esta información no es indicador de falta alguna.

*En este enunciado: "**En las dos soluciones de software se encontraron las siguientes situaciones:***
● Decreto 092 del 2021 (Elecciones de consejo vendedores informales) No se evidencia la correcta gestión de proyectos de parte de los lideres asignados por los responsables de los proyectos, se realizaron mesas de trabajo en las cuales se solicitó qué se requería, y ofrecieron una herramienta tecnológica que se llama VOTEC, donde no se observa cómo se asegura la continuidad del proyecto, tanto del factor humano como del tecnológico.
***● Software digitalización de plazas de mercado – MARKETPLACE El objetivo de este proyecto es dar la posibilidad de que los locatarios de plazas puedan contar con un e-commerce, por lo tanto, el IPES se encuentra desarrollando una plataforma de MARKETPLACE.**"*
La plataforma Marketplace es una herramienta adquirida y gestionada desde SESEC, para la cual no conto con conocimiento el PGSIRT hasta el momento en que ya se iba a implementar dada la necesidad de recursos tecnológicos para lo cual se proporcionó un servidor institucional, un dominio de la entidad ipes.gov.co y el despliegue del certificado de seguridad SSL.
En lo que respecta al Servicio Web que se integra con VOTEC, no hay claridad a la falta de evidencia referida respecto a la gestión del proyecto. No tenemos relación de ninguna solicitud formal realizada en este sentido. Adicionalmente, reiteramos la explicación y aclaración correspondiente: Es la SGRSI la encargada de ejercer las actividades administrativas y de gestión en lo relacionado con establecer los términos y condiciones de la interoperabilidad entre los dos componentes o entidades y en la coordinación e interacción administrativa y de equipos entre las dos partes. El proyecto se realizó cumpliendo los plazos estipulados y ha operado sin problemas desde el día de su lanzamiento.
En vista de la situación de emergencia sanitaria alrededor del mundo fue necesaria la reorganización de múltiples actividades, dentro de ellas en el IPES se hizo necesaria la realización de las elecciones de concejos locales de vendedores informales de forma electrónica, por tal razón se celebró la interoperabilidad entre HEMI y VOTEC, lo que no falta a la debida planeación ya que se surtieron las diferentes fases, lo que ha conllevado a total éxito tecnológico de la funcionalidad."

Análisis ACI: Respecto al Decreto 092 del 2021 (Elecciones de consejo vendedores informales) y Software digitalización de plazas de mercado – MARKETPLACE, se evidencia en la CARACTERIZACIÓN DEL PROCESO GSIRT, indica como OBJETIVO: *"Analizar, diseñar e implementar soluciones de tecnologías de información y comunicaciones que aumenten niveles de continuidad en la prestación de los sistemas y servicios informáticos misionales, administrativos y de gestión que apoyan el cumplimiento de los objetivos y la misionalidad de la entidad, a través de la administración, seguimiento, monitoreo, mantenimiento y mejora de la infraestructura tecnológica que soporta la operación informática del Instituto Para la Economía Social en el marco de las políticas y la normativa vigente".*

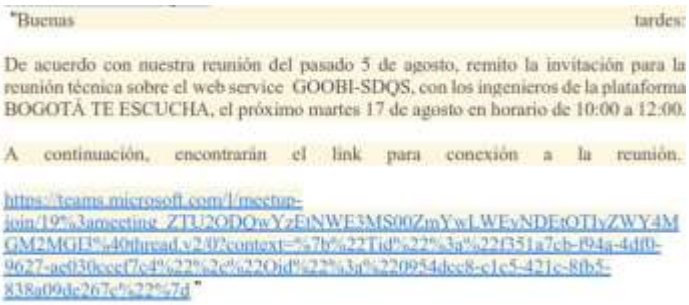
El enlace https://hemi.ipes.gov.co/services/swagger/index.html, ha sido suministrada hasta la réplica, no fue mencionada durante las solicitudes de información ni durante las mesas de trabajo.

La importancia de la documentación adecuada, para asegurar la disponibilidad de los recursos que cuenta el IPES y facilitar el alcance de herramientas con las que cuenta el IPES para cumplir sus operaciones.

Se reconoce que HEMI no requiere conectarse a BOGOTÁ TE ESCUCHA, pero si puede conectarse con otras soluciones (ejemplo VOTEC).

Respecto a las pruebas de GOOBI no fueron suministradas.

Respecto a la reunión que se suministra imagen:



"Buenas tardes:

De acuerdo con nuestra reunión del pasado 5 de agosto, remito la invitación para la reunión técnica sobre el web service GOOBI-SDQS, con los ingenieros de la plataforma BOGOTÁ TE ESCUCHA, el próximo martes 17 de agosto en horario de 10:00 a 12:00.

A continuación, encontrarán el link para conexión a la reunión.

https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZTI3ZODOwYzEtNWE3MS00ZmYwLWEyNDEtOTIyZWY4MGM2MGI3%40thread.v2/0?context=%7b%22Tid%22%3a%22f351a7cb-f94a-4df0-9627-ae030ccef7c4%22%2c%22Oid%22%3a%220954dcc8-c1c5-421c-8fb5-838a09dc267c%22%7d"

Esta información no puede ser aceptada, debido ya que fue suministra por fuera de tiempo, no se entregó ni en requerimientos, ni habiéndose dado la oportunidad a los responsables del proceso auditado de aportar evidencias adicionales en la mesa de socialización del 30-jul-2021.

Como se indicó con anterioridad respecto a https://hemi.ipes.gov.co/services/swagger/index.html no puede ser aceptado para su evaluación, debido a que la información fue suministrada por fuera de tiempo, no se entregó ni en requerimientos, ni el día de la socialización.

En ningún momento se pone en duda que *"la SGRSI la encargada de ejercer las actividades administrativas y de gestión en lo relacionado con establecer los términos y condiciones de la interoperabilidad entre los dos componentes o entidades y en la coordinación e interacción administrativa y de equipos entre las dos partes*", la observación hace referencia de asumir controles estratégicos desde la interoperabilidad con los sistemas que lo requieran, ya sean internos o externos.

Respecto a *"que decir que no existe referencia ni lineamiento obligatorio en la materia que exija a la Entidad cumplir ciertas implementaciones en este sentido. Si bien lo expuesto en el enunciado está inmerso dentro las guías del MinTIC en lo relacionado con la adopción de una Arquitectura Empresarial y la Implementación de Servicios Digitales esto hace parte de un marco de referencia susceptible de ser usado en el momento en que se decidan adoptar e implementar. Actualmente el IPES no está incumpliendo la implementación de ninguna regulación en este sentido ni de ningún plazo relacionado con la materia en lo referente a entidades territoriales",* la solicitud de interoperabilidad es una solicitud por medio de resoluciones de origen de MINTIC como:

> ***Resolución 3564 de 2015 de EL MINISTRO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES: CONSIDERANDO:*** *"Que la Ley N° 1341 de 2009 contempla dentro de sus principios orientadores, la masificación de Gobierno en línea, exigiendo a las entidades públicas adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones En el desarrollo de Sus funciones con el fin de lograr la prestación de servicios eficientes a los ciudadanos. Que una de las maneras orlas cuales las entidades públicas garantizan el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones para prestar servicios eficientes a los ciudadanos es a través de la Estrategia de Gobierno en línea. Que*

en el Decreto N° 1078 de 2015 se conságrala Estrategia Gobierno en línea y específicamente, en el artículo N° 2.2.9.1.2.1 se establecen los componentes de la Estrategia, entre los que se encuentra el de seguridad y privacidad de la información, que comprende las acciones transversales a los demás componentes, tendientes a garantizar la confidencialidad, la integridad y la disponibilidad de la información. Que atendiendo a los lineamientos de la Sentencia C-274 de 2013 de la Corte Constitucional, el acceso a la información pública es un derecho fundamental que cumple al menos tres funciones esenciales en nuestro ordenamiento. (i) garantiza la participación democrática y el ejercicio de los derechos políticos. (ii) cumple una función instrumental para el ejercicio de otros derechos constitucionales, ya que permite conocer las condiciones necesarias para su realización. (iii) garantiza la transparencia de la gestión pública, y, por lo tanto, se constituye en un mecanismo de control ciudadano de la actividad estatal." // ***Anexo 2: LINEAMIENTOS SOBRE EL FORMULARIO ELECTRONICO PARA LA RECEPCION DE SOLICITUDES DE INFORMACION PÚBLICA.***

Por parte de la alta consejería para las TIC de la alcaldía de Bogotá DC, existe las circulares 07 de 2019, y la 032 y 053 de 2018 en las cuales se establece la interoperabilidad con Bogotá te escucha.

Respecto a la situación de emergencia sanitaria, esto no impide realizar documentación para asegurar continuidad del negocio y conservación del conocimiento para cualquier tipo de la actividad de las partes interesadas en el IPES.

En mérito de lo expuesto, el hallazgo se mantiene y se debe establecer un plan de mejoramiento por parte del responsable del proceso.

Riesgo Asociado: Desarticulación de los lineamientos con la normatividad aplicable: Factores como el desconocimiento y no aplicabilidad de la normatividad externa o los cambios imprevistos de escenarios políticos, económicos, sociales e Inadecuada articulación con los entes distritales, como la emisión de directrices y lineamientos no claros dados desde la SDAE, pueden generar como riesgo la desarticulación de los lineamientos con la normatividad aplicable.

Normatividad o Criterio:

Resolución 3564 de 2015 de EL MINISTRO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES: CONSIDERANDO: *"Que la Ley N° 1341 de 2009 contempla dentro de sus principios orientadores, la masificación de Gobierno en línea, exigiendo a las entidades públicas adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones En el desarrollo de Sus funciones con el fin de lograr la prestación de servicios eficientes a los ciudadanos. Que una de las maneras orlas cuales las entidades públicas garantizan el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones para prestar servicios eficientes a los ciudadanos es a través de la Estrategia de Gobierno en línea. Que en el Decreto N° 1078 de 2015 se conságrala Estrategia Gobierno en línea y específicamente, en el artículo N° 2.2.9.1.2.1 se establecen los componentes de la Estrategia, entre los que se encuentra el de seguridad y privacidad de la información, que comprende las acciones transversales a los demás componentes, tendientes a garantizar la confidencialidad, la integridad y la disponibilidad de la información. Que atendiendo a los lineamientos de la Sentencia C-274 de 2013 de la Corte Constitucional, el acceso a la información pública es un derecho fundamental que cumple al menos tres funciones*

esenciales en nuestro ordenamiento. (i) garantiza la participación democrática y el ejercicio de los derechos políticos. (ii) cumple una función instrumental para el ejercicio de otros derechos constitucionales, ya que permite conocer las condiciones necesarias para su realización. (iii) garantiza la transparencia de la gestión pública, y, por lo tanto, se constituye en un mecanismo de control ciudadano de la actividad estatal." // **Anexo 2: LINEAMIENTOS SOBRE EL FORMULARIO ELECTRONICO PARA LA RECEPCION DE SOLICITUDES DE INFORMACION PÚBLICA.**

MAE.G.GEN.01 – Documento Maestro del Modelo de Arquitectura Empresarial
5. Principios del Marco de Referencia
5.1. Excelencia del servicio al ciudadano
Fortalecer de forma digital la relación de los ciudadanos con el Estado enfocándose en la generación de valor público sobre cada una de las interacciones entre ciudadano y Estado.
5.2. Costo / Beneficio
El criterio de selección de un proyecto de TI debe priorizar el valor público por encima de su costo, de tal forma que se garantice que las inversiones en TI tengan un retorno definido por el beneficio.
5.3. Racionalización
Optimizar el uso de los recursos de TI teniendo en cuenta criterios de pertinencia y reutilización, sin perjuicio de la calidad el servicio y de la operación de la entidad.
5.4. Estandarización
Definir un ecosistema tecnológico estandarizado para controlar la diversidad tecnológica, la complejidad técnica y reducir los costos asociados al mantenimiento de la operación.
5.5. Interoperabilidad
Utilizar los estándares que fortalezcan la plena interoperabilidad entre los sistemas de información e infraestructura tecnológica y que faciliten el intercambio de información entre las entidades y los sectores.
5.6. Co-Creación
Componer soluciones y generar servicios sobre lo ya construido y definido, con la participación de todos los interesados (internos y externos) para garantizar su máximo valor.
5.7. Calidad
Cumplir con los criterios y atributos de calidad definidos para los procesos y soluciones de TI construidas para la entidad.
5.8. Seguridad Digital
Establecer la seguridad y privacidad de la información teniendo en cuenta los lineamientos definidos en la Política de Gobierno Digital.
5.9. Sostenibilidad
Definir las acciones que propendan por el cumplimiento de los objetivos de desarrollo sostenible de las Naciones Unidas.
5.10. Neutralidad tecnológica
Garantizar la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes en la materia, fomentando la eficiente prestación de servicios, el empleo de contenidos y aplicaciones, la garantía de la libre y leal competencia mediante criterios de selección objetivos.
5.11. Foco en las necesidades
Las decisiones sobre el ecosistema tecnológico deben enfocarse en responder y dar solución las necesidades de la Entidad.

6. Dominios

El MAE está compuesto por siete dominios que las entidades deben considerar para realizar los ejercicios de AE completos para alinear las necesidades del negocio con el uso adecuado de las TIC, aquellas entidades que por el tiempo o por los recursos de los que dispone no tiene la capacidad de abordar los siete dominios de forma completa, deben considerar acotar el alcance de cada dominio disminuyendo el nivel de profundidad vertical, el nivel de detalle con el que abordan cada dominio y el alcance horizontal, es decir, la cantidad de procesos y áreas que van a ser impactadas en cada ejercicio de Arquitectura Empresarial. Los dominios del MAE son: Dominio de Planeación de la Arquitectura, Dominio de Arquitectura Misional, Dominio de Arquitectura de Información, Dominio de Arquitectura de Sistemas de Información, Dominio de Infraestructura Tecnológica, Dominio de Arquitectura de Seguridad y Dominio de Uso y Apropiación de la Arquitectura.

7.3. Dominio de arquitectura de información

En las entidades, la información se ha convertido en el principal generador de valor estratégico. La información se usa para responder a las necesidades de los usuarios de las entidades. Los lineamientos de este dominio permiten definir: el diseño de los servicios de información, la gestión del ciclo de vida del dato, al análisis de información y el desarrollo de capacidades para el uso estratégico de la misma. Para este dominio se utiliza el concepto "Componente de Información", que se refiere al conjunto de: datos, información, servicios de información, los flujos de intercambio de información y fuentes de información bajo un mismo nombre.

7.3.3. MAE.LI.AI.03 - Marco de interoperabilidad del Estado

La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe hacer uso del Marco de Interoperabilidad definido por el Estado Colombiano para compartir datos con otras entidades a partir de las necesidades de intercambio de información.

7.3.10. MAE.LI.AI.10 - Apertura de datos

La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar los conjuntos de datos abiertos y asegurar que se diseñen mecanismos que permitan generarlos a partir de los componentes de información. Estos mecanismos de extracción deben estar automatizados para la generación y publicación de conjuntos de datos abiertos en el portal de datos abiertos del Estado.

PA08-DE-001 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN
7.2. ANÁLISIS DE LA SITUACIÓN ACTUAL

Este apartado comprende un entendimiento estratégico de la Entidad, así como un diagnóstico teniendo en cuenta los dominios del marco de referencia de arquitectura Empresarial (MAE). El Instituto para la Economía Social - IPES, elaboró un análisis a partir del cumplimiento de la Política de Gobierno Digital teniendo en cuenta los dos componentes y los tres habilitadores transversales; permitiendo así contar con una medición del nivel madurez tecnológico y una línea base para proyectar la visión de lo que se espera en materia de gestión de TI en el Instituto.

7.2.1.1. Objetivos Estratégicos de TI

El IPES comprende los siguientes objetivos estratégicos alineados en 3 componentes para lograr su misión:

Beneficiarios
- *Ofrecer mejores servicios a través de la herramienta misional.*
- *Fortalecer estrategias para obtener la calidad de los datos e integridad.*
- *Propender por mejoras tecnológicas en los procesos de caracterización.*

Procesos Internos
- *Analizar, diseñar, desarrollar nuevas funcionalidades en los sistemas de información.*
- *Implementar funcionalidades en desuso con el apoyo de los directivos.*
- *Actualizar procedimientos incorporando las herramientas tecnológicas de la entidad.*
- *Apoyar en la optimización de procesos misionales.*

Capacitación
- *Definir estrategias de apropiación de los sistemas de Información, que incluya socialización, sensibilización y capacitación.*
- *Fortalecer el uso de la tecnología.*

7.2.3. Sistemas de Información

Para soportar los procesos misionales y de apoyo en la entidad, es importante contar con sistemas de información que se conviertan en fuente única de datos útiles para la toma de decisiones ejecutivas. A continuación, se mencionan los sistemas de información en los que se soportan los diferentes procesos de la entidad, un análisis de la situación actual de los mismos.

Recomendación:
- Documentar las actividades de control relacionadas con el proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, en el flujo de actividades del procedimiento, con la inclusión de los 6 elementos de control dado por la Guía de Administración del Riesgo y el Diseño de Controles (DAFP, 2020).
- Fortalecer una metodología para el desarrollo de los proyectos a nivel tecnológico que estén definidos para conocer quién es el responsable de cada proyecto (sponsor y líderes de proyecto), ciclo de vida, cuáles son los objetivos y los alcances, como se hace, cuáles son sus riesgos y controles, retorno de inversión y su mantenimiento.
- Fortalecer la documentación de las aplicaciones para asegurar la continuidad del negocio ante la ausencia o renovación del personal involucrado en los proyectos TIC (Tecnologías de la Información y Comunicación).
- En PA08-DE-001 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN indicar en el marco de referencia de arquitectura Empresarial (MAE) cuales son los dominios aplicados y como los aplica.

Connotación: Administrativa.

Proceso: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS
Procedimientos: PR-131 Monitoreo Acceso a los Medios de Procesamiento de Información

No.: 2
DEFICIENCIAS FUNCIONALES DEL SOFTWARE GOOBI

Responsable de las acciones de mejora: SDAE

Se ha evidenciado que existe un software para el desarrollo de las actividades operativas del IPES, hay tareas que se están realizando de manera manual y no se puede tener un registro confiable de sus transacciones debido a que se realiza con hojas de cálculo.

Se evidenció que algunos usuarios finales del aplicativo no acceden a GOOBI como medio de procesamiento de información.

Las pruebas de software funcionales ayudan a conocer y entender el beneficio del desarrollo y poder reducir la cantidad de errores y así evitar que estos sean entregados al clientes y usuario final; para esto podemos realizar diferentes tipos de pruebas:

- Pruebas funcionales
- Pruebas no-funcionales
- Pruebas estructurales
- Pruebas de manejo de cambios

En las entrevistas realizada en SAF de los siguientes módulos:

- Modulo: Operaciones de Ingresos (Cartera)
- Modulo: Talento Humano (Provisiones de Nómina)
- Modulo: Almacén
- Modulo Tramites y expedientes
- *Product Owner*/Analista de requerimientos de SAF

Se evidenció que la aplicación GOOBI no está agregando valor a las siguientes partes interesadas de acuerdo a los siguientes resultados de las pruebas de recorrido:

- **Modulo: Talento Humano (Provisiones de Nómina):**

Se evidenció en el área tiene asignado el módulo de Nomina, pero no han podido utilizarlo debido a que ni si quiera les carga en el equipo que está instalado que pertenece al usuario Nelson Sanabria (Profesional Universitario Encargado), y los otros usuarios funcionales no lo tienen instalado.

No se puede realizar de manera automatizada la nómina electrónica que está regulada por 013 del 11 de febrero de 2021 de la DIAN, en donde se establece para el reporte mensual que se deben enviar los primeros 5 días de cada mes, el proveedor IT GOP, no aparece como proveedor autorizado para prestar este servicio, como se indica en los puntos del 15 al 19:

> *"15. Sujetos obligados a generar y transmitir, para validación el documento soporte de **pago de nómina y las notas de ajuste del documento soporte de pago de nómina***
> *16. Transmisión del documento **soporte de pago de nómina electrónica y de las notas de ajuste del documento soporte de pago de nómina electrónica**:*
> *17. Validación del documento soporte de pago de nómina electrónica y de las notas de ajuste del documento soporte de pago de nómina electrónica.*
> *18. **Valor devengado de nómina:***

19. ***Valor deducido de nómina"***

Ver **ANEXO 3,** con los proveedores autorizados puede ser verificado en https://www.dian.gov.co/impuestos/factura-electronica/proveedores-tecnologicos/Paginas/Proveedores-tecnologicos-autorizados-DIAN.aspx

Se evidenciaron registros de nómina llevada en hojas de cálculo desde el año 2008, afectando la optimización de los servicios del IPES.

Como se evidencia en el acta de la mesa de trabajo con los usuarios de nómina. Ver **ANEXO 4**.

- **Modulo: Operaciones de Ingresos (Cartera)**

El módulo de cartera no se encuentra en servicio alternativas comerciales y parcialmente para plazas de mercado, se tiene soportada la cartera de alternativas comerciales en hojas de cálculo de Google (paquete corporativo), para plazas de mercado en Access 2010. Como se evidenció en el acta de la mesa de trabajo el usuario de Cartera-Alternativas Comerciales. Ver **ANEXO 5.**

- **Modulo: Almacén**

El área de almacén realizó un memorando (radicado 00110-817-003989) sobre las inconsistencias que presenta GOOBI en el momento de generar el boletín para contabilidad, informando lo siguiente:

- Caso boletín almacén saldos finales valores negativos.
- Caso bienes inservibles, defectuosos u obsoletos.
- Caso módulos en inventarios por cuentadante.
- Caso bienes que no se ubican.
- Caso módulo recategorizaciones sin uso.
- Caso placas bienes inmuebles con mejoras.
- Creación centro costo centro gastronómico plaza de mercado doce de octubre.
- Caso actualización opción de búsqueda placas características del bien.
- Caso equipos ingresados completos desglose en características del bien.

Como se evidenció en el acta de la mesa de trabajo el usuario de almacén. Ver **ANEXO 6.**

- **Modulo Trámites y Expedientes**

GOOBI como gestor documental:

- En la creación de tablas de retención documental de la gestión documental el software no evidencia la creación la BPMN para la gestión documental.
- No se evidencia la generación de expedientes electrónicos, se registra los diferentes tipos documentales internos y externos de las comunicaciones oficiales enviadas, recibidas e internas.
- No se tiene interoperabilidad con las aplicaciones.

- No se genera alarmas.
- No permite la creación, administración y ejecución de flujos de trabajo electrónicos.
- Los radicados se deben generar de manera manual realizando siempre la solicitud a la unidad de correspondencia de la entidad, realizando reprocesos a los gestores líderes.
- Cuando se realiza un radicado no se permite adjuntar archivos digitales como audio, videos, entre otros.
- El tema de preservación y conservación a largo plazo teniendo en cuenta hoy en día el tema de conservación tecnológica, con la finalidad de los archivos con los objetivos de consulta, conservar y preservación.

Como se evidenció en el acta de la mesa de trabajo el usuario de Trámites y expedientes. Ver **ANEXO 7.**

La ausencia de calidad de software como una etapa importante en los proyectos de ingeniería de software, no permite validar la funcionalidad, la algoritmia y mitigar las fallas.

Desconocimiento de lineamientos, políticas y directrices asociadas al sistema de gestión de seguridad y privacidad de la información en los sistemas de información, lo cual afecta la pérdida o manipulación de la confidencialidad e integridad de la información, provocando violaciones a las políticas de seguridad, lo cual impacta los servicios misionales de la entidad llegando a afectar la imagen y credibilidad del IPES.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR-133 Otorgar acceso a los medios de procesamiento de información, presentó el siguiente Diseño de Control:

Control 1: Matriz de Riesgos y Controles:
Los profesionales del área de sistemas informan a los usuarios sobre las responsabilidades en el uso de los activos de información, desde el momento de la asignación de acceso a la plataforma tecnológica institucional. así como paralelamente desde el proceso de Gestión de Seguridad de la información y Recursos Tecnológicos se realizan jornadas de sensibilización a usuarios.

Resolución No.047 de 2020, Documento Estratégico DE-039 Plan de Seguridad y Privacidad de la Información. Ítem 6.3 Acciones Particulares a Seguir, Tabla 12. Cumplimiento.

Actividad 1: Actualizar el Normograma
Actualizar el Normograma de Seguridad de la información.

Diseño del Control: De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidades en el procedimiento, el manejo de excepciones y Evidencia de la ejecución del control, el procedimiento no está asegurando recibir un producto de acuerdo a los estudios

previos, las evidencias no soportan en totalidad el cumplimiento del procedimiento PR- 154 EJECUCION Y CIERRE DEL EXPEDIENTE CONTRACTUAL ACTIVIDAD DE CONTROL.

Valoración comentarios del Auditado

Los comentarios dejados por la SDAE fueron:

> *"No se acoge la observación ya que el auditado no tuvo conocimiento de las entrevistas realizadas en SAF, así como el auditor no corroboró la información con el PGSIRT, lo que lleva a las imprecisiones de la observación.*
> *En los anexos se demuestra cómo las funcionalidades del software GOOBI no presentan las deficiencias mencionadas, sino se evidencia de uso de las mismas y la incorrecta operación de algunas, por lo que el PGSIRT ha realizado diversas estrategias de propuestas y comunicaciones para solventar la causa del uso inapropiado de la herramienta.*
> *El proceso de nómina se realiza a través del sistema GOOBI hecho fácilmente demostrable ya que es la única herramienta empleada para gestionar el egreso de los pagos, los parafiscales, la emisión de Certificado de Disponibilidad*
> *Presupuestal, el registro presupuestal, entre otros, todo el flujo de información se realiza en la herramienta, por temas de pruebas y diferencias conceptuales en la formulación, así como la ausencia de datos históricos ha llevado a que se realice el paralelo con hojas de cálculo en el cargue de novedades, lo que no conlleva a indicar que no opere la funcionalidad.*
> *Como tal no existe una funcionalidad de cartera ya que la misma es un flujo de información que involucra las siguientes actuaciones (Todas se operan en GOOBI actualmente):*
> *Gestión de terceros*
> *Gestión de contratos comerciales*
> *Gestión de facturación*
> *Gestión de recaudo*
> *Gestión contable*
> *Gestión de recibos*
> *Operaciones de ingreso"*

Análisis ACI: De acuerdo a la resolución IPES 050 de 2021 "Estatuto de Auditoría", en su artículo 12:

> *"Artículo 12. Autoridad de la Asesoría de Control Interno. El/la Asesor(a) de Control Interno y su equipo de personal, con estricta responsabilidad por la confidencialidad y la salvaguarda de la información y de los registros, están autorizados a:*
>
> *12.1 Asignar recursos, establecer frecuencias, seleccionar temas, determinar alcances de trabajo y aplicar las técnicas requeridas para cumplir los objetivos de auditoría.*
> *12.2 Acceder libre y sin restricciones a todos los registros, información, bases de datos, personal y bienes del Instituto que sean necesarios para lograr los objetivos y responsabilidades de la Asesoría de Control Interno, incluso aquellos bajo el control de terceros.*
> *12.3 Requerir y obtener la colaboración pronta y necesaria del personal en las áreas del Instituto en las cuales se desarrollan las auditorías, así como de otros servicios especializados propios y ajenos al Instituto."*

Siendo la ACI autónoma para determinar los procedimientos a aplicar en el ejercicio de auditoría, no se realizó invitación al responsable del proceso GSIRT porque una de las pruebas de auditoría consistió en corroborar la eficiencia y eficacia de GOOBI, con los usuarios en el flujo de operaciones, quienes son finalmente quienes hacen uso día a día del mismo para optimizar sus operaciones desde el apoyo de la plataforma tecnológica, en el mismo sentido, el auditado ha insistido con las evidencias suministradas indicando que los procesos estaban optimizados con las aplicaciones del IPES. De lo cual afirma la

supervisión y los apoyos de la supervisión de los contratos suscritos con IT GOP que existe eficiencia y eficacia en el servicio contratado; afirmación que, contrastada con la realidad, es parcialmente cierta. Por ello, se requiere establecer acciones efectivas de mejorar para el cierre de brechas.

Respecto a los anexos (actas de las mesas de trabajo, ANEXO 4, 5 y 6) no se pudo evidenciar con los usuarios diversas estrategias de propuestas y comunicaciones para solventar la causa del uso inapropiado de la herramienta, y tampoco se tuvo evidencia por parte de los auditados, información que debió comunicarse durante el tiempo de ejecución de la auditoría.

En las mesas de trabajo con los usuarios finales de nómina (ver ANEXO 4) se notificó el no uso de GOOBI desde el año 2008, como evidencia se suministraron varias hojas de cálculo que se utilizan para llevar la nómina, además que a la fecha tampoco se puede subir la nómina electrónica, al ser una herramienta con aproximadamente 14 años de maduración en el IPES no se debería tener trabajando de forma parcial como se indica en la respuesta de la réplica, en la mesa de trabajo los usuarios suministraron hoja de cálculo en donde se realizaba la gestión el egreso de los pagos, los parafiscales; además que el pago de nómina electrónica, COMPENSAR como caja de compensación del IPES estaba ayudando al IPES a subir la nómina con su proveedor.

En el caso de cartera, como se indica en la observación, la evidencia es que se usa de manera parcial y en ALTERNATIVAS COMERCIALES no es posible su uso. (Ver ANEXO 5).

El usuario de Cartera para soportar y optimizar el proceso utiliza hojas de cálculo de GOOGLE para poder controlar la gestión de las alternativas comerciales para poder gestionar la atención de los usuarios.

La gestión de terceros, gestión de contratos comerciales, gestión de facturación, gestión de recaudo, gestión contable, gestión de recibos y operaciones de ingreso se encuentran en cartera de manera parcial.

Los comentarios dejados por la SDAE fueron:

> *"La afirmación "No se otorga acceso a GOOBI como medios de procesamiento de información, no se mantiene acceso a los medios de procesamiento de información, mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables dentro de la entidad, ni tampoco registro del responsable." no es cierta ya que múltiples servidores públicos, de diferentes procesos y diversas sedes tienen acceso al sistema de información según su rol y el perfil identificado."*

Análisis ACI: Cuando se realiza referencia a: *"No se otorga acceso a GOOBI como medios de procesamiento de información, no se mantiene acceso a los medios de procesamiento de información, mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables dentro de la entidad, ni tampoco registro del responsable"*, se está comunicando que se usan medios de información que no permiten registrar y controlar el ingreso y modificación de la información.

Los comentarios dejados por la SDAE fueron:

> *"En el caso de almacén "El área de almacén realizó un memorando (radicado 00110817-003989) sobre las inconsistencias que presenta GOOBI en el momento de generar el boletín para contabilidad", al efectuar una auditoria objetiva se evidencia que no corresponde a inconsistencias en la funcionalidad del sistema, la causal de los errores en la salida del sistema obedece a que se han solicitado múltiples ajustes (recategorizaciones) por fuera del sistema, lo que lleva a modificar datos de vigencias ya cerradas y reportadas, este ejercicio puede atender a consecuencias de las modificaciones por los cambios en las normas internacionales contables, lo que afecta de forma integral la contabilidad, la depreciación de bienes, entre otros. Para el caso de trámites y expedientes: el IPES en ninguna de las contrataciones para el software GOOBI ha requerido las características propias de un gestor documental y así no se requiriera la entidad a ha decidido emplear solo la funcionalidad de radicación, cuando existen funcionalidades de anexos, adjuntos, control de radicación, sin embargo por ahora los trámites y servicios internos así como los procedimientos se enfocan en la información física y no se brinda relevancia a la documentación electrónica y digital."*

Análisis ACI: Para el memorando radicado 00110817-003989 de almacén no se puede aceptar la observación, cuando indican: *"al efectuar una auditoría objetiva se evidencia que no corresponde a inconsistencias en la funcionalidad del sistema, la causal de los errores en la salida del sistema obedece a que se han solicitado múltiples ajustes (recategorizaciones) por fuera del sistema, lo que lleva a modificar datos de vigencias ya cerradas y reportadas, este ejercicio puede atender a consecuencias de las modificaciones por los cambios en las normas internacionales contables, lo que afecta de forma integral la contabilidad, la depreciación de bienes, entre otros",* esto da entender que cuando se realizaba alguna modificación en programación o parametrización se debe por salir a producción sin realizar pruebas correctamente, afectando los datos ya registrados con anterioridad.

Los comentarios dejados por la SDAE fueron:

> *"Es conveniente expresar que los diferentes módulos/documentos del S.I. goobi GRP son funcionales, y en la actualidad existe un proceso de cumplimiento contractual frente al ajuste de los mismos, esto acorde a las necesidades funcionales y administrativas actuales de la Entidad.*
> *Es importante mencionar que los ajustes a los módulos del sistema de información no nacen en el área de sistemas (PGSIRT) sino en las áreas funcionales donde se ha evidenciado que en sus procesos es necesario realizar ajustes, optimización y acatamiento de los mismos para operar de forma adecuada la herramienta administrativa. En los últimos años se han realizado migraciones de información (cartera y nómina) y en el presente se encuentra en marcha una adicional con el fin de tener al día la cartera y a partir de allí ir haciendo las mejoras continuas en los procesos administrativos y dejando de lado recursos externos como fuente de información (excel, access, etc)*
> *Desde PGSIRT también se han hecho propuestas a SAF, para mejoras de algunos procedimientos con el fin de optimizar y fortalecer la labor administrativa e ir cerrando brechas. En el contrato suscrito con el proveedor Goobi vigencia 2021 se está realizando un trabajo conjunto con las áreas funcionales y técnica para sacar adelante los procesos (módulos) que no se estaban utilizando pero que si están configurados en el Sistema Integrado de Información Goobi (Adjunto Estudio Previo Contrato Goobi vigencia 2021)*
> *Procesos requeridos*
> *● Información exógena: Asegurar que el sistema genere toda la información requerida para reportar a la DIAN.*
> *● Información exógena: Asegurar que el sistema genere toda la información requerida para reporte a la Secretaría de Hacienda Distrital*
> *● Generación de pagos masivos en el sistema (egreso). Proceso que permita el registro de pagos por lotes en el sistema.*

● Generación de recaudos (multicash o reportes ACH). Proceso que permita el registro de los comprobantes de ingreso/recaudos a partir de un archivo plano o una hoja de cálculo, manteniéndose la identificación del recibo pagado.
● Planilla de Autorizaciones/Órdenes de pago
● Proceso que permita el registro de autorizaciones y órdenes de pago a través de plantillas para que el proceso se realice de forma masiva.

Análisis ACI: Para el caso de trámites y expedientes el contrato 1499 de 2012 indica que se contrató:

Gestión Documental
- Cambiar el nombre del icono CARPETAS por GESTIÓN DOCUMENTAL.
- Cambiar el componente GESTIÓN DOCUMENTAL por OFICINA DE RADICACIÓN.
- Datos estadísticos para la generación de indicadores
- Seguimiento de las comunicaciones oficiales; para evidenciar los plazos establecidos de respuesta oportuna de
- estas (semáforos estableciendo plazos de respuesta)
- Consulta en tiempo real de los trámites y las personas responsables de dar respuesta a las comunicaciones (fecha de
- asignación, trámite necesario y trámite efectuado)
- Radicación masiva.
- Digitalización de soportes en los procesos
- Archivo

El contrato 516 de 2017 indica que se contrató *Manejo de las funcionalidades de Gestión Documental.*

Cuando indican *"la entidad a ha decidido emplear solo la funcionalidad de radicación, cuando existen funcionalidades de anexos, adjuntos, control de radicación, sin embargo por ahora los trámites y servicios internos así como los procedimientos se enfocan en la información física y no se brinda relevancia a la documentación electrónica y digital"*, se reconoce la falta de cumplimiento de la *Directiva Presidencial 4 de 2012* (Eficiencia administrativa y lineamientos de la política cero papel en la administración pública).

Cuando el auditado indica: *"en el presente se encuentra en marcha una adicional con el fin de tener al día la cartera y a partir de allí ir haciendo las mejoras continuas en los procesos administrativos y dejando de lado recursos externos como fuente de información (excel, access, etc). // Desde PGSIRT también se han hecho propuestas a SAF, para mejoras de algunos procedimientos con el fin de optimizar y fortalecer la labor administrativa e ir cerrando brechas. // En el contrato suscrito con el proveedor Goobi vigencia 2021 se está realizando un trabajo conjunto con las áreas funcionales y técnica para sacar adelante los procesos (módulos) que no se estaban utilizando pero que si están configurados en el Sistema Integrado de Información Goobi (Adjunto Estudio Previo Contrato Goobi vigencia 2021)",* se puede tener en cuenta para el plan de mejoramiento, la auditoria comprende vigencias pasadas y no la presente. Sin embargo, como buena práctica es necesario documentar estos controles asociados.

La información suministrada en la réplica corresponde de a partir del 30 de abril de 2021, se recuerda que la auditoria tenía vigencia de enero de 2020 a abril 2021, únicamente se

podría aceptar el FO-069 MEMORANDO V9 - Propuestas para SAF, pero no es posible aceptarlo debido a que no se presentó en el momento de la auditoría, teniendo como limite el día 29 de julio cuando se realizó la socialización.

El resto de evidencias aplican para el plan de mejoramiento en su respectivo momento.

En mérito de lo expuesto, el hallazgo se mantiene y se debe establecer un plan de mejoramiento por parte del responsable del proceso.

Riesgo Asociado: Extracción, manipulación o adulteración de información confidencial o reservada almacenada en los sistemas de información institucionales, para fines de beneficio personal o de terceros ajenos a la misión institucional: El acceso a la data almacenada en los activos de información, sistemas y servicios informáticos institucionales (HEMI, GOOBI, Correo, Directorio activo, file server, bases de datos, documentos u otros), puede generar escenarios en los cuales los usuarios de acuerdo a su perfil pudiesen identificar posibles beneficios particulares que conduzcan a generar conductas no autorizadas o legales frente a la manipulación, alteración, sustracción de la información digital institucional de la Entidad.

Normatividad o Criterio:

000013 RESOLUCIÓN NÚMERO (11 FEB 2021), Por la cual se implementa y desarrolla en el sistema de facturación electrónica la funcionalidad del documento soporte de pago de nómina electrónica y se adopta el anexo técnico para este documento: "*Que de conformidad con el numeral 6 del artículo 1.6.1.4.3. del Decreto 1625 de 2016, Decreto Único Reglamentario en Materia Tributaria y el numeral 6 del artículo 7 de la Resolución 000042 del 5 de mayo de 2020, no están obligadas a expedir factura de venta y/o documento equivalente, "Las personas naturales vinculadas por una relación laboral o legal y reglamentaria y los pensionados, en relación con los ingresos que se deriven de estas actividades. // Que, en virtud de lo anterior, el soporte de pago de nómina electrónica se configura como documento soporte de costos, deducciones o impuestos descontables, que se derivan de pagos que se realizan en virtud de una relación laboral o legal y reglamentaria y de los pagos a los pensionados a cargo del empleador. // Beneficiario del pago: Se entiende como beneficiario del pago, a las personas naturales vinculadas mediante una relación laboral o legal y reglamentaria y los pensionados a cargo del empleador, en relación con estas actividades. // **15.Sujetos obligados a generar y transmitir, para validación el documento soporte de pago de nómina y las notas de ajuste del documento soporte de pago de nómina:** Son aquellos contribuyentes que realizan pagos o abonos en cuenta que se derivan de una vinculación por una relación laboral o legal y reglamentaria y por pagos a los pensionados a su cargo, que requieran soportar los costos y deducciones en el impuesto sobre la renta y complementarios e impuestos descontables en el impuesto sobre las ventas -IVA cuando aplique. // 1**6.Transmisión del documento soporte de pago de nómina electrónica y de las notas de ajuste del documento soporte de pago de nómina electrónica:** Es el procedimiento electrónico mediante el cual se remite a la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales -DIAN, la información que contendrá el documento soporte de pago de nómina electrónica y las notas de ajuste al documento soporte de pago de nómina electrónica. // **17.Validación del documento soporte de pago de nómina electrónica y de las notas de ajuste del**

documento soporte de pago de nómina electrónica. *Es el procedimiento que genera un documento electrónico por parte de la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales -DIAN, que contiene la verificación de las reglas de validación del documento soporte de pago de nómina electrónica y de las notas de ajuste al documento soporte de pago de nómina electrónica, cumpliendo con los requisitos, términos, mecanismos técnicos y tecnológicos que para el efecto establezca la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales -DIAN. //* ***18.Valor devengado de nómina****: Son los conceptos que constituyen ingresos de nómina para el beneficiario del pago que hacen parte integral del documento soporte de pago de nómina electrónica y de las notas de ajuste del mencionado documento, conforme a lo indicado en el «Anexo técnico documento soporte de pago de NÓMINA ELECTRÓNICA». //* ***19.Valor deducido de nómina:*** *Son los conceptos que se detraen de los valores devengados de nómina por parte del beneficiario del pago y que hacen parte integral del documento soporte de pago de nómina electrónica y de las notas de ajuste del mencionado documento conforme a lo indicado en el «Anexo técnico documento soporte de pago de NÓMINA ELECTRÓNICA»*

En los contratos se indica:
Obligaciones Generales

- *Presentar al supervisor del contrato los informes y los soportes que sean requeridos sobre la ejecución del objeto y las obligaciones contractuales. Cuando sean solicitados por el mismo.*
- *Ejecutar el objeto y las obligaciones contractuales de manera eficaz y oportuna. así como atender los requerimientos que le sean efectuados por el supervisor del contrato y/o por la Dirección General de la Entidad, en los términos y las condiciones pertinentes.*
- *Cumplir con el objeto y las obligaciones contractuales conservando un comportamiento de cordialidad y buen trato con la población sujeto de atención del Instituto para la Economía Social, así como con los funcionarios y contratistas de la Entidad, tanto en las instalaciones de la misma como donde quiera que se desarrollen las actividades derivadas del contrato.*
- *Dirigir las observaciones. quejas o reclamaciones relacionadas con la obligaci6n anterior, al supervisor del contrato.*
- *Ejecutar el contrato adjudicado en los términos y condiciones señalados en los estudios y documentos previos y la propuesta presentada por el CONTRATISTA, de conformidad con las normas legales que los regulen.*

Obligaciones de los supervisores (Contrato 307, 1080, 1498, 179, 516, 692, 24)

- *Aprobar los informes de ejecución y de cumplimiento presentados por los contratistas que se encuentran bajo su supervisión, teniendo presente que dicha aprobaci6n implica la cabal ejecución del objeto contractual.*
- *Verificar las vigencias de las garantías de seriedad y las que amparen los riesgos propios de la etapa contractual y realizar los requerimientos necesarios para lograr el cumplimiento de esta obligaci6n par parte del contratista, con base en las prórrogas, adiciones o suspensiones que puedan presentarse dentro del proceso contractual. Las garantías y/o sus modificaciones deberán allegarse dentro de las plazas establecidos en el pliego de condiciones definitivo a la Subdirección Jurídica y de Contratación.*

Recomendación:

- Documentar las actividades de control relacionadas con el proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, en el flujo de actividades del procedimiento, con la inclusión de los 6 elementos de control dado por la Guía de Administración del Riesgo y el Diseño de Controles (DAFP, 2020).
- Fortalecer una metodología para el desarrollo de los proyectos a nivel tecnológico que estén definidos para conocer quién es el responsable de cada proyecto (sponsor y líderes de proyecto), ciclo de vida, cuáles son los objetivos y los alcances, como se hace, cuáles son sus riesgos y controles, retorno de inversión y su mantenimiento.
- Aplicar una metodología para pruebas funcionales.
- Fortalecer las capacitaciones y medir el conocimiento de los usuarios finales con el fin detectar el correcto uso de la herramienta y a través de estas actividades conocer a tiempo las posibles falencias o necesidades de actualización de las herramientas tecnológicas.

Connotación: Administrativa.

Proceso: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS
Procedimientos: PR-136 Atención de Mesa de Ayuda

No.: 3
DEFICIENCIAS EN GESTIÓN DE ATENCIÓN EN MESA DE AYUDA

Responsable de las acciones de mejora: SDAE

En la revisión realizada de la muestra de reportes de Mesa de Ayuda GOOBI y HEMI, respecto a los reportes de enero, mayo, octubre de 2020 y febrero de 2021, para un total de 24 registros, se observó el incumplimiento de los siguientes KPI:

- La métrica de un tiempo de respuesta de 15 a 20 minutos para dar solución a un ticket de conformidad con la actividad de control establecida en el procedimiento.
- El monitoreo por parte del Técnico del Equipo de Sistemas.

Se observaron las siguientes deficiencias de control:

1. *Deficiencias en la medición de la atención por el cierre por parte de los usuarios*

La gestión de la mesa de ayuda presentó carencias en la optimización de los procesos y los KPI (*Key Performance Indicator*), debido a que existe inconsistencias en la encuesta de satisfacción que no corresponde a la descripción del proceso PR-136 ATENCIÓN MESA DE AYUDA, en donde se omitieron conceptos de buenas prácticas y recomendaciones de marcos definidos como ITIL, y así evidenciar el cumplimiento del servicio de atención, medible para la gestión que realizan los agentes de la mesa de ayuda.

Cómo muestra se tuvo los siguientes incidentes de mesa de ayuda de GOOBI y HEMI:

▪ 31613	▪ 31665	▪ 31978	▪ 32217
▪ 31614	▪ 31672	▪ 31979	▪ 32241

- 31628
- 31629
- 31630
- 31641
- 31862
- 31863
- 31943
- 31955
- 31982
- 32209
- 32213
- 32216
- 32247
- 32271
- 32275
- 32285

Se evidenciaron que existe cuatro (4) incidentes en nivel II sin calificar, según el PR-136 ATENCIÓN MESA DE AYUDA no se da por cerrado hasta su calificación.

Los incidentes que continuaban abiertos son:

- 31640 de SAF-SERVICIOALUSUARIO
- 31675 de SDAE-SISTEMAS
- 31863 de ACI
- 32216 de SFE-FORMACIONYCAPACITACION

Para cerrar un caso se depende de la calificación del usuario que solicitó el servicio, esto conlleva a que la mesa de ayuda no lleve un récord del cumplimiento de los tiempos establecidos. No es posible medir su efectividad y eficacia porque la herramienta de *Help Desk* y su proceso no permite medir los tiempos de respuesta, dado que se depende de la calificación del usuario que solicitó el servicio, la herramienta de *Help Desk* no permitió a los agentes cerrar el servicio prestado y no ofrece la posibilidad de un proceso automatizado.

En el contenido del PR-136 ATENCIÓN DE MESA DE AYUDA y el 047 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES no se observó la aplicación de buenas prácticas como ITIL y norma ISO 20000 para la efectiva y eficiente atención a los usuarios y resolución de incidentes.

La ausencia de la aplicación de *frameworks,* guías, normas y buenas prácticas dificulta la medición (KPI) del uso de los recursos y la mejora continua en cualquier organización.

2. *Ausencia en definir ANS y OLA*

En el procedimiento PR-136 ATENCIÓN DE MESA DE AYUDA no se evidenció una separación de los ANS/SLA (Acuerdos de niveles de servicio/ *Service Level Agreement*) y OLA (Acuerdo de Nivel Operacional). La ausencia de esto no permite definir los KPI (*key performance indicator*) son elementos de la gestión de procesos de negocio, los ANS son los acuerdos de nivel de servicio que el proveedor ofrece a su cliente, y el OLA son los acuerdos que el IPES brinda a sus usuarios.

La gran mayoría de incidentes ocasionados en HEMI se evidenció que se está realizando por medio de correos electrónicos enviados a:

- jepenap@ipes.gov.co
- soporte@goobi.net

En el contenido del PR-136 ATENCIÓN DE MESA DE AYUDA y el 047 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

no se observó la aplicación de buenas prácticas como ITIL y norma ISO 20000 para la efectiva y eficiente atención a los usuarios y resolución de incidentes.

La ausencia de definir los OLA posee importancia para para abordar y resolver problemas en los procesos TI estableciendo un conjunto específico de criterios y definiendo el conjunto de servicios del que cada equipo es responsable. La separación de y de SLA es importante para diferenciar el servicio a nivel interno en la operación y el servicio prestado a terceros (clientes).

3. *Ausencia de pruebas de GOOBI antes de salir a producción*

Para asegurar el funcionamiento de la operación de los sistemas de información y las políticas de MIPG no se realizan pruebas del aplicativo GOOBI, todas las actualizaciones se han enviado directamente a producción sin pasar por los servidores de pruebas del IPES, en cada una de las cuales se detiene el servicio del aplicativo GOOBI en horas no laborales, lo que se comunica a los usuarios mediante correos masivos, tal como se identificó en el acta de reunión con el contratista de SDAE encargado de GOOBI el 25-jun-2021. Ver **ANEXO 9.**

De acuerdo al marco ITIL, el objetivo de atender un incidente es restaurar los servicios de la operación normal tan pronto como sea posible y minimizar el impacto adverso sobre las operaciones del negocio. En contrario, un requerimiento es una propuesta formal para hacer un cambio, incluye los detalles del cambio propuesto y puede ser registrado en papel o electrónicamente. A menudo, el término es mal utilizado para referirse a un registro de cambio o al propio cambio.

De manera concordante, la norma ISO 20000/ITIL “Calidad de Servicios TI” “gestión de servicios de tecnologías de la información (TI)”, e ISO 27001 solicita frente a la Gestión de Cambio, los siguientes controles:

Gestión del Cambio: (Transición del Servicio) El Proceso encargado del control del Ciclo de Vida de todos los Cambios. El objetivo primario de la Gestión del Cambio es permitir que se realicen los Cambios beneficiosos, con el mínimo de interrupción de los Servicios de TI.

ISO 27001:2013
10.1.2 Gestión de Cambios
10.1.4 Separación de los recursos de desarrollo, prueba y operación
12.5.1 Procedimiento de control de cambios
12.5.3 Restricciones en los cambios de paquetes de software

Gestión de cambios de los sistemas de información - LI.SIS.17(MINTIC)
La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar formalmente un procedimiento de control de cambios para los sistemas de información de la institución.

Código: LI.SIS.17
Ámbito: Ciclo de vida de los Sistemas de Información
Dominio: Sistemas de Información

Lineamiento: En los servicios de soporte de los sistemas de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe formalizar la petición de nuevas funcionalidades o de cambios a las existentes, a través de un procedimiento de control de cambios.

Durante la vigencia 2020 se realizaron una actualización confirmada el 5 de agosto de 2020 y hasta abril de 2021 no se tiene confirmado actualizaciones del aplicativo GOOBI. En el IPES los requerimientos son entendidos como incidentes. Los requerimientos para el aplicativo GOOBI están siendo tomados por la mesa de ayuda o por correo electrónico, y no se evidenció la validación de la toma de cada uno de los requerimientos que implican cambios para GOOBI.

No se revisa el cumplimiento funcional de los requerimientos solicitados, debido a que se pasan las actualizaciones de una vez a ambiente de producción y no en pruebas, lo que no permite asegurar el control de cambios, la estabilidad del servicio y la no afectación de la continuidad de la operación.

Al existir ausencia en las pruebas de calidad de software es faltar a una de las actividades de cualquier proyecto de tecnología, la falta de realizar estas pruebas nos puede llevar a que las funciones indicadas no son realizadas de la manera correcta y además puede afectar módulos, funciones, clases y/o servicios que hacen parte su correcto

En los responsables del PR-136 se establece que: ***El personal profesional / técnico de Sistemas:*** *Será el encargado de gestionar los servicios solicitados a través de los medios establecidos en la actividad 2, a su vez es el responsable de garantizar la gestión de todos los incidentes y requerimientos reportados a la mesa de ayuda, generar análisis y reportes que lleven a la mejora continua de los procedimientos de resolución de incidentes y solicitudes.*

Sin embargo, no se obtuvo evidencia de la atención de los requerimientos efectuados respecto a mejoras solicitadas por los usuarios de GOOBI. En las visitas de auditoría efectuadas a la SAF, se evidenció que algunas funcionalidades no están operando en GOOBI, respecto a los módulos:

- Operaciones de Ingresos (Cartera)
- Talento Humano
- Trámites y Expedientes
- Almacén

Visita del 13-jul-2021: Los usuarios encargados de gestionar la nómina indican que esta gestión se realiza llevando en archivos en Excel desde el 2008. Ver **ANEXO 4.**

Visita del 14-jul-2021: El usuario de Cartera-Alternativas Comerciales indica que esta gestión de alternativas comerciales se está realizando con hojas de cálculo de Google del paquete corporativo. De manera parcial, para la administración de la cartera plazas de mercado las funciones:

- Alternativa comercial no funciona

- Parcialmente plazas

Ver **ANEXO 5.**

Visita del 14-jul-2021: El usuario de Almacén manifestó que se vienen presentando inconsistencias en saldos finales, valores negativos en los reportes de inventarios, reintegros y salidas de bienes inservibles, defectuosos u obsoletos, control de cuentadantes, recategorizaciones sin uso, creación de centros de costo. Ver **ANEXO 6.**

Visita del 19-jul-2021: El usuario líder de Gestión Documental evidenció que los requerimientos solicitados no se cumplen. Ver **ANEXO 7.**

Al existir ausencia en módulos funcionales en la operación de una aplicación en las pruebas de calidad de software es faltar a una de las actividades de cualquier proyecto de tecnología, la falta de realizar estas pruebas nos puede llevar a que las funciones indicadas no son realizadas de la manera correcta y además puede afectar módulos, funciones, clases y/o servicios que hacen parte su correcto.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR-136 ATENCIÓN MESA DE AYUDA, presentó el siguiente Diseño de Control:

Control 1: PR-136: Actividad 2: Coordinar la asignación (Según el problema): El técnico que coordina revisa identifica y verifica el tipo de requerimiento. // Vía telefónica: El personal designado para la atención indicará de manera explícita y remota al usuario para la atención y solución a su requerimiento. // Mesa de ayuda: Se informará al usuario por este mismo medio el número del ticket que le fue asignado, el estado de ticket de su solicitud y el técnico asignado para su atención.

Actividad 3: Analizar y asignar mesa de ayuda: Se realiza análisis y se asigna según el nivel. ¿La solicitud está dentro de la competencia? SI: Realizar diagnostico; NO: Se rechaza se hace el cierre en el sistema. // Actividad 5: Solucionar requerimiento: El técnico asignado soluciona el requerimiento. // Actividad 7: Revisar Requerimiento. El especialista o proveedor revisa el requerimiento. ¿El requerimiento se soluciona? SI: Continua con la actividad 6; NO: Fin del procedimiento // Actividad 8: Verificar y realizar prueba del equipo Se verifica que el equipo funcione bien, se realiza prueba. ¿Funciona el equipo? SI: Continua con la actividad 10; NO: Regresa a la actividad 6 // Actividad 10: Realizar encuesta para cierre de la mesa de ayuda. El usuario realiza la calificación de la mesa de ayuda atendida y realiza el cierre.

De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidad en el manejo de excepciones respecto a la actividad 10 "*Actividad 10: Realizar encuesta para cierre de la mesa de ayuda. El usuario realiza la calificación de la mesa de ayuda atendida y realiza el cierre",* en los tickets sin culminar con el ciclo del caso, ósea sin la respectiva aprobación

de cierre por parte de los usuarios. Así mismo en la mesa de ayuda requiere de una mejora continua en el proceso, PR-136 ATENCIÓN MESA DE AYUDA con el fin de poder medir la efectividad del servicio, la mesa de ayuda comienza la atención a tiempo, pero se desconoce el tiempo real de cierre de cada caso.

Control 2:
DE-039 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
5.3.1 Administrador infraestructura Tecnológica
Garantizar la continuidad en la prestación de los sistemas y servicios informáticos que apoyan el cumplimiento de los objetivos y la misión de la entidad, a través de la administración (configuración, pruebas, puesta en operación, migración, actualización. mantenimiento) de los activos de infraestructura tecnológica que soportan la operación informática institucional.

De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidad en el manejo de procedimiento respecto Garantizar la continuidad en la prestación de los sistemas y servicios informáticos a través de la administración (configuración, pruebas, puesta en operación, migración, actualización. mantenimiento).

Valoración Comentarios del Auditado

Los comentarios dejados por la SDAE fueron:

> *"Esta observación no se acoge debido a que la misma se encuentra inmersa en el informe de auditoría regular a la gestión de seguridad de la información radicado 00110-817-006634 del 11-dic-2020 la que se encuentra en plan de mejoramiento suscrito con fecha de finalización 31 de diciembre de 2021 por lo que no sería necesario generar nuevamente la observación sobre algo que ya se evidencio y que se encuentra en medio de la ejecución de acciones de mejora."*

Análisis ACI: El alcance de la presente auditoría es distinto al señalado que comprendía hasta junio de 2020, lo que evidencia que 1 año después no se han tomado acciones de mejoramiento efectivas y oportunas para mitigar el riesgo identificado. Teniendo en cuenta que hasta el momento no ha sido actualizado el plan de mejoramiento y este procedimiento hace parte de la auditoria, se mantiene la observación, así aplique la misma acción de mejora que se encuentra en curso.

Los comentarios dejados por la SDAE fueron:

> *"A su vez el procedimiento actual de mesa de ayuda expresa acuerdos de niveles de servicio sobre la atención inicial al solicitante ya que no se puede establecer "La métrica de un tiempo de respuesta de 15 a 20 minutos para dar solución a un ticket de conformidad con la actividad de control establecida en el procedimiento." Debido a que las solicitudes son de diversos temas y de variedad de complejidades como por ejemplo al requerir intervención de un tercero o la adquisición de un repuesto (actividades que no se pueden cumplir en 15 a 20 minutos), así mismo las solicitudes sobre los sistemas de información pueden pasar desde el otorgamiento de permisos hasta la necesidad de un desarrollo que involucra las fases clásicas del desarrollo de software incluyendo levantamiento y análisis de requerimientos, costeo de recursos, diseño, desarrollo, pruebas, implementación, que no cumplirían con el mencionado tiempo."*

Análisis ACI: La métrica 15 a 20 minutos como lo indica el procedimiento se tuvo en cuenta debido a que para cerrar un caso se depende de la calificación del usuario que solicito el servicio, y hay 4 casos que superan los tiempos de respuesta debido a que están abiertos con bastante tiempo de superación, como se evidencio en el informe los incidentes:

- 31640 de SAF-SERVICIOALUSUARIO
- 31675 de SDAE-SISTEMAS
- 31863 de ACI
- 32216 de SFE-FORMACIONYCAPACITACION

Los comentarios dejados por la SDAE fueron:

> *"La afirmación de "en donde se omitieron conceptos de buenas prácticas y recomendaciones de marcos definidos como ITIL, y así evidenciar el cumplimiento del servicio de atención, medible para la gestión que realizan los agentes de la mesa de ayuda" no es cierta ya que dentro de las buenas prácticas se encuentra la percepción del usuario, la que se realiza a través de una herramienta de encuesta de satisfacción, la que también es registrada y medida en el actual instrumento de mesa de ayuda."*
>
> *Así mismo en la afirmación "Para cerrar un caso se depende de la calificación del usuario que solicitó el servicio, esto conlleva a que la mesa de ayuda no lleve un récord del cumplimiento de los tiempos" no es cierto ya que la herramienta genera registro de tiempos y medición en diferentes estados tales como el solicitado, asignado, terminado por el responsable de atención y la finalización del usuario a través de la encuesta de satisfacción, por lo que hay múltiples formas de realizar medición.*

Análisis ACI: Se reconoce que la percepción del usuario es una práctica importante, lo que se está indicando en la auditoria es que los controles asociados al servicio y cierre de caso no se deben entregar al usuario, es responsabilidad del dueño del proceso. Para cerrar un caso no se puede depender de la calificación de un usuario, porque puede significar tiempos largos y no van a mostrar la correcta gestión realizada por los agentes. No se puede medir el servicio.

La herramienta utilizada para mesa de ayuda lleva tiempos, pero el cierre del caso depende de la calificación del usuario, por lo tanto, existe ese desfase.

Los comentarios dejados por la SDAE fueron:

> *"La afirmación "La gran mayoría de incidentes ocasionados en HEMI se evidenció que se está realizando por medio de correos electrónicos enviados a:*
> *jepenap@ipes.gov.co*
> *soporte@goobi.net", tampoco es cierta dado que los correos relacionados pertenecen a la atención del Sistema de Información GOOBI."*

Análisis ACI: Como la afirmación de los auditados lo indica *"dado que los correos relacionados pertenecen a la atención del Sistema de Información GOOBI",* se está dando entender que los incidentes presentados de GOOBI se están manejando por fuera de la mesa de ayuda, por lo que es importante diferenciar entre incidente y requerimiento, aclarar esta terminología y su procesamiento en el procedimiento. Los controles son responsabilidad del dueño del proceso.

Los comentarios dejados por la SDAE fueron:

Las diferentes funcionalidades del sistema de información GOOBI, mencionadas en la descripción de la observación se encuentran operativas, la auditoría no gestionó la corroboración de la información de los usuarios funcionales con el PGSIRT, sin embargo existen inconvenientes no relacionados con las funcionalidades del sistema si no con la operación organizacional desde la parte procedimental, para lo cual el PGSIRT ha generado múltiples propuestas y solicitudes de generación de reglas de negocio a los procesos funcionales ((Ver anexo,https://drive.google.com/drive/folders/1vyPXdh_780sV3s6Qjoo5A3XNvnUDoPr?usp=sharing)
Actualmente se está trabajando en la implementación de una nueva mesa de ayuda con mayores y mejores opciones de atención y resolución de solicitudes los cuales tendrán mejoras significativas teniendo en cuenta los ANS y los KPI, notificaciones de los estados, cambios, encuesta de satisfacción de los tickets por medio de correo electrónico, control de estadísticas y optimización de solicitud de atención.
La atención de las solicitudes no se ha podido atender al 100% por algunas limitaciones de la actual mesa de ayuda. (ver anexos)"

Análisis ACI: La documentación de diferentes funcionalidades del sistema de información GOOBI suministradas como evidencias no puede ser aceptada debido a que superan la vigencia de la auditoria, son actividades que se están realizando en presente y no en la alcance auditado, además debieron ser presentadas, por tarde, en la reunión de socialización.

La implementación de la nueva mesa de ayuda es válida como plan de mejoramiento de la auditoria actual.

En mérito de lo expuesto, el hallazgo se mantiene y el responsable del proceso debe establecer un plan de mejoramiento con acciones efectivas de mitigación del riesgo.

Riesgo Asociado: Inoportunidad en la atención de incidentes y requerimientos e inoportunidad en la puesta en operación de soluciones tecnológicas o en la generación de información respecto a la prestación de los servicios informáticos de la entidad: Factores asociados con fallas en la definición y ejecución del plan de mantenimiento, deficiencias en la calidad de la información registrada en los sistemas de información institucional, alta rotación del personal, debilidades en la definición de los acuerdos de niveles de servicios, pueden ocasionar que se realice de manera inoportuna la atención a requerimientos, soluciones tecnológicas o de generación de información.

Normatividad o Criterio:

1. Deficiencias en la medición de la atención por el cierre por parte de los usuarios
Matriz de Riesgos y Controles:
Los técnicos y profesionales de sistemas verifican diariamente a través del sistema de información de mesa de ayuda los tickets a su cargo, realizan diagnóstico y brindan solución al requerimiento o incidente conforme el procedimiento PR-136 ATENCIÓN MESA DE AYUDA

PR-136 ATENCIÓN MESA DE AYUDA:
Actividad 2: Coordinar la asignación (Según el problema): *El técnico que coordina revisa identifica y verifica el tipo de requerimiento.*

Vía telefónica: El personal designado para la atención indicará de manera explícita y remota al usuario para la atención y solución a su requerimiento.
Mesa de ayuda: Se informará al usuario por este mismo medio el número del ticket que le fue asignado, el estado de ticket de su solicitud y el técnico asignado para su atención.
Actividad 3: Analizar y asignar mesa de ayuda: *Se realiza análisis y se asigna según el nivel. ¿La solicitud está dentro de la competencia?*
SI: Realizar diagnostico
NO: Se rechaza se hace el cierre en el sistema. Fin del procedimiento.
Actividad 5: Solucionar requerimiento: *El técnico asignado soluciona el requerimiento.*
Actividad 7: Revisar Requerimiento: *El especialista o proveedor revisa el requerimiento ¿el requerimiento se soluciona?*
SI: Continua con la actividad 6
NO: Fin del procedimiento
Actividad 8: Verificar y realizar prueba del equipo:
Se verifica que el equipo funcione bien, se realiza prueba.
¿Funciona el equipo?
SI: Continua con la actividad 10
NO: Regresa a la actividad 6
Actividad 10: Realizar encuesta para cierre de la mesa de ayuda: *El usuario realiza la calificación de la mesa de ayuda atendida y realiza el cierre.*

2. *Ausencia en definir ANS y OLA*
Glosario de ITIL/ITSM:
"La implementación y administración de servicios de TI de calidad que satisfacen las necesidades de la empresa. La gestión del servicio de TI la realizan los proveedores de servicios de TI a través de una combinación adecuada de personas, procesos e información. tecnología."

- *ITSM (Information Technology Service Management/gestión de servicios de tecnologías de la información)*
- *ANS/SLA Acuerdo formal entre el cliente y el proveedor de servicios, registra los acuerdos de niveles de servicio)*
- *Acuerdo de Nivel Operacional (OLA) (Es un acuerdo entre el Proveedor de Servicios de TI y otra parte de ese mismo negocio que le provee servicios al proveedor)*

Resolución No.049 de 2020, por la cual se adopta la actualización del Documento Estratégico DE-047 Plan Estratégico de tecnologías de la Información y las Comunicaciones. Ítem 7.10 Estrategias del Plan: *Estrategias que contribuyen a garantizar la continuidad operativa de la entidad; incluye iniciativas orientadas, entre otras, a la actualización tecnológica o establecimiento de planes de contingencia.*

3. *Ausencia de pruebas de GOOBI antes de salir a producción*
Resolución No.047 de 2020, Documento Estratégico DE-039 Plan de Seguridad y Privacidad de la Información. *Ítem 6.3 Acciones Particulares a Seguir, Tabla 9 Adquisición, Desarrollo y Mantenimiento de Sistemas.*
Control A.14.1.1 Análisis y especificación de requisitos de seguridad de la información:

Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información para mejoras a los sistemas de información existentes.

Actividad 1: Revisión de los Procedimientos.

Se debe realizar revisión de los procedimientos para levantamiento o especificación de requisitos de la entidad para ajuste o desarrollo de sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.

Resolución No.049 de 2020, por la cual se adopta la actualización del Documento Estratégico DE-047 Plan Estratégico de tecnologías de la Información y las Comunicaciones. Ítem 7.10 Estrategias del Plan

Estrategias que contribuyen a garantizar la continuidad operativa de la entidad; incluye iniciativas orientadas, entre otras, a la actualización tecnológica o establecimiento de planes de contingencia.

Estrategia 15: *Realizando mantenimiento preventivo y correctivo de la plataforma tecnológica.*

Recomendación:

- Documentar las actividades de control relacionadas con el proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, en el flujo de actividades del procedimiento, con la inclusión de los 6 elementos de control dado por la Guía de Administración del Riesgo y el Diseño de Controles (DAFP, 2020).
- Para cubrir las deficiencias en la medición de la atención por el cierre por parte de los usuarios, se recomienda actualizar el proceso cambiando la forma de medir el cierre apoyado por prácticas como ITIL 4, y además mejorando una solución tecnológica que cumpla las funciones de ITSM, ITIL, ISO 20.000 y otras prácticas desarrollen KPI (*Key Performance Indicator,* Indicador clave de rendimiento) para la medición de la eficacia de los tiempos de servicio, además ayuda a automatizar la gestión de servicio para los agentes, gestión del conocimiento, seguimiento a las necesidades de la organización.
- Dividir los tiempos en OLA y SLA para el proceso PR-136 ATENCIÓN MESA DE AYUDA, con el fin de definir el servicio para las partes interesadas, tener en cuenta que los OLAs son para el servicio operacional interno, los SLAs aplica para clientes de la organización.
- Definir una metodología para la atención de "requerimiento" lo cual se significa: "*proceso se refiere a todas las solicitudes que generan los usuarios y que no están asociadas a un incidente en un servicio".*

Connotación: Administrativa.

Proceso: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS
Procedimientos: PR-033 Backup generación y recuperación

No.: 4

AUSENCIA DE PRUEBAS PARA CORROBORAR RESPALDOS DE LA INFORMACIÓN

Responsable de las acciones de mejora: SDAE

La falta de pruebas a los respaldos de los aplicativos HEMI y GOOBI respecto al plan de contingencia puede manifestar un incidente grave, debido a que no se realizan pruebas, los profesionales de la SDAE (GSIRT) ponen a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

Cómo indica norma ISO 27001:2013 con el control A.12.3.1 Respaldo de la información: "*Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas,* ***y ponerlas a prueba regularmente*** *de acuerdo con una política de copias de respaldo acordadas"*

COBIT 2019 nos solicita Gestionar la seguridad y gestionar el aseguramiento en los procesos: "**APO13 Gestionar la seguridad** **Mantener el impacto y la existencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo** de la empresa." y **"MEA04 Gestionar el aseguramiento** Facilitar a la organización el diseño y desarrollo de **iniciativas de aseguramiento eficaces y eficientes**, proporcionando una guía sobre la planificación, alcance, ejecución y **seguimiento de las revisiones de aseguramiento**, usando una hoja de ruta basada en criterios de aseguramiento que sean bien acogidos."

Durante la auditoria se realizó pruebas de back ups realizando restauración de GOOBI el día 2 de julio de 2021 (ver **ANEXO 8**), el cual fue exitoso, pero hay que tener en cuenta que la periodicidad de las pruebas para corroborar que están funcionando de forma adecuada.

Cuando se están realizando back ups y no se realizando pruebas es posible que cuando se requieran estén de manera incorrecta.

La inadecuado administración y monitoreo de los activos de infraestructura tecnológica, puede producir pérdida o afectación en la integridad de la información, se deben tener encuentra las fallas tanto a nivel humano y tecnológico.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR-033 Backup generación y recuperación, presentó el siguiente Diseño de Control:

Control 1: PA08-DE-003 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
9.2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
9.2.1. Política general del Sistema de Gestión de Seguridad de la Información
Es obligación de todos los funcionarios, contratistas y terceros con acceso autorizado a la infraestructura tecnológica, servicios de red, aplicaciones y a los activos de información institucional, dar estricto cumplimiento a la política de seguridad y privacidad de la información del Instituto para la Economía Social.

De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidad en el manejo de prioridad en donde el control se apoya en el DE-047 Cómo se hace: Estrategias que

contribuyen a garantizar la continuidad operativa de la entidad, en el manejo de las excepciones, no se investigan y resuelven oportunamente, y además no existe evidencias.

Control 2: PR-033-BACKUP GENERACIÓN Y RECUPERACIÓN
No contempla monitoreo
PA08-DE-004 PLAN DE CONTINGENCIA DE TI
7.4.4 Sistemas de monitoreo de capacidad de servidor.
Las herramientas de monitoreo de los recursos de tecnología (incluidas variables fundamentales del servidor y ancho de banda de canales), son necesarias para establecer comportamientos de los recursos de tecnología y predecir incidentes. El Monitoreo de la capacidad de servidores es una medida preventiva frente a incidentes de seguridad de la información. Sin embargo, en la actualidad el monitoreo se realiza manualmente a través de los profesionales a cargo de la infraestructura de TI, y se encuentra en proceso de implementación de la herramienta NAGIOS para automatizar el monitoreo
7.4.5 Sistemas de monitoreo de aplicación
En la actualidad no se cuenta con herramientas centralizadas de monitoreo de las aplicaciones. Una de las oportunidades de mejora para el plan de contingencia incluye la implantación de herramientas de supervisión que permitan identificar comportamientos anómalos en las aplicaciones y así prevenir incidentes

De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control; se encontró debilidad en el manejo de excepciones.

Valoración comentarios del Auditado:

Los comentarios dejados por la SDAE fueron:

> *No se acoge la observación dado que en medio de la respuesta al requerimiento 00110817-003881, bajo el número de radicado 00110-817-003955-21 (Ver anexo,https://drive.google.com/drive/folders/1vyPXdh_78-0sV3s6Qjoo5A3XNvnUDoPr?usp=sharing), se evidencio el monitoreo efectuado a la infraestructura y las métricas de disponibilidad a través de la herramienta NAGIOS, la cual opera y genera alertas los 7 días de la semana y las 24 horas del día, a su vez si se realizan pruebas de los respaldos de backup, en la reunión sostenida con el auditor en la cual se le presentó el funcionamiento de la herramienta institucional de backup, se hacen pruebas periódicas, dado que para la generación de nuevos servidores y /o servicios se realiza la práctica de restauración definitiva de backups tal como ocurrió con los servidores de pruebas y de bases de datos de pruebas, en medio de la respuesta al mismo requerimiento se remitieron evidencias documentales de los ejercicios mencionados. A su vez y como parte de la misma respuesta se hizo entrega de las bitácoras de respaldo y restauración generadas de forma automática por el sistema de backup.*
> *Lo anterior se confirma en la descripción de observaciones del número 6 del informe, en el cual se indica "En la visita de auditoría efectuada el 02-jul-2021, se realizó una prueba al sistema de Back Up actual que es VEEM Back Up respecto a GOOBI y se pudo comprobar que está funcionando de manera correcta. Ver ANEXO 9."*

Análisis ACI: Respecto al uso de la herramienta NAGIOS no se discute que su monitoreo, teniendo en cuenta que NAGIOS es un sistema para monitorización de redes, que vigila los equipos y servicios que se especifiquen, alertando cuando el comportamiento de los

mismos no sea el deseado, la observación hace referencia a que de manera periódica se deben realizar prueba(s) para comprobar que cualquier elemento de contingencia y/o respaldo va a funcionar de manera correcta cuando se necesite, por eso durante la auditoría se pidió realizar la prueba de restauración la cual fue exitosa. De acuerdo a su análisis de riesgos y conocimiento de los expertos, los responsables de las herramientas deciden cada cuanto se realiza esta prueba.

Se ha reconocido que la restauración realizada durante la auditoria el día 2 de julio de 2021 fue exitosa, solo se ha indicado que debe documentarse el control y efectuarse la actividad periódicamente, de acuerdo a las necesidades del IPES.

En mérito de lo expuesto, el hallazgo se mantiene y se requiere formulación de un plan de mejoramiento por parte del responsable del proceso.

Riesgo Asociado: Daños o funcionamiento inadecuado de la plataforma tecnológica, sistemas y servicios informáticos de la entidad: Daños o funcionamiento inadecuado de la plataforma tecnológica, servidores, correo electrónico e información digital de la entidad

Normatividad o Criterio:

ISO 27001:2013
A.12.3 Copias de respaldo
Objetivo:
Proteger contra la pérdida de datos.
A.12.3.1 Respaldo de la información:
Control
Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

COBIT 2019
APO13 Gestionar la seguridad
Mantener el impacto y la existencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.

MEA04 Gestionar el aseguramiento
Facilitar a la organización el diseño y desarrollo de iniciativas de
aseguramiento eficaces y eficientes, proporcionando una guía sobre la planificación, alcance, ejecución y seguimiento de las revisiones de aseguramiento, usando una hoja de ruta basada en criterios de aseguramiento que sean bien acogidos.

Recomendación:

- Documentar las actividades de control relacionadas con el proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, en el flujo de actividades del procedimiento, con la inclusión de los 6 elementos de control dado por la Guía de Administración del Riesgo y el Diseño de Controles (DAFP, 2020).

- Incluir dentro de las pruebas periódicas de los sistemas de respaldos a los sistemas de información o a cualquier actividad de contingencia para asegurar la continuidad del negocio.

Connotación: Administrativa.

No.: 5

DESACTUALIZACIÓN DEL PROCEDIMIENTO DE BACK UP, GENERACIÓN Y RECUPERACIÓN

Responsable de las acciones de mejora: SDAE

En el marco de la documentación del procedimiento PR-033 no se encontraron documentados controles relacionados con las de recuperación de backup de acuerdo al marco ISO 27001, en el mismo sentido, no se definió un plan de pruebas de las copias de seguridad, esto para la vigencia 2020. Esta misma observación se dejó en el informe de auditoría regular a la gestión de seguridad de la información radicado 00110-817-006634 del 11-dic-2020, que a la fecha no ha actualizado.

Se observó en el proceso para PR-033 BACK UP, GENERACIÓN Y RECUPERACIÓN que la SDAE realizó un cambio significativo durante la vigencia 2020, debido a que se modificó el proceso de Back Up, que se realizaba mediante cintas por un software especializado llamado VEEAM BACKUP a partir de enero 2020; modificación que no se había establecido en el procedimiento ni el control de cambios.

El cambio está relacionado con la forma de realizar copias de seguridad y así asegurar la continuidad del negocio.

Tal como se encuentra estipulado en el PR-033 BACK UP, GENERACIÓN Y RECUPERACIÓN. En el punto 5. CONDICIONES GENERALES (página 2) se evidencia que toda la descripción está a realizada en cinta, adicionalmente se mencionada que las medidas de Back Up "*debe realizarse de manera estricta* ".

Aunque el sistema VEEAM BACK UP demostró ser eficiente y eficaz en la recuperación de información el proceso PR-033-BACKUP GENERACIÓN Y RECUPERACIÓN si se encuentra totalmente desactualizado, faltando al PR-005 CONTROL DE DOCUMENTOS y al IN-001 ELABORACIÓN, MODIFICACIÓN O ANULACIÓN DE DOCUMENTOS DEL IPES.

Respecto a las pruebas de las copias de seguridad, la entidad no se ha efectuado pruebas de los sistemas de respaldo, además que el sistema de Back Up fue cambiado y no se realiza por medio de cintas como lo indica el procedimiento.

En la visita de auditoría efectuada el 02-jul-2021, se realizó una prueba al sistema de Back Up actual que es VEEM Back Up respecto a GOOBI y se pudo comprobar que está funcionando de manera correcta. Ver **ANEXO 10.**

Los procesos y las herramientas de backup son una gestión propia y habitual de las organizaciones, donde la actividad está muy ligada al proceso de backup. Su gestión requiere de conocimiento, personal técnico, tiempo e infraestructura para garantizar la productividad y versatilidad requerida.

Las copias de seguridad son duplicados de la data de la información de valor para una organización, se usa para poder recuperarlos ante cualquier pérdida o incidente. De esta forma, las organizaciones evitan almacenar datos erróneos o duplicidades. Además, las copias de seguridad ocupan bastante espacio.

Estas pérdidas de datos son realmente comunes, por lo cual es usual contar con backup en distintos formatos, destino y protección y transporte por empresas dedicadas a respaldo de valores.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR-033 Backup generación y recuperación, presentó el siguiente Diseño de Control:

Control 1: El Plan de Contingencia de TI del Instituto Para La Economía Social IPES, aplica para los activos y sistemas de información digital del IPES, y da cubrimiento a la sede principal ubicada en el Edificio Torre 73 Calle 73 No 11 – 66, dado que allí se centraliza la gestión de tecnología.

El plan de contingencia incluye:
● Resultados de auditorías al cumplimiento del plan de contingencia
● Retroalimentación de partes interesadas como Comisión Distrital de Sistemas, Secretaria de Hacienda, Proveedores relacionados con el plan de contingencia,
oficina de control interno entre otros
● Técnicas, productos o herramientas que se puedan utilizar para mejorar el plan de contingencia
● Cambios internos o externos que puedan afectar al plan de contingencia
● Resultados de las pruebas que se realicen al plan de contingencia
● Lecciones aprendidas de incidentes que afectaron la disponibilidad de servicios o la efectividad del plan de contingencia
● Resultados de las actividades de capacitación y toma de conciencia del plan de contingencia

De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidad en Procedimiento y Manejo de excepciones en donde el control se apoya en el Plan de Contingencia de TI Cómo se hace: Estrategias que contribuyen a garantizar la continuidad operativa de la entidad, en el manejo de las excepciones, no se investigan y resuelven oportunamente, y además no existe evidencias.

Valoración comentarios del Auditado

Los comentarios dejados por la SDAE fueron:

> *Esta observación no se acoge debido a que tal como se argumenta en la misma "Esta misma observación se dejó en el informe de auditoría regular a la gestión de seguridad de la información radicado 00110-817-006634 del 11-dic-2020, que a la fecha no ha actualizado.", la misma ya se encuentra en plan de mejoramiento suscrito con fecha de finalización 31 de diciembre de 2021 por lo que no sería necesario generar nuevamente una observación sobre algo ya se evidencio y que se encuentra en medio de la ejecución de acciones de mejora.*
> *A su vez, la desactualización documental no indica que la ejecución de actividades no se realice de la debida forma, para este caso a través de la respuesta al requerimiento 00110817-003881, bajo el número de radicado 00110-817-003955-21 (Ver anexo, https://drive.google.com/drive/folders/1vyPXdh_78-0sV3s6Qjoo5A3XNvnUDoPr?usp=sharing) , se hizo entrega de las muestras de las bitácoras (logs) de toma de backup y recuperación, así como la relación de tareas (jobs) de respaldo; así como se expuso al auditor en una presentación, también anexa a la respuesta, la operación del sistema de backup de la entidad, demostrando cómo funcionan los diferentes jobs y herramientas, la diferencia de los respaldos según la criticidad de los servicios, los backups que tienen redundancia por archivos, por servidor, por hypervisor y como existe contingencia con las aplicaciones y bases de datos incluso manteniéndolas en servidores físicos cruzados. Adicionalmente y según el requerimiento, se efectuó visita al datacenter de la entidad y se llevó a cabo una demostración de la recuperación de respaldos y la generación de restauraciones instantáneas de servicios y servidores en cuestión de minutos.*
> *La afirmación de "debido a que se modificó el proceso de Back Up, que se realizaba mediante cintas por un software especializado llamado VEEAM BACKUP a partir de enero 2020;" no es cierta dado que el actual sistema de backup no trabaja librerías físicas en cintas si no se adquirió un servidor robusto dedicado de manera exclusiva para el almacenamiento de backup.*
> *Frente a la afirmación "la entidad no ha efectuado pruebas de los sistemas de respaldo, además que el sistema de Back Up fue cambiado y no se realiza por medio de cintas como lo indica el procedimiento.", no es cierta ya que se le comunicó al auditor en medio de la presentación que se hacen pruebas periódicas, dado que para la generación de nuevos servidores y /o servicios se realiza la práctica de restauración definitiva de backups tal como ocurrió con los servidores de pruebas y de bases de datos de pruebas, en medio dela respuesta al mismo requerimiento se remitieron evidencias documentales de los ejercicios mencionados.*
> *Lo anterior se confirma en la descripción de observaciones de este mismo numeral "En la visita de auditoría efectuada el 02-jul-2021, se realizó una prueba al sistema de Back Up actual que es VEEM Back Up respecto a GOOBI y se pudo comprobar que está funcionando de manera correcta. Ver ANEXO 9."*
> *Debido a que ya se tenía contemplada la actualización documental del proceso desde la vigencia 2020 y con el acompañamiento de una empresa consultora, con un equipo experto en temas de ISO27000, así como la ejecución de actividades del plan de mejoramiento de la auditoría 2020 se cuenta con un documento actualizado del PR-033, el cual fue revisado y socializado entre PGSIRT y el área de calidad donde se efectuaron ajustes para su actualización, sin embargo se reitera que la fecha de cumplimiento es el 31 de diciembre de 2021.*
> *(https://drive.google.com/drive/folders/1vyPXdh_780sV3s6Qjoo5A3XNvnUDoPr?usp=sharing)*

Análisis ACI: El alcance de la presente auditoría es distinto al señalado, que comprendía hasta junio de 2020, lo que evidencia que 1 año después no se han tomado acciones de mejoramiento efectivas y oportunas para mitigar el riesgo identificado. Teniendo en cuenta que hasta el momento no ha sido actualizado el plan de mejoramiento y este procedimiento hace parte de la auditoria, se mantiene la observación, así aplique la misma acción de mejora que se encuentra en curso.

La observación no dice*: "no indica que la ejecución de actividades no se realice de la debida forma"* como describe el auditado, se está evidenciando que el procedimiento se encuentra desactualizado, se ha reconocido que la solución ha funcionado bien en el momento de probarla.

En la presentación se hizo una descripción de cómo funciona la solución, y se comunicó que el software realizaba diferentes tipos de respaldos, pero no se evidenció que se realice pruebas, y la prueba realizada en la auditoria fue exitosa.

Se está reconociendo que durante la auditoria se realizó de manera correcta la restauración del back up, la observación hace referencia a que el procedimiento documentado no está actualizado.

En mérito de lo expuesto, el hallazgo se mantiene y el responsable del proceso debe establecer un plan de mejoramiento con acciones efectivas de mitigación del riesgo.

Riesgo Asociado: Fallas en los medios de recuperación de la información: Fallas en el momento de realizar los respaldos, su custodia, alcance y sus pruebas de restauración.

Normatividad o Criterio:
PA08-DE-004 PLAN DE CONTINGENCIA DE TI - 4. ALCANCE: *El Plan de Contingencia de TI del Instituto Para La Economía Social IPES, aplica para los activos y sistemas de información digital del IPES, y da cubrimiento a la sede principal ubicada en el Edificio Torre 73 Calle 73 No 11 – 66, dado que allí se centraliza la gestión de tecnología.*

7.2 Mantenimiento del plan de contingencia
El plan de contingencia de IT se debe revisar a intervalos planificados, mínimo una vez al año. La revisión del plan de contingencia es una de las actividades que se debe incluir en la revisión del Sistema Integrado de gestión del IPES. Las entradas que se deben revisar Respecto al Plan de contingencia incluyen:

- *Resultados de auditorías al cumplimiento del plan de contingencia*
- *Retroalimentación de partes interesadas como Comisión Distrital de Sistemas, secretaria de Hacienda, Proveedores relacionados con el plan de contingencia, oficina de control interno entre otros.*
- *Técnicas, productos o herramientas que se puedan utilizar para mejorar el plan de contingencia*
- *Cambios internos o externos que puedan afectar al plan de contingencia*
- *Resultados de las pruebas que se realicen al plan de contingencia*
- *Lecciones aprendidas de incidentes que afectaron la disponibilidad de servicios o la efectividad del plan de contingencia*
- *Resultados de las actividades de capacitación y toma de conciencia del plan de contingencia.*

5. CONDICIONES GENERALES● Cambios internos o externos que puedan afectar al plan de contingencia

- *Resultados de las pruebas que se realicen al plan de contingencia*
- *Lecciones aprendidas de incidentes que afectaron la disponibilidad de servicios o la efectividad del plan de contingencia*

- *Resultados de las actividades de capacitación y toma de conciencia del plan de contingencia*

PR-033-BACKUP GENERACIÓN Y RECUPERACIÓN
5. CONDICIONES GENERALES
*Los respaldos en **cinta** se desarrollarán de manera automática y serán reemplazadas semanalmente en el desarrollo de las actividades de contrato de custodia de medios.*
Actividad 1: *Identificar Activos de Información susceptibles de BackUp*
Análisis de información para la programación de tareas de BackUp Automáticas.
Actividad 2: *Diligenciar Formato de Soporte de ejecución de BackUp FO-319. Tareas de registro de ejecución de BackUp.*
Actividad 5: *Restauración Cinta a través de herramienta de BackUp.*
Tarea de recuperación de Información, a partir de medios de almacenamiento.
Actividad 8: *Monitorear que el BackUp se realice.*
Tareas de administración y seguimiento a la ejecución de copias de respaldo de la información Institucional.
Actividad 9: *El BackUp se ejecutó correctamente. SI pasar a la actividad No. 11 - NO pasar a la actividad No.7*
Verificación Automática de la Plataforma.
Actividad 11: *Etiquetar y Almacenar Cinta.*
Identificación de la información contenida en medios de almacenamiento seguro.
Actividad 12: *Diligencia Formato de soporte de ejecución de BackUp.*
Registro de actividades relacionadas con copias de respaldo.

PR-005 CONTROL DE DOCUMENTOS: *La actualización de los documentos se reportará como realizada, siempre y cuando haya sido solicitada a la Subdirección de Diseño y Análisis Estratégico mediante el formato "FO-021 Solicitud de elaboración, modificación y/o anulación de documentos", además de haber sido revisados los documentos por la misma y subidos a la carpeta compartidos.*

IN-001 ELABORACIÓN, MODIFICACIÓN O ANULACIÓN DE DOCUMENTOS DEL IPES
5. CONDICIONES GENERALES
Acorde al Modelo Integrado de Planeación y Gestión, hay una gran necesidad de procedimentar los procesos que sustentan la gestión de la Entidad para el cumplimiento de su misionalidad, con el fin que sea conocido por las partes interesadas y grupos de valor, como parte del ejercicio de interacción entre el Estado y la Ciudadanía.

Por ello, la adecuada elaboración, manejo y control de los documentos y registros del Instituto se fundamentan en el fomento de transparencia, mayor eficiencia administrativa, acceso a la información pública y protección al patrimonio documental del Instituto.
Es por ello, que a continuación se tendrán en cuenta las siguientes consideraciones:
- *Los documentos no usarán ningún tipo de logo institucional a excepción de los formatos comunes.*
- *Todo documento debe estar al alcance de consulta de cualquier Colaborador con las versiones vigentes.*
- *Los documentos deben ser revisados por el gerente de cada proceso al menos una vez al año y actualizarlos, a fin de asegurar la continua adaptabilidad y cumplimiento de los requisitos aplicables.*

- *Todas las solicitudes de elaborar, modificar o anular documentos deben ser diligenciadas por responsables de respectivo proceso, el cual debe ser justificado y sustentado en el formato FO-021 Solicitud de elaboración, modificación y/o anulación de documentos, y control de cambios.*

6.1.4 Actualización o Modificación de Documentos

El cambio de versión de un documento o formato se presenta en un procedimiento, cuando se requiera modificar la información registrada en alguno de los siguientes campos: Objetivos, alcance, políticas de operación, el orden o descripción de las actividades, marco normativo, documentos o registros asociados. Cuando un documento cambie de versión, deben relacionarse los cambios realizados en el cuadro de control de cambios, dispuesto al final de cada documento. Dicha relación debe conservar el historial de cambios relacionados a través de las versiones. Si se requieren modificaciones tales como correcciones en ortografía, códigos, paginación, la Subdirección de Diseño y Análisis Estratégico hará los cambios sin que ello implique una nueva versión del documento. La creación, modificación y o anulación de los documentos se reportará como realizada, siempre y cuando hayan sido revisados los documentos por el profesional responsable del SIGD y publicados en el Drive. Además, debe ser solicitada a la Subdirección de Diseño y Análisis Estratégico- SDAE mediante el formato "FO-021 Solicitud de elaboración, modificación y/o anulación de documentos".

6.1.5 Documentos Anulados y obsoletos

Todo documento o formato que ha perdido vigencia por una nueva actualización o eliminación se considera un documento o formato OBSOLETO. Esté documento deberá ser identificado con la marca de DOCUMENTO OBSOLETO, para prevenir el uso inadecuado. El control de los documentos y formatos del SIGD está a cargo del profesional responsable de la Subdirección de Diseño y Análisis Estratégico, quien guardará en una carpeta digital de control de documentos y formatos obsoletos las versiones que ya no se encuentran vigentes, adicional a ello es el responsable restringir su uso o autorizarlo. Cuando se requiera una copia de un documento o formato obsoleto, el líder o responsable del proceso debe solicitarlo mediante correo electrónico al subdirector de Diseño y Análisis Estratégico, exceptuando las solicitudes de los Órganos de Control o la Oficina de Control Interno.

6.1.7 Seguimiento y control de cambios

Los documentos se revisan periódicamente y actualizan según las necesidades con el fin de asegurar que continúen siendo aplicables o deban ser modificados.

***El control de los documentos se encuentra bajo la responsabilidad** de Gestión Documental y los **Líderes de proceso y/o subproceso** a nivel nacional, deben asegurar su aplicación e informar de los que estén obsoletos, fuera de uso o vigencia.*

ISO 27001:2013

A.12.3 Copias de respaldo
Objetivo:
Proteger contra la pérdida de datos.
A.12.3.1 Respaldo de la información:
Control

Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

Recomendación:

- Documentar las actividades de control relacionadas con el proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, en el flujo de actividades del procedimiento, con la inclusión de los 6 elementos de control dado por la Guía de Administración del Riesgo y el Diseño de Controles (DAFP, 2020).
- Actualizar el PR-033 Back Up Generación Y Recuperación indicando como se realiza en la actualidad.

Connotación: Administrativa.

No.: 6
DEFICIENCIAS EN EL DISEÑO DEL CONTROL DEL PROCESO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS

Responsable de las acciones de mejora: SDAE

Se evidenciaron deficiencias en los diseños de los controles establecidos en los diferentes procedimientos del Proceso de PO-013 PROCESO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS que se encuentran en el SIG, los cuales deben servir para mitigar las causas que hacen que los riesgos se materialicen y su estructuración debe ajustarse a los parámetros establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP, así:

RIESGO 1: Inadecuada planeación y ejecución de los planes, proyectos, metas e indicadores

1) **Actividad de Control Analizada:** PR-042 PLANEACIÓN ESTRATÉGICA Y OPERATIVA

5.1. Formulación del plan estratégico institucional (PEI) del cuatrienio
a. Diseño de marco metodológico para el proceso de planeación estratégica.
b. Análisis sectorial y normativo de las herramientas de Planificación según el modelo en cascada establecido para la planificación distrital y los planteamientos establecidos desde la función pública.
f. Priorización por la alta dirección

PA08-DE-002 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
8.3 MONITOREO, SEGUIMIENTO Y EVALUACIÓN
8.3.2. Monitoreo y Seguimiento
La entidad a través de la Subdirección de Diseño y análisis estratégico realizara un monitoreo mensual del plan a través del formato FO-264 Bitácora Plan, y los cortes de análisis de seguimiento al interior de la entidad se realizarán trimestralmente, según lo establecido en el procedimiento PR-042, dado que el esquema de seguimiento y medición

al sistema de gestión de riesgos de la seguridad de la información es fundamental para contextualizar la toma de decisiones de manera oportuna.

PA08-DE-004 PLAN DE CONTINGENCIA DE TI
8 DESARROLLO DEL PLAN
8.1 METODOLOGÍA
Para la definición del plan de tratamiento de riesgos de seguridad digital se señalan las actividades desarrolladas previamente:

- Comprensión del contexto.
- Identificación del riesgo.
- Análisis del riesgo inherente.
- Evaluación del riesgo.
- Definición de controles existentes.
- Análisis del riesgo residual.
- Selección de la opción de tratamiento del riesgo.
- Definición del plan de tratamiento.

Diseño del Control: De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidad en el manejo de la periodicidad, debería ser eventual cada vez que se presente un retraso en la ejecución de la planeación

RIESGO 4: Implementación inadecuada de las políticas públicas de seguridad digital

2) Actividad de Control Analizada: PR-123 GESTION DE INCIDENTES DE SEGURIDAD

Actividad 1: Registrar el Incidente de Seguridad de la Información.
Identificar y alertar sobre posibles fallas en la Seguridad de la Información.

Actividad 2: Analizar e identificar el Incidente de Seguridad de la Información.
Evaluar la Información ambigua, contradictoria, o incompleta para determinar si está o no ocurriendo un incidente.

Actividad 5: Recuperar Sistemas afectados.
Restaurar los sistemas y servicios informáticos a su operación normal.

Actividad 6: Revisión Post Incidente de Seguridad de la Información.
Seguimiento al comportamiento y estabilidad de los sistemas y servicios informáticos.

Diseño del Control: De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidad en el manejo de la periodicidad, existe posibles incidentes que se pueden presentar, es posible que se no han sido tenido en cuenta debido a diferentes factores con los usuarios.

3) Actividad de Control Analizada: Resolución No.047 de 2020, por la cual se adopta la actualización del Documento Estratégico DE-039 Plan de Seguridad y Privacidad de la Información. Ítem 6.3 Acciones Particulares a Seguir, Tabla 2. Políticas de seguridad de la información.

Actividad 1: Revisión de la política de seguridad
Revisión periódica y aprobación de la política de seguridad de la información.

Diseño del Control: De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidad en el manejo de la periodicidad, los riesgos son cambiantes constantemente, en caso de mantenerse, se deben en el análisis de riesgos registrarlos como estadísticas para definir controles.

RIESGO 8: Acceso no autorizado a los sistemas de información instituciones

4) *Actividad de Control Analizada:* PR-131 MONITOREO ACCESO A LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN

. Actividad 2: Análisis de riesgos e identificación de monitoreo a realizar. MS-013 SEGURIDAD DE LA INFORMACION, monitoreo de:
Monitoreo al Recurso Humano: Monitorear los accesos y tareas realizadas por los usuarios habilitados para ingresar a los medios de procesamiento de información.
Monitoreo al hardware: Aplica a los componentes de hardware y a los logs de auditoria del mismo, implementados para seguimiento a usuarios.
Monitoreo al Software: Aplica a los procesos de software y al tratamiento de la información por parte de los usuarios.
Si hay incidentes
Actividad 4: Con la identificación en los monitoreos de las fallas en los procesos y/o procedimientos se deben establecer actividades de control con el fin de prevenir y neutralizar la materialización de los riesgos, corregir los riesgos ya materializados y mejorar lo que ya viene funcionando normalmente.
Actividad 5: Establecer y hacer seguimiento a actividades preventivas, correctivas y de mejora
Actividad 6: Con la identificación en los monitoreos de las fallas en los procesos y/o procedimientos se deben establecer actividades de control con el fin de prevenir y neutralizar la materialización de los riesgos, corregir los riesgos ya materializados y mejorar lo que ya viene funcionando normalmente.

Diseño del Control: De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidad en el manejo de la periodicidad, siendo la primera vez que se realiza en la entidad una actividad de penetración completa, se debe realizar al menos anual.

Normatividad o Criterio:

Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP v4, de octubre de 2018: Numeral 3.2 Evaluación de riesgos, 3.2.2 Valoración de los controles – diseño de controles.

Recomendación:

- Documentar las actividades de control relacionadas con el proceso de Gestión Contractual, en el flujo de actividades del procedimiento, con la inclusión de los 6 elementos de control dado por la Guía de Administración del Riesgo y el Diseño de Controles (DAFP, 2020).

Connotación: Administrativa.

Proceso: GESTIÓN CONTRACTUAL
Procedimientos: MS-012 Manual de Contratación, Supervisión e Interventoría

No.: 7
DEFICIENCIAS EN LA APLICACIÓN DE LOS PRINCIPIOS DE LA CONTRATACIÓN PÚBLICA: EFICACIA

Responsable de las acciones de mejora: SDAE

En la actualidad existen varias metodologías para la gestión de proyectos como son PRINCE2, PMI, XP, SCRUM entre otras; por lo tanto, es muy importante el análisis por fases de la formulación de un proyecto permitiendo un desglose completo lógicos que facilitan su planificación, ejecución, mantenimiento y finalización correcta ejecución de proyectos especialmente en áreas como integración, comunicación, cronograma, alcance y calidad.

Se realizó revisión de los contratos de GOOBI:

- 307 de 2006, por $ 216.050.000
- 1080 de 2011, por $ 29.893.200
- 1498 de 2012, por $ 28.536.000
- 179 de 2016, por $ 162.916.996
- 516 de 2017, por $ 79.135.000
- 692 de 2018, por $ 160.055.000
- 254 de 2020, por $ 165.267.200

Total= $841.853.396

Situaciones observadas en los diferentes contratos (ver **ANEXO 8)**:

- **307 de 2006:** Se le está diciendo adición a las prórrogas. Desde el inicio aparece como un GRP (*Goverment Resource Planning*).

- **1080 de 2011:** Se identifica que se realizaron solo actividades de mantenimiento y soporte. El acta de inicio empieza el año anterior al año de contrato
- **1498 de 2012:** El contrato no traía estudios previos, dentro del paquete contractual remitido no se encuentra el clausulado que debe formar parte del contrato para efectos de determinar cuáles son las obligaciones del contratista y con base en esto poder acreditar si este último cumplió con ellas.
- **179 de 2016:** En el informe 3179-2016.pdf suministrado se evidencia que Nómina y Cartera deberían estar en su totalidad, a la fecha nómina no es usado y cartera no se puede usar para alternativas comerciales y las otras funciones de cartera aplican parcialmente.
- **516 de 2017:** Se no evidencia que exista no conformidades ni desarrollos extras.
- **692 de 2018:** No se especifica las funcionalidades, existe una adición con renuncia que no es clara.
- **254 de 2020:** No se evidencia alguna ejecución en el SECOP II pero se encuentran las cuenta de cobro (ver **ANEXO 8 A** y **B).**

Análisis Técnico

Desde el año 2006 a la fecha, en la entidad se está utilizando GOOBI para atender la operación diaria. Dentro de la planificación y utilización del software han encontrado varias falencias, en donde se resaltan cinco factores:

- El IPES realiza pliegos de condiciones de manera adecuada, completa y oportuna en las características técnicas, pero observa debilidad por parte del proveedor que no ha entregado funcionales todos los procesos, entonces no existe una concordancia con lo que indica el supervisor y la realidad de la ejecución del contrato, por cuanto el supervisor acredita que el objeto contractual se cumplió a cabalidad, pero la realidad de la ejecución del contrato dice lo contrario.

- Falta planificación en cuanto el servicio de mantenimiento y soporte para cuando la entidad requiere, ya que un incidente que requiera apoyo profesional del fabricante o *partner* se puede manifestar en cualquier momento.

- Hay varias funciones como son los procesos de nómina y cartera que se han entregado varias veces, pero se ha identificado en mesas de trabajo con los usuarios finales que llevan mucho tiempo sin usarse.

- En el proceso de Gestión Documental desde el año 2006 se encuentra desarrollado, pero no cumple con las actividades de gestor documental.

- Ausencia de una metodología de gestión de proyectos que cubra las 5 etapas de un proyecto que son: inicio, planificación, ejecución, control y cierre como lo indica una metodología tradicional, o también se puede seguir una metodología ágil o un hibrido para llevar a operación total cada uno de los proyectos y asegurar retorno de inversión.

También se observa la ausencia en la aplicación de los objetivos de gobierno de COBIT como son BAI11 Gestionar los proyectos y DSS01 Gestionar las operaciones.

La ausencia de una metodología como las tradicionales como son por ejemplo PMI o PRINCE2 en que nos guía como se debe como documentar y poner en operación un proyecto una metodología ágil como es SCRUM, XP, SAFE entre otras que van orientadas a productos mínimos comercializables, afecta la puesta de producción de cualquier proyecto.

Análisis Jurídico

Desde el punto de vista jurídico, el régimen de contratación estatal colombiano está orientado y regido por principios y reglas de obligatorio acatamiento por parte de las entidades estatales para el cabal ejercicio de sus funciones. Esto es así, porque desde los postulados constitucionales encaminados a definir los fines esenciales del Estado, es necesario garantizar la inversión adecuada de los recursos públicos y la prevalencia del interés general sobre el particular durante las etapas precontractual, contractual y postcontractual; todo esto con el ánimo de asegurar la satisfacción de las necesidades ciudadanas y la garantía de los derechos de las personas.

En este contexto, se vislumbra la presencia de principios como la planeación, mediante el cual se busca que las entidades públicas procedan con la elaboración de estudios previos por medio de los cuales se justifique la necesidad, la conveniencia y la oportunidad de un determinado contrato antes de su celebración, en aras de lograr que todos los contratos suscritos estén sometidos y ajustados a los planes de desarrollo, de acción, de inversión y compras de la entidad estatal de que se trate.

Así mismo, principios como el de eficacia, particularmente relevante en cuanto tiene que ver con el cumplimiento de los fines esenciales del Estado en general y con los fines de la contratación estatal en particular, y que consiste en que todos los procedimientos y trámites de carácter contractual alcancen su cometido, evitando para ello decisiones inhibitorias y removiendo los obstáculos puramente formales que se presenten.

Estos principios: planeación y eficacia, encuentran su punto de partida en el principio de economía en la contratación pública, *"el cual propende por la obtención de los resultados que se buscan con esta actividad, es decir, el cumplimiento de los fines estatales, la continua y eficiente prestación de los servicios públicos y la efectividad de los derechos e intereses de los administrados que colaboran con las entidades públicas en la consecución de dichos fines estatales."* [2]

En este orden de ideas, se encuentra que la aplicación GOOBI no está agregando valor a la Entidad debido a que no está satisfaciendo las necesidades de ésta al no cumplir a cabalidad con los requerimientos técnicos que demanda el IPES para su adecuado funcionamiento y gestión administrativa a nivel interno, particularmente en lo que tiene que ver con los procesos de Talento Humano (Provisiones de Nómina), Operaciones de Ingresos (Cartera), Almacén y en todo lo relacionado con la Gestión Documental, en materia de trámites y expedientes, según se pudo establecer a lo largo de esta Auditoría y de

[2] RODRÍGUEZ TAMAYO, Mauricio. "Derecho Disciplinario de la Contratación Estatal". Primera Edición. Editorial Legis. Bogotá D.C., Colombia. 2020. Página 37

acuerdo con las evidencias aportadas para el efecto (Ver Hallazgo No. 2 – **ANEXOS 4, 5, 6 y 7**).

Lo anterior, lleva a colegir necesariamente que los procesos contractuales relacionados con la adquisición y funcionamiento de la aplicación GOOBI a lo largo del tiempo en la Entidad (si bien es cierto han contado con documentos precontractuales -Estudios Previos y Pliegos de Condiciones- elaborados de manera adecuada, completa y oportuna, desde el punto de vista técnico) en cuanto a la ejecución del objeto contractual no han contado con la eficacia suficiente, por cuanto, según se ha podido establecer, aunque las actividades de Supervisión respectiva han arrojado como resultado el cumplimiento satisfactorio de las obligaciones contractuales a cargo del Contratista, esto último, a todas luces, no se compadece con la realidad, debido a la presencia clara de variadas y reiterativas fallas en el funcionamiento de la herramienta tecnológica, según como se ha podido precisar con detalle mediante el análisis de las evidencias correspondientes.

Así pues, y con base en los argumentos expuestos, resulta forzoso concluir que los procesos de contratación alusivos a la adquisición y funcionamiento de la aplicación GOOBI han resultado eficaces en la práctica, por cuanto, según se ha podido evidenciar, la herramienta en mención no está logrando satisfacer a plenitud las necesidades puntuales para las cuales fue adquirida.

La ineficacia en la supervisión de los contratos tiende a no cumplirse los proyectos de acuerdo a los requerimientos de estudios previos.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR- 154 EJECUCION Y CIERRE DEL EXPEDIENTE CONTRACTUAL ACTIVIDAD DE CONTROL 3 EJECUTAR Y HACER SEGUIMIENTO AL CONTRATO y el MANUAL DE CONTRATACIÓN, SUPERVISION E INTERVENTORIA DEL INSTITUTO PARA LA ECONOMÍA SOCIAL – IPES, 5.3.2. EJECUCION DEL CONTRATO Y SEGUIMIENTO, 5 “CONDICIONES GENERALES” del PA04-PD-001 V5 “EJECUCIÓN Y CIERRE DEL EXPEDIENTE CONTRACTUAL”., Se presentó el siguiente Diseño de Control:

Control 1: De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidad en Procedimiento, Manejo de excepciones y evidencias, el procedimiento no asegura la ejecución de acuerdo a estudios previos, no se indica desviaciones y las evidencias de cumplimiento o su negativa no coinciden con los resultados.

Valoración comentarios del Auditado

Los comentarios dejados por la SDAE fueron:

> *“No se acoge la observación ya que como se expresa en la descripción “En la actualidad existen varias metodologías para la gestión de proyectos como son PRINCE2, PMI, XP, SCRUM entre otras”, las mencionadas metodologías son de la actualidad, el proceso en mención de adquisición del software ERP GOOBI se realizó en el 2006, época en la que no existían o no*

se encontraban adoptadas en Colombia las metodologías mencionadas, sin embargo no se puede afirmar que el proceso no fue planeado en debida forma, se puede apreciar fácilmente como desde la adquisición se efectuó la correcta planeación con la interacción de todos los integrantes de la entidad y los diferentes procesos, así mismo se puede verificar en las diferentes contrataciones, como se ha mantenido la operación y se ha hecho frente a los diferentes retos, propios de la función pública.
La ley 80 de 1993 y sus diferentes modificaciones contemplan las adiciones y prorrogas de contratos, el materializar alguna de estas actuaciones no representa la ausencia de buenas prácticas y el no cumplimiento del ciclo de vida de los proyectos, la gestión de los mismos contempla, bajo cualquier metodología las holguras propias de factores externos que conlleven al dinamismo de un proyecto y en la contratación estatal se evidencia en adiciones y prórrogas.
Así mismo cada contrato es una realidad jurídica independiente que no es comparable, así se trate del mismo proveedor ya que no se puede realizar la equivalencia ni en costos ni en tiempos del contrato de adquisición y desarrollo de un ERP, con un contrato de soporte del mismo.
Los diferentes contratos han surtido las diferentes etapas de la contratación estatal, se han ejecutado y liquidado según lo acordado, también los mencionados contratos han sido objeto de múltiples auditorías internas y externas incluyendo personal especializado en tecnología y no se han hecho este tipo de observaciones de ausencias de metodologías de proyectos.
Para la contratación de adquisición e implementación del sistema de Información goobi GRP en el IPES, se cumplió con fases de análisis, planeación, diseño, desarrollo, e implementación acorde con las necesidades de la entidad. Este desarrollo a la medida fue llevado a cabo en el año 2007 y el cual a través de los posteriores contratos ha continuado con ajustes pertinentes.
Cada contrato ha tenido un alcance diferente en su momento y por ende ajustes en su valor.
Se ha garantizado la planeación del proyecto. (Ver anexo, https://drive.google.com/drive/folders/1vyPXdh_780sV3s6Qjoo5A3XNvnUDoPr?usp=sharing)"

Análisis ACI: La gestión de proyectos se realiza con metodologías modernas como son PMI (1969), PRINCE2 (1996), SCRUM (1986), las cuales se usan para planificar y dirigir los procesos de un proyecto.

La gestión de proyectos comprende conceptos establecidos para lograr un objetivo con un alcance, recursos, inicio y final establecidos.

Los objetivos de la gestión de proyectos son:

- Gestionar el inicio y la evolución de un proyecto
- Controlar riesgos y responder ante inconvenientes que se puedan presentar o se presenten durante un proyecto
- Facilitar la aprobación, mantenimiento y finalización de un proyecto.

Sin embargo, y desde el punto de vista jurídico, no son de recibo los comentarios del auditado, por cuanto, si bien es cierto el régimen de contratación estatal colombiano contempla la presencia de figuras como la adición y la prórroga[3], esto está previsto

[3] No está de más advertir y reiterar (según como ya lo manifestó esta Asesoría de Control Interno en el Informe Final de Auditoría Interna Seguridad de la Información y Recursos Tecnológicos radicado 00110-817-006634 del 12-dic-2020) que figuras como la adición y la prórroga en la ejecución de un contrato estatal, si bien es cierto pueden ser herramientas útiles para el logro de los fines del Estado y aliviar así el impacto fiscal que pueda llegar a ocasionar la ruptura del equilibrio económico del negocio (específicamente aquellos de largo plazo), su empleo debe ser excepcional en virtud de los principios de planeación y seguridad jurídica, precisamente por la naturaleza vinculante del contrato y del principio de planeación. Así pues, la modificación (adición y/o prórroga) de que se trate, precisamente por su carácter excepcional, debe estar debidamente justificada con base en argumentos, pruebas y razones amparados en el ordenamiento jurídico.

justamente con el fin de llevar a cumplido efecto la satisfacción de las necesidades para las cuales se adelantan todos los procesos de contratación en sus diferentes etapas (precontractual, contractual y postcontractual), lo cual, y según se ha podido evidenciar en el desarrollo de esta Auditoría, no ha ocurrido, tornándose ineficaz, en la práctica, la adquisición y funcionamiento de la aplicación GOOBI, debido, precisamente, a que se ha demostrado su falta de idoneidad para satisfacer a cabalidad con las necesidades de funcionamiento y gestión administrativas de la Entidad.

En mérito de lo expuesto, el hallazgo se mantiene y el responsable del proceso debe establecer un plan de mejoramiento con acciones efectivas de mitigación del riesgo.

Riesgo Asociado: Ineficacia del proceso de contratación por deficiencias en los documentos previos del proceso contractual: Definición inadecuada de los bienes o servicios a contratar por la entidad, así como de las condiciones para la ejecución del proceso de selección.

Normatividad o Criterio:

CONSTITUCIÓN POLÍTICA DE COLOMBIA. ARTÍCULO 209. *La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones.*

Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La Administración Pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley.

LEY 80 DE 1993. ARTÍCULO 3º. DE LOS FINES DE LA CONTRATACIÓN ESTATAL. *Los servidores públicos tendrán en consideración que al celebrar contratos y con la ejecución de los mismos, las entidades buscan el cumplimiento de los fines estatales, la continua y eficiente prestación de los servicios públicos y la efectividad de los derechos e intereses de los administrados que colaboran con ellas en la consecución de dichos fines.*

Los particulares, por su parte, tendrán en cuenta al celebrar y ejecutar contratos con las entidades estatales que, además de la obtención de utilidades cuya protección garantiza el Estado, colaboran con ellas en el logro de sus fines y cumplen una función social que, como tal, implica obligaciones.

(El texto subrayado fue derogado por el art. 32 de la Ley 1150 de 2007).

LEY 80 DE 1993. ARTÍCULO 23. DE LOS PRINCIPIOS EN LAS ACTUACIONES CONTRACTUALES DE LAS ENTIDADES ESTATALES. *Las actuaciones de quienes intervengan en la contratación estatal se desarrollarán con arreglo a los principios de transparencia, economía y responsabilidad y de conformidad con los postulados que rigen la función administrativa.*

Igualmente, se aplicarán en las mismas las normas que regulan la conducta de los servidores públicos, las reglas de interpretación de la contratación, los principios generales del derecho y los particulares del derecho administrativo.

CORTE CONSTITUCIONAL. SENTENCIA C-508 DE 2002. M.P. ALFREDO BELTRÁN SIERRA.

"Los principios de la contratación estatal que el legislador enuncia, precisa de manera concreta y regula en los artículos 23 y siguientes de la Ley 80 de 1993, no son simples definiciones legales, sino normas de contenido específico, de obligatorio acatamiento en toda la contratación estatal, sea cual fuere la modalidad en que ésta se realice. Es decir, que tanto en el caso de la contratación mediante licitación pública o concurso de méritos, como en la contratación directa, son aplicables de manera estricta los principios que orientan la contratación pública, cuales son, la transparencia, responsabilidad, selección objetiva, economía, celeridad, imparcialidad y publicidad, en armonía con lo preceptuado por el artículo 209 de la Carta, que los instituye para el ejercicio de la función administrativa."

CONSEJO DE ESTADO SALA DE LO CONTENCIOSO ADMINISTRATIVO SECCIÓN TERCERA SUBSECCION B. C.P.: RUTH STELLA CORREA PALACIO BOGOTÁ D.C., VEINTIOCHO (28) DE MAYO DE DOS MIL ONCE (2012) RADICACIÓN NÚMERO: 07001-23-31-000-1999-00546-01(21489):

"(…)

***3.** Los principios de planeación, transparencia, responsabilidad y selección objetiva en la contratación estatal 3.1. Según lo tiene ya establecido la jurisprudencia, dentro de los principios capitales que de antaño han informado la actividad contractual del Estado, ocupa especial lugar el de economía, una de cuyas manifestaciones es la planeación. Por virtud de ésta la entidad estatal contratante está en el deber legal (Ley 80 de 1993 numerales 7, 12, 25 y 26 del artículo 25, e inciso segundo del numeral 1º del artículo 30) de elaborar, antes de emprender el proceso de selección del contratista, los estudios completos y análisis serios que el proyecto demande, los cuales inciden en la etapa de formación del contrato y en forma. (…)*

En tal virtud, el deber de planeación, en tanto manifestación del principio de economía, tiene por finalidad asegurar que todo proyecto esté precedido de los estudios de orden técnico, financiero y jurídico requeridos para determinar su viabilidad económica y técnica y así poder establecer la conveniencia o no del objeto por contratar; si resulta o no necesario celebrar el respectivo negocio jurídico y su adecuación a los planes de inversión, de adquisición o compras, presupuesto y ley de apropiaciones, según el caso; y de ser necesario, deberá estar acompañado, además, de los diseños, planos y evaluaciones de prefactibilidad o factibilidad; qué modalidades contractuales pueden utilizarse y cuál de ellas resulta ser la más aconsejable; las características que deba reunir el bien o servicio objeto de licitación; así como los costos y recursos que su celebración y ejecución demanden."

Ley 1474 de 2011 ARTÍCULO 83. SUPERVISIÓN E INTERVENTORÍA CONTRACTUAL. *Con el fin de proteger la moralidad administrativa, de prevenir la ocurrencia de actos de corrupción y de tutelar la transparencia de la actividad contractual, las entidades públicas están obligadas a vigilar permanentemente la correcta ejecución del objeto contratado a través de un supervisor o un interventor, según corresponda.*

La supervisión consistirá en el seguimiento técnico, administrativo, financiero, contable, y jurídico que, sobre el cumplimiento del objeto del contrato, es ejercida por la misma entidad estatal cuando no requieren conocimientos especializados. Para la supervisión, la Entidad estatal podrá contratar personal de apoyo, a través de los contratos de prestación de servicios que sean requeridos.

DECRETO 1082 DE 2015; ART. 2.2.1.1.1.6.1 - DEBER DE ANÁLISIS DE LAS ENTIDADES ESTATALES. La Entidad Estatal debe hacer, durante la etapa de planeación, el análisis necesario para conocer el sector relativo al objeto del Proceso de Contratación desde la perspectiva legal, comercial, financiera, organizacional, técnica, y de análisis de Riesgo. La Entidad Estatal debe dejar constancia de este análisis en los Documentos del Proceso.

PR- 154 EJECUCION Y CIERRE DEL EXPEDIENTE CONTRACTUAL ACTIVIDAD DE CONTROL 3 EJECUTAR Y HACER SEGUIMIENTO AL CONTRATO: *El contratista ejecuta el contrato de acuerdo al objeto y obligaciones contractuales. El supervisor del contrato realizara el seguimiento conforme a las obligaciones señaladas en el contrato.*

PMI: 1.4 ÉXITO DEL PROYECTO Y GESTIÓN DE BENEFICIOS

Los proyectos se inician para aprovechar oportunidades de negocio que están alineadas con las metas estratégicas de una organización. Antes de iniciar un proyecto, a menudo se desarrolla un caso de negocio para definir los objetivos del proyecto, la inversión requerida, y los criterios financieros y cualitativos para el éxito del proyecto. El caso de negocio proporciona la base para medir el éxito y el avance a lo largo del ciclo de vida del proyecto mediante la comparación de los resultados con los objetivos y los criterios de éxito identificados.

Por lo general, los proyectos se inician como resultado de una o más de las siguientes consideraciones estratégicas:

- *Demanda del mercado,*
- *Oportunidad estratégica/necesidad de negocio*
- *Necesidad social*
- *Temas ambientales*
- *Solicitud del cliente,*
- *Avance tecnológico,*
- *Requisito legal o regulatorio, y*
- *Problema existente o previsto.*

Un plan de gestión de beneficios describe el modo y el momento en que se entregarán los beneficios del proyecto y cómo se medirán los mismos. El plan de gestión de beneficios puede incluir lo siguiente:

- *Beneficios esperados. El valor de negocio tangible e intangible que se espera ganar con la implementación del producto, servicio o resultado.*
- *Alineación estratégica. El modo en que los beneficios del proyecto apoyan y se alinean con las estrategias de negocio de la organización.*
- *Plazo para obtener los beneficios. Beneficios por fase: corto plazo, largo plazo y continuos.*
- *Responsable de los beneficios. La persona o grupo responsable que monitorea, registra e informa los beneficios obtenidos en el transcurso del plazo establecido en el plan.*
- *Métricas. Las mediciones directas e indirectas utilizadas para mostrar los beneficios obtenidos.*
- *Riesgos. Riesgos asociados con el logro de los beneficios esperados.*

1.5 EL CICLO DE VIDA DEL PROYECTO

El ciclo de vida de un proyecto es la serie de fases que atraviesa un proyecto desde su inicio hasta su conclusión. Una fase del proyecto es un conjunto de actividades del proyecto, relacionadas de manera lógica, que culmina con la finalización de uno o más entregables. Las fases pueden ser secuenciales, iterativas o superpuestas. Los nombres, número y duración de las fases del proyecto se determinan en función de las necesidades de gestión y control de la(s) organización(es) que participa(n) en el proyecto, la naturaleza propia del proyecto y su área de aplicación. Las fases son acotadas en el tiempo, con un inicio y un final o punto de control (a veces denominado revisión de fase, punto de revisión de fase, revisión de control u otro término similar). En el punto de control, el acta de constitución del proyecto y los documentos de negocio se reexaminan en base al entorno actual. En ese momento, el desempeño del proyecto se compara con el plan para la dirección del proyecto para determinar si el proyecto se debe cambiar, terminar o continuar tal como se planificó.

COBIT 2019

BAI11 Gestionar los proyectos

Lograr los resultados definidos del proyecto y reducir el riesgo de retrasos inesperados, costes y erosión del valor mediante la mejora de las comunicaciones y la participación del negocio y de los usuarios finales. Asegurar el valor y la calidad de los entregables del proyecto y maximizar su contribución a los programas y al portafolio de inversión definidos.

DSS01 Gestionar las operaciones

Proporcionar los resultados de los productos y servicios operativos de I&T según lo planeado.

Recomendación:

- Documentar las actividades de control relacionadas con el proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, en el flujo de actividades del procedimiento, con la inclusión de los 6 elementos de control dado por la Guía de Administración del Riesgo y el Diseño de Controles (DAFP, 2020).
- Diseñar y madurar una metodología para la gestión de proyectos que se pueda integrar con la gestión de contratación pública.

Connotación: Administrativa con posible connotación disciplinaria.

9. PLAN DE MEJORAMIENTO

A la fecha, en el Archivo Excel *"FO-656 PLAN DE MEJORAMIENTO AUDITORIAS INTERNAS"* adjunto al presente informe han sido relacionadas las observaciones para que el Subdirector de Diseño y Análisis Estratégico SDAE, junto con los responsables de los procesos auditados, suscriban un Plan de Mejoramiento relacionando la causa raíz de cada observación, las acciones de mejora que mitiguen la causa raíz, los tiempos, responsables y los resultados entregables, para lo cual tiene 8 hábiles a partir de la fecha de radicación de este Informe Final.

La Asesoría de Control Interno realizará seguimiento al cumplimiento del Plan de Mejoramiento con el fin de asegurar que hayan sido tomadas las acciones definidas por el auditado y corregidas las observaciones.

10. ANEXOS

Anexo 1. Mapas de riesgos
Anexo 2. Muestra proceso gestión de seguridad de la información y recursos
Anexo 3. Proveedores tecnológicos autorizados DIAN
Anexo 4. Acta mesa de trabajo con usuarios finales de Nómina
Anexo 5. Acta mesa de trabajo con usuarios finales de Cartera- Alternativas Comerciales
Anexo 6. Acta mesa de trabajo con usuarios finales de Almacén
Anexo 7. Acta mesa de trabajo con usuarios finales de Gestión Documental
Anexo 8. Relación de observaciones de auditoría respecto a la contratación de GOOBI
Anexo 8A. Imagen de pagos de GOOBI 2020 en SECOP II
Anexo 8B. Imagen de modificaciones del GOOBI 2020 en SECOP II
Anexo 9. Acta de revisión de infraestructura de GOOBI
Anexo 10. Acta de recuperación de Back Ups