MEMORANDO

POR FAVOR AL CONTESTAR CITE EL No. DEL RADICADO
IPES - Correspondencia Administrativa- INTERNAS
Radicado: 00110-817- 006634
Fecha: 11/12/2020 - 08:32 AM
Remitente: CARMEN ELENA BERNAL ANDRADE
Destinatario: LIBARDO ASPRILLA LARA

110301

Bogotá DC.,

PARA: LIBARDO ASPRILLA LARA, Director General

DE: CARMEN ELENA BERNAL ANDRADE, Asesora de Control Interno

ASUNTO: Informe Final de Auditoría

Respetado doctor Asprilla:

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 2019, 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, y de manera transversal al proceso de apoyo: GESTIÓN CONTRACTUAL, a través de la socialización de observaciones con los auditados, en su defecto, la entrega de un

[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

informe preliminar para réplicas y finalmente, reunión de cierre de auditoría regular realizada el 10-dic-2020. Se remite el informe final de auditoría con el presente oficio.

Una vez radicado el Informe Final, en el Archivo Excel "FO-656 PLAN DE MEJORAMIENTO AUDITORIAS INTERNAS", la Subdirección de Diseño y Análisis Estratégico y la Subdirección Jurídica y de Contratación, 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.

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: 149 Folios y 1 Carpeta Comprimida en Drive con ANEXOS.

Copia:
Doctor CRISTIAN FELIPE GONZÁLEZ GUERRERO, Subdirector de Diseño y Análisis Estratégico (E)
Doctor DANIEL ALBERTO GALINDO LEÓN, Subdirector Jurídico y de Contratación (E)
Doctor JUAN CARLOS REYES ROJAS, Asesor del Despacho del Director General
Doctor JAVIER MORA ANDRADE, Asesor del Despacho del Director General

	NOMBRE, CARGO O CONTRATO	FIRMA	FECHA
Aprobó	Carmen Elena Bernal Andrade - Asesora de Control Interno	*Original Firmado*	10-dic-2020
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

ALCALDÍA MAYOR DE BOGOTÁ D.C. DESARROLLO ECONÓMICO Instituto para la Economía Social	**INSTITUTO PARA LA ECONOMÍA SOCIAL - IPES** **SISTEMA INTEGRADO DE GESTIÓN -SIG** **ASESORÍA DE CONTROL INTERNO** **Informe Final de Auditoría Interna**

Tipo de Auditoría	**Especial**		**Regular**	**X**	
Fecha Auditoría	27 de mayo al 25 de septiembre de 2020				
Dependencias	● Subdirección de Diseño y Análisis Estratégico - SDAE ● Subdirección Jurídica y de Contratación - SJC				
Procesos	● Gestión de Seguridad de la Información y Recursos Tecnológicos ● Gestión Contractual				

Contenido

1. CONTEXTO Y JUSTIFICACIÓN 2

1.1. ANTECEDENTES 2

1.2. DIAGNÓSTICO DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN..... 6

1.3.GLOSARIO..... 18

2. OBJETIVO GENERAL 20

3. ALCANCE 20

3.1. LIMITACIÓN AL ALCANCE 22

4. CONFORMACIÓN EQUIPO DE TRABAJO DE AUDITORÍA..... 22

5. FORTALEZAS..... 23

6. CONCLUSIONES..... 23

7. RESUMEN DE RESULTADOS DE LA AUDITORÍA 25

8. DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA 27

9. PLAN DE MEJORAMIENTO 149

10. ANEXOS 149

INFORME FINAL DE AUDITORÍA REGULAR
PROCESO DE APOYO GESTIÓN DE SEGURIDAD
DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS

1. CONTEXTO Y JUSTIFICACIÓN

Dentro de las competencias de la Oficina 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 Auditoría Interna de la vigencia 2020, aprobado por el comité institucional de Coordinación de Control Interno, la Asesoría de Control Interno programó una Auditoría Interna Regular al proceso de apoyo: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS a cargo de la Subdirección de Diseño y Análisis Estratégico. De manera transversal, al proceso GESTIÓN CONTRACTUAL a cargo de la Subdirección Jurídica y de Contratación.

Esta Auditoría comprende la FASE 1: ISO27001 SEGURIDAD DE LA INFORMACIÓN, que se llevó a cabo entre el 27-may-2020 al 25-sep-2020[1].

1.1. ANTECEDENTES

De acuerdo a la solicitud de la Dirección General del IPES el 14-ene-2019 a la Asesoría de Control Interno, la cual fue incluir en el Plan Anual de Auditoría Interna de la vigencia 2019, una auditoría regular basada en riesgos del proceso de SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECOLÓGICOS del Instituto, se asignaron recursos en el Plan Anual de Adquisiciones de 2019 por $91 millones.

El Decreto 648 de 2017, frente a la necesidad de regular la organización de las Oficinas de Control Interno, su rol y actualizar lo relativo al Comité de Coordinación de Control Interno en las entidades de la Rama Ejecutiva del orden nacional frente a las nuevas tendencias internacionales en materia de auditoría interna, en su artículo 17, modificatorio del artículo 2.2.21.5.3 del Decreto 1983 de 2015, señaló: *"… **Artículo 2.2.21.5.3 De las oficinas de***

[1] Radicado 00110-817-003084 del 26-may-2020 se notifica la Auditoría Regular, con alcance mediante radicados N° 00110-817-003347, 00110-817-003821, 00110-817-004267, 00110-817-004297 y 00110-817-004897 donde se amplía el cronograma de auditoría, por suspensión y posterior liquidación del CPS 1391726/2020 adjudicado al profesional que realizó la planificación de la presente auditoría desde el proceso de Gestión de Seguridad de la Información y Recursos Financieros. El CPS 1703540/2020 del 23-jul-2020 se reactivó la ejecución de auditoría en responsabilidad de otro profesional.

control interno. *Las Unidades u Oficinas de Control Interno o quien haga sus veces desarrollarán la labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención; evaluación de la gestión del riesgo; evaluación y seguimiento; relación con entes externos de control …"*

Para el cumplimiento de las funciones de la ACI, el Instituto mediante resolución 378 de 2016 asignó a la Asesoría de Control Interno para el ejercicio de sus funciones, la siguiente planta de cargos:

Tabla 1. *Planta de cargos asignada a la ACI – Res. IPES 378/2016*

DENOMINACIÓN DEL EMPLEO	CÓDIGO	GRADO	N° EMPLEOS
Asesor	105	1	1
Profesional Universitario	219	15	3
Auxiliar Administrativo	407	21	1

Sin embargo, dentro de este equipo interdisciplinario ningún profesional de planta cuenta con el perfil idóneo que pueda desarrollar la actividad que se requiere contratar.

Frente a lo anterior, el artículo 7° de la Ley 87 de 1993 faculta a las entidades estatales para contratar el servicio de control interno con empresas privadas, en los siguientes términos: *"… Las entidades públicas podrán contratar con empresas privadas colombianas, de reconocida capacidad y experiencia, el servicio de la organización del Sistema de Control Interno y el ejercicio de las auditorías internas. Sus contratos deberán ser a término fijo, no superior a tres años, y deberán ser escogidos por concurso de méritos en los siguientes casos: (…) b) Cuando se requieran conocimientos técnicos especializados. (…) Cuando por razones de conveniencia económica resultare más favorable."*

En este orden de ideas y como quiera que la Ley lo prevé y autoriza, de acuerdo al alcance aprobado del Plan Anual de Auditoría Interna de la vigencia 2019, respecto a la auditoría regular al proceso de apoyo GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS del IPES, se hacía necesario contratar los servicios de auditoría para procurar la asesoría, verificación y evaluación de todas las actividades que debe cumplir la Entidad en materia de tecnología de la información y comunicación, la asignación de los recursos y que ésta se realice conforme a las normas legales y constitucionales.

Se requería la contratación de los servicios de auditores con la experiencia e idoneidad para planear, ejecutar y presentar resultados de auditoría basada en riesgos para proporcionar aseguramiento en relación con el diseño y la operación de las actividades de control general del proceso de Tecnología de Información y Comunicación del Instituto para la Economía Social - IPES en ejecución del Plan Anual de auditoría Interna de la Asesoría de Control Interno de la vigencia 2019.

De acuerdo con lo anterior, el IPES debía seleccionar una empresa que prestara servicios especializados de auditoría basada en riesgos para proporcionar aseguramiento en relación con el diseño y la operación de las actividades de control de la tecnología de información y

comunicación del IPES; mediante la modalidad de concurso de méritos, toda vez que no existe acuerdo marco de precios vigente que incluya esta modalidad de auditorías.

Se adelantaron por parte de la ACI los estudios previos y demás documentos de la etapa precontractual del Concurso de Méritos, para llevar a cabo la adjudicación de los servicios a contratar en cumplimiento del Plan Anual de Auditoría Interna de la vigencia 2019.

Sin embargo, en comunicación establecida el 25-jul-2019 con la SDAE para la solicitud del CDP respectivo para esta contratación, la respuesta que se obtuvo es que no había recursos disponibles en el presupuesto para dar cumplimiento al Plan Anual de Adquisiciones asignado a la ACI respecto de esta contratación.

Mediante comunicación radicado 00110-817-006790 del 25-jul-2019 (Ver **ANEXO 1**), la ACI informó a la Dirección General del IPES los avances para la contratación por Concurso de Méritos para contratar los servicios especializados de auditoría de controles para el proceso de Seguridad de la Información y Recursos Tecnológicos. En la misma comunicación, la ACI solicitó:

> ***"Solicitudes a la Directora General***
>
> *Con el ánimo de prestar el mejor servicio desde el rol de Evaluador Independiente, de manera atenta me permito formular las siguientes solicitudes a la Directora General del IPES:*
>
> 1. *Asegurar la asignación de un presupuesto por valor de **$ 110.604.000** (CIENTO DIEZ MILLONES SEISCIENTOS CUATRO MIL PESOS M/L), con el fin de dar cumplimiento a la auditoría regular al proceso SEGURIDAD DE LA INFORMACIÓN Y RESCURSOS TECNOLÓGICOS del Instituto, en atención a su solicitud.*
>
> 2. *Informar por escrito a la Asesoría de Control Interno si se ejecuta o no la auditoría regular de TI solicitada por la Dirección General, en ejecución del Plan Anual de Auditoría Interna de la vigencia 2019 aprobado por el CICCI el 29-ene-2019. En consecuencia, la Asesoría de Control Interno adelantó las acciones necesarias para iniciar un proceso contractual de acuerdo a la solicitud de la Directora General, con seriedad y responsabilidad.*
>
> *A la fecha no hay claridad frente a la decisión de asignar o no los recursos por parte de la Ordenadora del Gasto, con el fin de contratar mediante concurso de méritos, los servicios especializados de auditoría basada en riesgos de TI. No es clara la decisión, teniendo en cuenta, por un lado, la solicitud de incluir esta auditoría por parte de la Directora General en el plan de la ACI y los comentarios realizados en Comités Directivos frente a la revisión de los alcances presentados para aprobación; pero en sentido contrario, la negativa de la SDAE frente a la disponibilidad de recursos para este proceso contractual.*
>
> *Por favor, tener en cuenta que en comunicación del 24-jul-2019 con radicado 00110-817-006714 la Directora General solicita informar el plan de choque para cumplir las actividades del Plan de Acción de la Asesoría de Control Interno,*

donde las auditorías regulares presentan al corte de 30-jun-2019 una ejecución del 40% (2 auditorías ejecutadas de 5 programadas, incluye la auditoría regular de TI).

3. *Teniendo en cuenta la importancia de la revisión del proceso de TI en el IPES por su nivel de criticidad en la identificación de riesgos y diseño de controles que aseguren un Gobierno y una Gestión de TI de acuerdo a las necesidades del IPES, como Asesora de Control Interno le sugiero a la Directora General tener en cuenta una de las siguientes opciones:*

   - *Asignar recursos para la contratación de servicios personales para 2 Ingenieros de Sistemas certificados en COBIT 5 e ISO 27001:2013, con el fin de que personalmente la ACI asuma la ejecución de esta auditoría regular basada en riesgos, sin llegar a la contratación de un externo, y poder cumplir así con el plan propuesto para 2019 y las expectativas de la Alta Administración.*

   - *Aprobar la inclusión de una partida presupuestal asignada a la Asesoría de Control Interno para la vigencia 2020 por $110.604.000 (CIENTO DIEZ MILLONES SEISCIENTOS CUATRO MIL PESOS M/L), con el fin de llevar a cabo esta auditoría regular de TI basada en riesgos en la próxima vigencia".*

No se obtuvo respuesta de esta solicitud por parte de la Representante Legal del IPES en la vigencia 2019. Por lo que se limitó el alcance de auditoría interna de la vigencia 2019 con la exclusión de la auditoría regular al proceso de apoyo GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS a cargo de la Subdirección de Diseño y Análisis Estratégico.

En consecuencia, el Plan Anual de Auditoría Interna para la vigencia 2020 presentado por la ACI y aprobado por el Comité Institucional de Coordinación de Control Interno en su sesión del 06-feb-2020, aprobó la inclusión de la presente auditoría regular con la asignación de recursos para su ejecución.

La presente auditoría incluye en el marco del Modelo Integrado de Planeación y Gestión MIPG:

- la identificación de riesgos de TI,
- la revisión de la efectividad y la aplicación de controles,
- la existencia de adecuados planes de contingencia, y
- las actividades de monitoreo vinculadas a riesgos claves de TI de la entidad;

Con el fin de proporcionar información sobre la eficiencia, efectividad e integridad de los controles tecnológicos y recomendar mejoras a las actividades de control específicas. Lo anterior en el marco de la metodología COBIT 5 y los estándares exigidos por la normatividad aplicable a las entidades públicas respecto a la norma ISO 27001 Seguridad de la Información.

La auditoría regular al proceso de apoyo GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS para la vigencia 2020 se ha definido en 2 fases:

FASE 1:
Evaluación de la administración de riesgos y diseño de controles de acuerdo al marco ISO 27001:2013 SEGURIDAD DE LA INFORMACIÓN. Riesgos principales frente a: Disponibilidad, Confidencialidad e Integridad de la Información.

FASE 2:
Diagnóstico de Control, con identificación de brechas del marco COBIT 5 *(Control Objetives for Information and related Technology),* con asesoría y acompañamiento de la ACI en la formulación de un plan de mejoramiento para el cierre de brechas.

COBIT 5: Proporciona un marco integral de ayuda a las organizaciones a lograr sus metas y generar valor mediante un gobierno y una administración efectivos de TI. Aplica un marco único integrado[2]:

- Corporativo: COSO, COSO ERM, ISO/IEC 9000 (Gestión de Calidad), ISO/IEC 31000 (Administración de Riesgos)
- Relacionado con TI: ISO/IEC 38500 (Estándar de Gobierno de TI), la serie ISO/IEC 27000 (Seguridad de la Información), TOGAF, ITIL, PMBOOK/PRINCE2, CMMI. [1]

Ver solicitud de la SDAE con expectativas de auditoría en la parte relacionada con Controles de TI, en **ANEXO 2.**

1.2. DIAGNÓSTICO DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Se hace necesario determinar el gobierno, la gestión de riesgos y control del proceso GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS por parte de la Administración del Instituto, mediante la aplicación de diferentes procedimientos e instrumentos de auditoría como: inspección en sitio, observación en tiempo real, entrevistas semi estructuradas, cuestionarios, listas de chequeo, registros fotográficos, pruebas de validación efectividad operativa de controles asociadas a los riesgos identificados y otras pruebas sustantivas.

En el marco de la FASE 1 de auditoría interna regular se aplicaron cuestionarios para medir el estado de cumplimiento del IPES frente a la norma ISO 27001:2013, mediante la realización de mesas de trabajo con las diferentes dependencias para efectuar el entendimiento de las actividades de control basadas en esta norma que fueron para el Instituto, en consecuencia, llevar a cabo un diagnóstico de controles de **manera alterna e independiente** teniendo en cuenta los instrumentos de diagnóstico del MINTIC aplicados por la Administración.

[2] Instituto de Auditores Internos - IIA

Este ejercicio se realizó con el fin de identificar las brechas en la aplicación técnica del marco de un SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN - SGSI respecto a la norma 27001:2013 de obligatorio cumplimiento para las entidades públicas en cuanto a Seguridad Digital, en contraste con el despliegue que al respecto de este marco se ha tenido históricamente en el IPES.[3]

En muchas actividades tanto con fines comerciales y sin ánimo de lucro, las tecnologías de la información y comunicaciones (TIC), la seguridad de la información, la seguridad de la informática, la continuidad del negocio y el servicio se han vuelto la estrategia para la sostenibilidad, el crecimiento y la creación de valor para las partes interesadas. La seguridad de la información y la continuidad del negocio se ha posicionado como un proceso estratégico dentro de las organizaciones para definir los riesgos, los controles, los sistemas de información, los procesos y roles y responsabilidades. La tecnología hoy en día define la estrategia para el procesamiento de la información y los repositorios de la información, lo que ha requerido una maduración a formalizar el Gobierno de TIC dentro de las organizaciones de todo tipo.

La gestión respecto de los activos de la información permite aprovechar y asegurar no solo los recursos que posee, sino también mejorar la prestación de los servicios de la operación. Asimismo, apoya la aplicación y ejecución de todos los procesos del Instituto, a través del uso adecuado de las tecnologías de la información y comunicación, la administración de los activos de información, la asignación adecuada del personal relacionado y el monitoreo de la disponibilidad a las partes interesadas. En una entidad como el IPES, la implementación de un SGSI no impactará de manera directa una mejora en la calidad de vida de la población atendida, pero si asegurará la protección de sus derechos y la oportuna atención de sus necesidades.

El diagnóstico de control fue el resultado de la aplicación de cuestionarios de control, lo que implicó el relacionamiento con otras dependencias diferentes a la SDAE como responsable del proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, y de manera transversal, otras responsabilidades frente al concepto de Seguridad de la Información, entendido desde la ISO 27002 (2013, p.6) como:

> *"La seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluyendo las políticas, procesos, procedimientos, estructuras organizacionales y las funciones de software y hardware.*
>
> *Estos controles necesitan ser establecidos, implementados, seguidos, revisados y mejorados, cuando sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y de negocios. Un Sistema de Gestión de Seguridad de la Información (SGSI) como el que se especifica en la norma ISO/IEC 27001 tiene una visión holística y coordinada de los riesgos de seguridad de la información de*

[3] De la Guía de Administración del Riesgo y el Diseño de Controles (DAFP, 2018): Para mitigar/tratar los riesgos de seguridad digital se deben emplear como mínimo los controles del anexo A de la ISO/IEC 27001:2013, estos también se encuentran en el **ANEXO 3:** *ESTADO DE LA SEGURIDAD DE LA INFORMACION DE LA ISO 27001:2013*.

> *la organización a fin de implementar un conjunto completo de controles de seguridad de la información en el marco global de un sistema de gestión coherente."* Subraya fuera de texto.

El Manual Operativo del MIPG (2018, p. 52) define Seguridad de la Información en el marco de la Política de Gobierno Digital, así:

> *"**Seguridad de la Información:** Busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de las entidades del Estado, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado."* Subraya fuera de texto.

A su vez, el MINTIC definió el siguiente alcance respecto a la Seguridad Digital en Entidades Públicas:

> *"El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Gobierno Digital, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital.*
>
> *El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.*
>
> *(…)*
>
> *La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.*
>
> *Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital."* Subrayas fuera de texto.

Por otro lado, también el MINTIC conceptualiza la Seguridad de la Información en la Guía para la Implementación de Seguridad de la Información en una MIPYME (2016, p.18) así:

> ***"4.1. SEGURIDAD DE LA INFORMACIÓN***
> *La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.*
>
> *El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.*
>
> *La seguridad de la información se encarga de garantizar la integridad, confidencialidad, disponibilidad de nuestra información."* Subraya fuera de texto.

Tomando como criterio de auditoría los anteriores conceptos, se concluye que:

En el MIPG se da lineamientos hacia la seguridad digital y el MinTIC tiene el objetivo de evolucionar al cumplimiento de la seguridad de la información en todas las organizaciones del estado y la orientación a la industria colombiana en el marco de la Política de Gobierno Digital. En cada versión de las guías del MSPI, el concepto de SEGURIDAD DE LA INFORMACIÓN se orienta a la mejora continua de este aspecto asociado a la continuidad del negocio. De los conceptos anteriormente relacionados, hay un punto en común, la unión de todos los procesos, personal e insumos que la Organización tiene a su alcance para implementar un Sistema Integrado de Seguridad de la Información (SGSI) garantizando la integridad, disponibilidad y confidencialidad de la información, que incluye todos los activos de información independiente de su repositorio, no solo el digital (informático), para crear valor a las partes interesadas.
Es por ello, que el alcance de la presente auditoría interna regular incluyó el análisis del nivel de maduración de los controles del marco ISO 27001: 2013 en todos sus componentes para todos los activos de información, con una visión articulada de los procesos.

Un SGSI debe estar orientado a la prevención y creación de valor de cada uno de los procesos, áreas funcionales, colaboradores y partes relacionadas del Instituto. Las entidades públicas deben buscar estándares y herramientas que les permita llevar a cabo sus esfuerzos en este sentido y dar cumplimiento a los requerimientos de la información y generación de valor público alineados con la estrategia de la organización, todo con el fin de incrementar la confianza de la ciudadanía y el valor de la información para las partes interesadas. En este sentido se presentan los siguientes resultados de auditoría.

Aplicación de Cuestionarios

Esta actividad fue realizada mediante seis (6) mesas de trabajo solicitando el acompañamiento permanente de un profesional del grupo de sistemas - delegado por SDAE: el Contratista Yamel Martínez, quien en las vigencias 2018, 2019 y 2020 fue contratado para la *"PRESTACIÓN DE SERVICIOS PROFESIONALES ESPECIALIZADOS, PARA EL FORTALECIMIENTO, IMPLEMENTACIÓN, MANTENIMIENTO Y MEJORA DE*

CONTROLES, LINEAMIENTOS Y DIRECTRICES PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL INSTITUTO PARA LA ECONOMIA SOCIAL – IPES", con obligaciones contractuales relacionadas con las funciones del Oficial de Seguridad de la Información[4] en las vigencias 2018 y 2019 y 2020.

En el desarrollo de estas mesas de trabajo se recibió información por parte de los diferentes actores requeridos en el marco de un SGSI, así como la verificación de la existencia de evidencias sobre los controles de aplicados. Se llevaron a cabo así:

- SAF, 20-ago-2020, funcionaria del proceso de Gestión del Talento Humano, Adriana María Parra Gómez
- SAF, 20-ago-2020, funcionario con cargo Almacenista del proceso Gestión de Recursos Físicos, Eduin Romero Burgos
- SDAE, 25-ago-2020, Contratista Yamel Orlando Martínez Balaguera con obligaciones contractuales relacionadas con las de un Oficial de Seguridad de la Información
- SDAE, 26-ago-2020, Contratista Yamel Orlando Martínez Balaguera con obligaciones contractuales relacionadas con las de un Oficial de Seguridad de la Información
- SAF, 27-ago-2020, Contratista Yasmidt Torres Esmeralda con obligaciones contractuales de apoyo a la supervisión del contrato de Seguridad Privada a cargo de la SAF
- SDAE, 31-ago-2020 (Acta de Cierre con socialización de resultados), Contratista Yamel Orlando Martínez Balaguera con obligaciones contractuales relacionadas con las de un Oficial de Seguridad de la Información

Los resultados obtenidos en la aplicación del cuestionario en la parte de los requerimientos obligatorios de la ISO 27001:2013 incluyó: (…) 4. Contexto de la Organización, 5. Liderazgo, 6. Planificación, 7. Soporte; indicaron una implementación del 44% como DEFINIDO, 30% como REPETIBLE, 19% como INICIAL, 7% como INEXISTENTE y no se evidenciaron requerimientos obligatorios en estado ADMINISTRADO y OPTIMIZADO. Ver tabla 2.

Ahora bien, los resultados obtenidos en la aplicación del cuestionario en la parte de los controles de la ISO 27001:2013 incluyó:

A5 Políticas de seguridad de la información
A5.1 Directrices de gestión de la seguridad de la información
A6 Organización de la seguridad de la información
A6.1 Organización interna
A6.2 Los dispositivos móviles y el teletrabajo
A7 Seguridad relativa a los recursos humanos
A7.1 Antes del empleo

[4] Manual Operativo del MIPG (2018, p. 112): "*El desarrollo de actividades de control se fortalece a partir de la implementación de la dimensión de Gestión con Valores para Resultados, de conformidad con las siguientes interacciones: (…) Acorde con la estructura de la entidad, el Oficial de Seguridad de la Información verifica el desarrollo y mantenimiento de controles de TI."*

A7.2 Durante el empleo
A7.3 Terminación y cambio de empleo
A8 Gestión de activos
A8.1 Responsabilidad sobre los activos
A8.2 Clasificación de la información
A8.3 Manipulación de los soportes
A9 Control de acceso
A9.1 Requisitos de negocio para el control de acceso
A9.2 Gestión de acceso de usuarios
A9.3 Responsabilidades de los usuarios
A9.4 Control de acceso a sistemas y aplicaciones
A10 Criptografía
A10.1 Controles criptográficos
A11 Seguridad física y del entorno
A11.1 Áreas seguras
A11.2 Equipos
A12 Seguridad de las operaciones
A12.1 Procedimientos operacionales y responsabilidades
A12.2 Protección contra códigos maliciosos
A12.3 Copias de seguridad
A12.4 Registro y seguimiento
A12.5 Control de software operacional
A12.6 Gestión de la vulnerabilidad técnica
A12.7 Consideraciones sobre la auditoria de sistemas de información
A13 Seguridad de las comunicaciones
A13.1 Gestión de la seguridad de las redes
A13.2 Intercambio de información
A14 Adquisición, desarrollo y mantenimiento de los sistemas de información
A14.1 Requisitos de seguridad en los sistemas de información
A14.2 Seguridad en el desarrollo y en los procesos de soporte
A14.3 Datos de prueba
A15 Relación con proveedores
A15.1 Seguridad en las relaciones con proveedores
A15.2 Gestión de la provisión de servicios del proveedor
A16 Gestión de incidentes de seguridad de la información
A16.1 Gestión de incidentes de seguridad de la información y mejoras
A17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio
A17.1 Continuidad de la seguridad de la información
A17.2 Redundancias
A18 Cumplimiento
A18.1 Cumplimiento de los requisitos legales y contractuales
A18.2 Revisiones de la seguridad de la información

Al respecto, se evidenció una implementación de controles del 36% en estado DEFINIDO, 18% como REPETIBLE, 20% como INICIAL, 15% como INEXISTENTE, 10% como

DESCONOCIDO, 2% como NO APLICABLE y no se evidenciaron controles obligatorios en estado ADMINISTRADO y OPTIMIZADO. Ver tabla 2.

La calificación del cuestionario incluyó los 14 dominios, 35 objetivos de control y 114 controles de la ISO 27001:2013 para conocer el nivel de implementación de los requerimientos para un SGSI (27 "debe" de la norma) y de la proporción de controles presentes y funcionando en IPES de acuerdo a su Matriz de Aplicabilidad (107 controles sobre 114 controles de la norma).

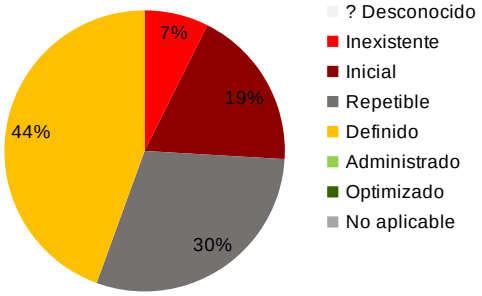
Las métricas: cada uno de los "debe" de la norma tiene un peso de 3.70 % (100% dividido 27 requerimientos) y los controles tienen un valor de 0.87% (100% dividido 114 controles), como se describen en la tabla 2, estos valores se determinaron con la media aritmética, también llamada promedio o media. La media aritmética se obtiene a partir de la suma de todos sus valores dividida entre el número de sumandos.

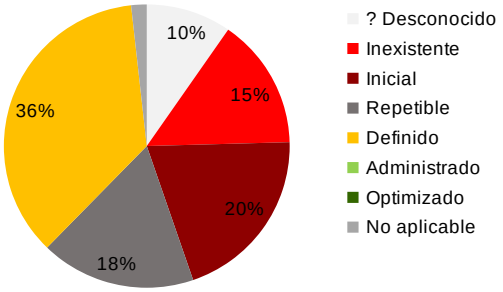
De acuerdo a este cuestionario, para calificar un requerimiento o control en un nivel OPTIMIZADO, se requiere que el control se encuentre aprobado y formalizado por la alta gerencia y el Oficial de Seguridad o el comité de seguridad; y que tenga los KPI (Key Performance Indicator, Indicador clave de rendimiento), definidos, y se demuestre el seguimiento a su cumplimiento.

Tabla 2. *Resultados Cuestionario de Controles ISO 27001:2013*

Estado	Significado	Proporción de requerimientos SGSI *Implementación*	Proporción de requerimientos SGSI *Controles*
¿? Desconocido	No ha sido verificado.	**0%**	**10%**
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	**7%**	**15%**
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	**19%**	**20%**
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	**30%**	**18%**
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	**44%**	**36%**
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	**0%**	**0%**
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	**0%**	**0%**

No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	**0%**	**2%**





En la Matriz de Aplicabilidad o *Statement of Aplicability* (SoA por sus siglas en inglés) desarrollado por la SDAE se definió un alcance de 107 controles frente a 114 en total del marco de aplicación ISO 27001:2013, presentando las siguientes características aquellos controles no incluidos en el alcance para el Instituto:

De los 114 controles del marco, la SDAE indicó que no aplican 2, los siguientes:

Tabla 3. *Controles ISO 27001:2013 que no aplican según SoA*

Control	Comentario Auditoría
A11.1.6 Áreas de despacho y carga: Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado	No aplican áreas de despacho.
A14.1.2 Seguridad de servicios de las aplicaciones en redes públicas: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	No aplica. Los servicios como página web, ERP-GOOBI y Herramienta Misional HEMI salen a redes públicas, pero son protegidas por la VPN. Por ejemplo, el correo electrónico está tercerizado y el proveedor se encarga de la respectiva protección sin necesidad de VPN.

De los 114 controles del marco, 5 se encontraron no especificados en el alcance de la Declaración de Aplicabilidad para el Modelo de Seguridad y Privacidad de la Información (MSPI) - CONTROLES DE LA NORMA NTC-IEC-27001-2013 (ANEXO A), así:

Tabla 4. *Controles ISO 27001:2013 no especificados según SoA*

Control	Comentario Auditoría
A14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación: Cuando se cambian las plataformas de	No se observó descripción del procedimiento para aplicación de este control. Sin embargo, en el diálogo con la Auditoría, la SDAE informó que este control está

Control	Comentario Auditoría
operación, se deben revisar las aplicaciones críticas del negocio y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la entidad.	asociado al servidor de desarrollo de Microsoft, pero no hay registro de esta actividad. Se recomienda documentar actividades como: aprobación de las soluciones tecnológicas cuando requieren una validación, evaluaciones de riesgo, recertificación de sistemas tras actualizaciones, mantenimiento, parches, cambios sistema operativo, actualizaciones de aplicaciones y cambios de cifrado, entre otros.
A15.1.3 Cadena de suministros de tecnología de información y comunicación: Los acuerdos con proveedores debe incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministros de productos y servicios de tecnología de información y comunicación.	No se observó descripción del procedimiento para aplicación de este control. Se recomienda documentar y validar las actividades relacionadas con los requisitos de seguridad de los productos o servicios adquiridos y la capacidad de recuperación cuando los productos o servicios críticos son suministrados por terceros.
A15.2.1 Seguimiento y Revisión de los servicios de los proveedores: Las Organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	No se observó descripción del procedimiento para aplicación de este control. Se recomienda documentar la manera de socializar la política de Seguridad de la Información a todos los proveedores con la seguridad de la información del Instituto, y no limitarlo solo a acuerdos de confidencialidad ni al cumplimiento de sus obligaciones contractuales.
A15.2.2 Gestión de cambios en los servicios de los proveedores: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	No se observó descripción del procedimiento para aplicación de este control. Se recomienda documentar y validar la manera cómo los proveedores comunican cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados. Se recomienda documentar la manera cómo se comunica a los proveedores los cambios en las políticas y requerimientos legales de la organización.
A16.1.3 Reporte de debilidades de seguridad de la información: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la entidad, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechosa en los sistemas o servicios.	No se observó descripción del procedimiento para aplicación de este control. Se recomienda documentar la manera comunicar al Equipo de Sistemas de la SDAE el reporte de cualquier tipo de ocurrencia inusual por parte de los empleados y contratistas.

Ver detalle del cuestionario aplicado en **ANEXO 3.**

Conclusiones del Diagnóstico

Se constataron por parte de esta auditoría los siguientes aspectos:

a. *El alcance del IPES se limita al aseguramiento de la información institucional digital, derivada del uso de la plataforma tecnológica, esto se puede validar en el: MS-013 MANUAL SEGURIDAD DE LA INFORMACIÓN, página 10, punto 7 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:*

> *"La (SIC) desarrollo de la presente política de seguridad y privacidad de la información, así como la definición, implementación, mantenimiento y mejora de los controles de seguridad informática cubren todos los activos de infraestructura tecnológica (servidores, equipos de cómputo, equipos de comunicaciones, entre otros) y a todos los activos de información, (Bases de Datos, Documentos, SIG, Servicios Informáticos, documentos, registros), a fin de proteger la información institucional digital contra daño, pérdida, sustracción, modificación accidental o intencional, describiendo buenas prácticas en el uso de los sistemas y servicios informáticos, así como de los activos de tecnologías de información y comunicaciones, dispuestos por el Instituto para la Economía Social a los usuarios para el cumplimiento de sus funciones. (…)"* Subraya fuera de texto.

Reconociendo la gestión realizada por la SDAE, se cuenta con un avance hacia la seguridad digital, pero resulta relevante madurar los procesos y los controles que ya se tienen formulados realizando una mejora continua mediante el monitoreo adecuado. Existen en el mercado diferentes metodologías, frameworks, normas, estándares que pueden apoyar la realización de la gestión sin necesidad de tener la presión de una certificación, pero generando valor con las medidas para proteger los activos de información los activos de la información del IPES, en sus diferentes formas y estados, con aplicación de controles para reducir los riesgos a un nivel aceptable, mitigando así las amenazas latentes.

En la ISO 27001:2013 en el punto *4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: "La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta Norma (…)"* Subraya fuera de texto. Se observó que el IPES ha realizado una gestión orientada a la seguridad digital, pero debe evidenciarse un avance hacia la mejora continua, una revisión periódica del estado de implementación de los requerimientos y controles para medir su avance y pasar a la implementación de un SGSI, que requiere no solo limitarse a la repetición de lo que se ha estado aprobando durante vigencias anteriores, sin responder a las variaciones del contexto del Instituto en el tiempo y el surgimiento de nuevas necesidades desde el punto de vista de la seguridad de la información.

Esta auditoría toma como marco conceptual de Seguridad de la Información, la ISO 27002[5]:

> *"**0.2 Requisitos de seguridad de la información***
>
> *Es esencial que una organización identifique sus requisitos de seguridad. Hay tres fuentes principales de requisitos de seguridad:*
>
> *a) La evaluación de riesgos para la organización, teniendo en cuenta su estrategia global de negocios y sus objetivos. A través de una evaluación de riesgos,*

[5] ISO/IEC 27002:2013, explica cómo se implementa la ISO 27001.

> *se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se estima el impacto potencial;*
> *b) Los requisitos legales, estatutarios, reglamentarios y contractuales que tiene que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio, y su entorno socio-cultural;*
> *c) El conjunto de principios, objetivos y requisitos de negocio para el manejo del procesamiento, almacenamiento, comunicación y archivo de información que una organización ha desarrollado para apoyar sus operaciones."*

Cómo lo indican los requisitos de la ISO 27002, la seguridad de la información es un concepto que abarca toda la organización y va más allá del aseguramiento de la información institucional digital, que es donde se encuentra limitado el alcance en el IPES.

b. *Cuando un control se encuentra administrado significa que se está llevando de acuerdo a un procedimiento documentado, aprobado y formalizado, no es posible indicar que los controles de seguridad de la información del IPES se encuentran en un nivel OPTIMIZADO ya que estaríamos haciendo referencia a que la entidad se encuentra lista para certificación ISO 27001:2013.*

Para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) se deben establecer buenas prácticas que mitiguen la ocurrencia de riesgos, vulnerabilidades y amenazas. Se destaca de un SGSI la aplicabilidad para la mejora continua. Todos los sistemas de gestión —de calidad, ambiental o de seguridad— se basan el ciclo PHVA: Planificar, hacer, verificar y actuar, por lo tanto, estaría articulado con el Sistema Integrado de Gestión (SIG), pudiendo lograr las siguientes oportunidades para el IPES:

- Estructura el sistema integrado de gestión (SIG): Un sistema de gestión integrado garantiza que los procesos de seguridad estén estructurados y coordinados en todos procesos de la organización.

- Reducir el riesgo de tener un incidente de seguridad: se puede identificar los riesgos y minimizarlos y aumentar el nivel de seguridad. Además, si se llegara a producir un incidente, ayuda a reducir los daños y los costos al tener un plan de continuidad del negocio.

La ISO 27001:2013, indica en el punto **1. OBJETO Y CAMPO DE APLICACIÓN** lo siguiente:

> *"Esta Norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. La presente Norma incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. <u>Los requisitos establecidos en esta Norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza</u>."* [6]
> Subraya fuera de texto.

[6] La ISO 27001:2013

Resulta importante que la Administración del Instituto tenga claridad frente a la aplicación de los conceptos y conocer las diferencias entre seguridad de la información, seguridad informática y comprender las limitantes del alcance *de "aseguramiento de la información institucional digital"*. Por lo cual se requiere la revisión del MS-013 MANUAL SEGURIDAD DE LA INFORMACIÓN, página 10, 7 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, y verificar el nivel de madurez del sistema para agregar valor al Instituto en temas de seguridad de la información, ya que se limita solo a las exigencias de la normatividad por parte del MINTIC, adoptando un enfoque de seguridad aplicado de manera exclusiva a herramientas tecnológicas.

Revisar y repensar hacer énfasis en la seguridad digital debido a que la seguridad de la información y la continuidad del negocio es un compromiso de la organización y de todas las áreas para así evitar riesgos financieros, reputacionales, operativos y jurídicos.

Citando a Bruce Schneider: *"La seguridad no es un producto, es un proceso"*[7].

c. *En este ejercicio se tuvo en cuenta la matriz de aplicabilidad, la gestión de riesgos y sus controles asociados definidos por la SDAE, evidenciando la importancia de enfatizar en conceptos como seguridad de la información vs seguridad informática.*

La presente auditoría aborda la aplicación de conceptos técnicos de la ISO 27001:2013 desde el punto de vista de la gestión de riesgos y la aplicación de controles, con el fin de ayudar a la Administración a estructurar y madurar en la entidad un SGSI (Sistema de Gestión de Seguridad de la Información) que se integre con el SIG (Sistema Integrado de Gestión).

El valor agregado de la evaluación independiente es traer otra mirada a los procesos para contribuir a su mejoramiento.

d. *Se realizó este ejercicio basado en la norma ISO 27001:2013 con el fin de encontrar las brechas a cerrar para llegar a un SGSI (Sistema de Gestión de Seguridad de la Información).*

Se observó que la SDAE limita su acción frente a un SGSI a la seguridad digital y la seguridad informática, creando una brecha respecto al concepto de seguridad de la información, como ya se explicó en párrafos antecedentes. Por lo tanto, este cuestionario de diagnóstico se realizó con el ánimo de establecer la madurez del sistema de seguridad de la información y proponer acciones de mejora para el cierre de brechas desde el punto de vista de los **procesos de gobierno, gestión de riesgos y control.**

[7] Bruce Schneider: Criptógrafo, experto en seguridad informática, y escritor. Es el autor de diversos libros de seguridad informática y criptografía, y es el fundador y oficial jefe tecnológico de Counterpane Internet Security. Libro "A Security Hero of Mine", 2000.

En conclusión, en general se obtuvo evidencias de la implementación de requerimientos y controles, en cada uno de los estados ya señalados en la Tabla 2; excepto las evidencias relacionadas con los siguientes controles:

A7 Seguridad relativa a los recursos humanos
A8 Gestión de activos
A11 Seguridad física y del entorno
A14 Adquisición, desarrollo y mantenimiento de los sistemas de información
A14.2 Seguridad en el desarrollo y en los procesos de soporte
A14.3 Datos de prueba
A18 Cumplimiento
A18.2 Revisiones de la seguridad de la información

Las brechas identificadas serán desarrolladas en las observaciones de auditoría del punto 5. DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA en este informe.

e. *La SDAE cuenta con profesionales con competencias para ejercer actividades y/o labores en seguridad de la información, asignados a otras actividades haciendo evidente la necesidad de un liderazgo con conocimientos y competencias en el tema de Seguridad de la Información.*

En la Resolución 307 de 2016 Manual Funciones Planta Global se evidenció que el líder en la SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO no incluye la exigencia de competencias y conocimiento para liderar un área de seguridad de la información y tampoco se requiere conocimientos para liderar los procesos de tecnología.

En los CONOCIMIENTOS BASICOS O ESENCIALES del cargo de subdirector (a) de Diseño y Análisis Estratégico se pide conocimiento en la presentación, evaluación y seguimientos de proyectos, evaluación financiera de proyectos no se ha evidenciado que se hubiera tenido una metodología para la gestión de proyectos.

La conformación del Equipo de Sistemas de la SDAE a cargo del proceso GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS que se observó en el detalle del **ANEXO 4 -** *Conformación del Equipo de Sistemas y/o Recursos Tecnológicos de la SDAE – A agosto/2020,* por niveles de atención.

1.3.GLOSARIO

Los conceptos técnicos utilizados en el presente informe:

Tabla 5. *Glosario*

Alta disponibilidad	Protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado.
Amenaza	Potencial ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas. Cuando el Agente de riesgo selecciona una víctima contra la cual pretende cometer un acto delictivo, automáticamente se convierte en una amenaza para ella. Se puede considerar que es la materialización del riesgo.
ANS/SLA	Acuerdo formal entre el cliente y el proveedor de servicios, registra los acuerdos de niveles de servicio).

Capacidad	Engloba tres subprocesos: gestión de la capacidad de negocio, gestión de la capacidad del servicio y gestión de la capacidad de los componentes.
Control Interno	Proceso que debe ser ejecutado por el directorio, la gerencia y el personal, es decir, por toda la Organización. Está diseñado principalmente para proveer una seguridad razonable acerca de los objetivos operacionales de reporte y de cumplimiento de la entidad.
Disponibilidad	Asegura que la infraestructura, los procesos, las herramientas y las funciones de TI sean adecuados para cumplir con los objetivos de disponibilidad propuestos.
Documentos	Serie conexa de formatos para realizar proyectos de resolución de problemas, o de mejora, basados en la realización del ciclo PHVA.
Formato	Lugar físico en el que se anotan los datos o registros. Un formato en blanco no es un registro hasta que se anotan datos en él. Los registros pueden utilizarse por ejemplo, para proporcionar evidencia de verificaciones, acciones, preventivas y acciones correctivas.
Framework	Entorno de trabajo, o marco de trabajo es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.
Help Desk	Su función consiste en escuchar los problemas técnicos que tienen los usuarios, interpretarlos con la mayor brevedad y dar una solución.
ISO	Organización Internacional de Normalización, también llamada Organización Internacional de Estandarización es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de normalización.
ITIL	Es una metodología que se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos que cubren las actividades más importantes de las organizaciones en sus Sistemas de Información y Tecnologías de Información.
ITSM	Information Technology Service Management/Gestión de Servicios de Tecnologías de la Información.
KPI	Indicador clave o medidor de desempeño o indicador clave de rendimiento, es una medida del nivel del rendimiento de un proceso. El valor del indicador está directamente relacionado con un objetivo fijado previamente y normalmente se expresa en valores porcentuales.
Maximum Tolerable Period of Disruption	MTPD, Periodo máximo tolerable de interrupción.
Metodología	Conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos.
OASIS	Acrónimo de Organization for the Advancement of Structured Information Standards (Organización para el Avance de Estándares de Información Estructurada, en idioma castellano), es un consorcio internacional sin fines de lucro que se orienta al desarrollo, la convergencia y la adopción de los estándares de comercio electrónico y servicios web.
OLA	Es un acuerdo entre el Proveedor de Servicios de TI y otra parte de ese mismo negocio que le provee servicios al proveedor.
PMI	Project Management Institute es una organización estadounidense sin fines de lucro que asocia a profesionales relacionados con la Gestión de Proyectos.
PRINCE2	Proviene del acrónimo en inglés Projects in Controlled Environments, es decir, convertir proyectos que manejan una carga importante de variabilidad y de incertidumbre en entornos controlados.
Puertas traseras	Es una secuencia especial o un término trasero dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autenticación) para acceder al sistema.
Recovery Point Objective	RPO, Objetivo del Punto de Recuperación.
Recovery Time Objective	RTO, Tiempo objetivo de recuperación.
Redundancia	Consiste en asegurar la supervivencia de la red ante un fallo, proporcionándole rutas de datos alternativas cuando se produce un fallo de enlace. Existen dos técnicas básicas de redundancia que aseguran la comunicación de datos: Redundancia activa: donde ambos enlaces están activos al mismo tiempo
Riesgo	Probabilidad latente de que ocurra un hecho que produzca ciertos efectos, la combinación de la probabilidad de la ocurrencia de un evento y la magnitud del impacto que puede causar, así mismo es la incertidumbre frente a la ocurrencia de eventos y situaciones que afecten los beneficios de una actividad.
SCRUM	Marco de trabajo para desarrollo ágil de software que se ha expandido a otras industrias. Es un proceso en el que se aplican de manera regular un conjunto de buenas prácticas para trabajar colaborativamente, en equipo y obtener el mejor resultado posible de proyectos.
SDQS	Sistema Distrital de Quejas y Solicitudes.
Seguridad de la Información	Conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.
Seguridad Informática	Ciberseguridad o seguridad de tecnología de la información,1 es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.
Servicio web/Web Service	Tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. Distintas aplicaciones de software desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma, pueden utilizar los servicios web para intercambiar datos en redes de ordenadores como Internet.
SGI	Sistema Integrado de Gestión, que constituye un mecanismo convergente de gestión para racionalizar, coordinar y organizar el trabajo, y así permitir el desarrollo de las distintas actividades.

SGSI	Diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.
SQL Injection	Método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos
Vulnerabilidad	Está íntimamente relacionado con el riesgo y la amenaza y se puede definir como la debilidad o grado de exposición de un sujeto, objeto o sistema. También son aquellas fallas, omisiones o deficiencias de seguridad que puedan ser aprovechadas por los delincuentes.
W3C	Consorcio WWW, en inglés: World Wide Web Consortium (W3C), es un consorcio internacional que genera recomendaciones y estándares que aseguran el crecimiento de la World Wide Web a largo plazo.
XP	Programación Extrema o eXtreme Programming es una metodología de desarrollo de la ingeniería de software formulada por Kent Beck, autor del primer libro sobre la materia, Extreme Programming Explained: Embrace Change.

2. OBJETIVO GENERAL

Realizar una evaluación y emitir una opinión independiente sobre el adecuado diseño y ejecución de los controles establecidos, para prevenir y mitigar los riesgos existentes en la ejecución del proceso de apoyo de Gestión de Seguridad de la Información y Recursos Tecnológicos a cargo de la Subdirección de Diseño y Análisis Estratégico SDAE. De manera transversal, se incluye el proceso de apoyo de Gestión Contractual a cargo de la Subdirección Jurídica y de Contratación SJC.

2.1. OBJETIVOS ESPECÍFICOS

2.1.1. Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos:

Identificar mediante el entendimiento y análisis del Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, las causas que pueden originar la materialización de los riesgos de seguridad, privacidad de la información y la infraestructura tecnológica del IPES, asociados al manejo de la información física y/o digital que se procesa, transmite y almacena en los sistemas de información de la entidad y los terceros, cumpliendo con estándares y normativas vigentes en la materia.

2.1.2. Proceso de Gestión Contractual:

Determinar si las etapas: Preparatoria, Precontractual, Contractual y Post-contractual de 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.
- Procesos sugeridos por dueños de los procesos o por la Alta Dirección.

- Nivel de Criticidad (*procesos sin identificación de riesgos, carencia de controles, alta rotación de personal, cambio de funciones, procedimientos, eventos recientes, SDQS, etc*.)
- Exposición a eventos externos e internos de la Entidad.
- Criterio profesional de los auditores aprobado por la Asesoría de Control Interno.
- Disponibilidad de recurso humano, técnico, financiero, etc.

Por lo anterior, esta Auditoría incluyó la verificación del cumplimiento a los siguientes procesos y procedimientos ejecutados durante las vigencias 2018, 2019 y lo corrido de la vigencia 2020:

Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos:

- DE-039 Plan de Seguridad y Privacidad de la Información
- DE-025 Plan de Contingencia
- DE-047 Plan Estratégico de Tecnologías de la Información y las Comunicaciones
- 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-132 Protección de Intercambio 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-085 Clasificación de Activos de Información
- IN-069 Gestión de Incidentes De Seguridad

Proceso de Gestión Contractual:

- MS 012 - Manual de Contratación, Supervisión e Interventoría
- PR 139 Selección Abreviada - Acuerdo Marco de Precios
- PR 141 Grandes Superficies TVEC
- PR 143 Etapa de Planeación Contractual - PAA
- PR 144 Etapa de Planeación Contractual Estudios Previos y Proyecto De Pliego
- PR 145 Etapa de Selección y Adjudicación
- PR 146 Etapa de Selección y Adjudicación Mínima Cuantía
- PR 150 Perfeccionamiento y Legalización del Contrato
- PR 152 Planeación Selección y Adjudicación Contratación
- PR 153 Etapa de Planeación, Selección y Adjudicación de Convenios y Contratos Interadministrativos
- PR 154 Ejecución y Cierre del Expediente Contractual

3.1. LIMITACIÓN AL ALCANCE

Debido a la Emergencia Sanitaria decretada por el Gobierno Nacional, y las medidas adoptadas por la Alcaldía de Bogotá, con motivo de la pandemia por COVID-19, y el inicio de la cuarentena obligatoria, la entrega de la información por parte de las áreas en los plazos inicialmente previstos se vio retrasada en 45 días hábiles del programa de auditoría inicial, por las siguientes situaciones:

- Decreto Distrital 081 del 11 de marzo de 2020, "*Por el cual se adoptan medidas sanitarias y acciones transitorias de policía para la preservación de la vida y mitigación del riesgo con ocasión de la situación epidemiológica causada por el Coronavirus (COVID-19) en Bogotá, D.C., y se dictan otras disposiciones"*
- Decreto Distrital 087 del 16 de marzo de 2020 *"Por el cual se declara la calamidad pública con ocasión de la situación epidemiológica causada por el Coronavirus (COVID-19) en Bogotá, D.C."*
- Decretos Distritales 90, 91, 106, y 162 de 2020 dentro de las que se encuentra la limitación a la libre circulación de personas y vehículos.
- Decreto 131 de 2020 "*Por el cual se imparten lineamientos para dar continuidad a la ejecución de la medida de aislamiento obligatorio en Bogotá D.C. y se toman otras determinaciones"*
- *Decreto 169 del 12 de Julio de 2020 "Por medio del cual se imparten órdenes para dar cumplimiento a la medida de aislamiento" preventivo obligatorio y se adoptan medidas transitorias de policía para garantizar el orden público en las diferentes localidades del Distrito Capital"*
- Decreto 186 de 15 de agosto de 2020 "*Por medio del cual se adoptan medidas transitorias de policía para garantizar el orden público en diferentes localidades del Distrito Capital y se toman otras determinaciones"*

Debido a esto, no fue posible efectuar las pruebas en campo relacionadas con una muestra de equipos asignados a Puntos Vive digital, Puntos de Venta y/o Plazas de Mercado para evidenciar el mantenimiento a la infraestructura. Esta prueba será incluida en la FASE 2 de auditoría.

4. CONFORMACIÓN EQUIPO DE TRABAJO DE AUDITORÍA

Auditor Responsable de Auditoría (ARA): Carmen Elena Bernal Andrade, Asesora de Control Interno

Contadora Pública, especializada en Control Gerencial Corporativo y en Gobierno, Gerencia y Asuntos Públicos, con 17 años de experiencia en auditoría.

Auditores

- *Rafael Eduardo Ortiz Gómez* – Ingeniero de Sistemas, Especialista en Seguridad de la Información – Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos.
- *Gabriel Sánchez Mejía* – Abogado, Especialista en Derecho Administrativo – Proceso Gestión Contractual.

Disponibilidad de recursos:

- Dos equipos de cómputo
- Una impresora con escáner

5. FORTALEZAS

En el Alcance se incluyeron los procedimientos, 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:

Proceso de Gestión Contractual:

- PR-139 Selección Abreviada – Acuerdo Marco de Precios
- PR-141 Mínima Cuantía
- PR-143 Etapa de Planeación Contractual–PAA
- PR-146 Etapa de Selección y Adjudicación Mínima Cuantía
- PR-150 Perfeccionamiento y Requisitos de Ejecución de Contrato
- PR-152 Etapa de Planeación, Selección y Adjudicación Contratación Directa

6. CONCLUSIONES

En los procesos y procedimientos evaluados se evidenció 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 de la Entidad.

De acuerdo con la Guía de Administración del Riesgo y el Diseño de Controles (DAFP, 2018) el siguiente es el análisis y evaluación del diseño del control de acuerdo con las seis (6) variables que deben estar documentadas en IPES en el marco del Sistema Integrado de Gestión - SIG:

Tabla 6. *Análisis y evaluación de los controles para la mitigación de los riesgos*

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DE CONTROL
1. Responsable	¿Existe un responsable **asignado** a la ejecución del control?
	¿El responsable tiene la **autoridad y adecuada segregación** de funciones en la ejecución del control?
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a **prevenir** la mitigación del riesgo o a **detectar** la materialización del riesgo de manera oportuna?
3. Propósito	¿Las actividades que se desarrollan en el control realmente **buscan por si sola prevenir o detectar** las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es **información confiable** que permita mitigar el riesgo?
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, **desviaciones o diferencias** identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?
6. Evidencia de la ejecución del control	¿Se deja **evidencia o rastro de la ejecución del control** que permita a cualquier tercero con la evidencia llegar a la misma conclusión?

Guía de Administración de Riesgos y Diseño de Controles (DAFP, 2018): Tabla 6. Análisis y evaluación de los controles para la mitigación de los riesgos.

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

Proceso Gestión de Seguridad de la Información y Recursos Tecnológicos:

- **PR-136 Atención Mesa de Ayuda**
  a. Deficiencias en gestión de atención en mesa de ayuda

- **PR-123 Gestión de Incidentes de Seguridad**
  b. Vulnerabilidades para seguridad de la información por limitante del alcance enfocado a seguridad digital
  c. Deficiencias en la gestión de los activos de la información

- **PR-033 BackUp, Generación y Recuperación**
  d. Desactualización procedimiento de back up, generación y recuperación

- **PR-133 Acceso a los Medios de Procesamiento de Información**
  e. Deficiencia en los lineamientos de seguridad de la información

- **PR-131 Monitoreo Acceso a los Medios de Procesamiento de Información**
  f. Inoperancia del plan de contingencia de TI
  g. Falta de pruebas al software y/o hardware para asegurar continuidad en los servicios críticos
  h. Deficiencias en el diseño de controles del proceso Gestión de Seguridad de la Información y Recursos Tecnológicos

Proceso de Gestión Contractual:

- **PR-144 Etapa de Planeación Contractual-Estudios Previos y Proyecto de Pliego**
  a. Inobservancia de principios que rigen la contratación estatal
  b. Deficiencias en los documentos previos del proceso de contratación

- **PR-145 Etapa de Selección y Adjudicación**
  c. Inobservancia de principios que rigen la contratación estatal

- **PR-154 Ejecución y Cierre del Expediente Contractual**
  d. Inobservancia normativa en la etapa postcontractual
  e. Deficiencias en la ejecución del contrato
  f. Deficiencias en el diseño de controles del proceso de Gestión Contractual

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 a los controles, 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 5 - MAPAS DE RIESGOS**), y que permitieron la identificación de los Hallazgos que se presentan a continuación.

En total se determinaron 13 Hallazgos, con connotación administrativa, de los cuales 3 con posible connotación disciplinaria:

Tabla 7. *Distribución de Hallazgos por proceso auditado*

N°	Proceso	Procedimiento	Total	%
1	***Gestión de Seguridad de la Información y Recursos Tecnológicos***	PR-123 Gestión de Incidentes de Seguridad	2	15%
		PR-131 Monitoreo Acceso a los Medios de Procesamiento de Información	2	15%
		PR-132 Protección de Intercambio de Información	0	0%
		PR-133 Otorgar Acceso a los Medios de Procesamiento de Información	1	8%
		PR-136 Atención Mesa de Ayuda	1	8%
		PR-033 BackUp, Generación y Recuperación	1	8%
		Transversal – Diseño de Controles	1	8%

	Total, Proceso Gestión de Seguridad de la Información y Recursos Tecnológicos		**8**	**62%**
2	***Gestión Contractual***	MS-012 Manual de Contratación, Supervisión e Interventoría	0	0%
		PR-145 Etapa de Selección y Adjudicación	1	8%
		PR-146 Etapa de Selección y Adjudicación Mínima Cuantía	0	0%
		PR-153 Etapa de Planeación, Selección y Adjudicación de Convenios y Contratos Interadministrativos	0	0%
		PR-139 Selección Abreviada - Acuerdo Marco de Precios	0	0%
		PR-141 Grandes Superficies TVEC	0	0%
		PR-143 Etapa de Planeación Contractual – PAA	0	0%
		PR-144 Etapa de Planeación Contractual Estudios Previos y Proyecto De Pliego	1	8%
		PR-150 Perfeccionamiento y Legalización del Contrato	0	0%
		PR-152 Planeación Selección y Adjudicación Contratación	0	0%
		PR-154 Ejecución y Cierre del Expediente Contractual	2	15%
		Transversal – Diseño de Controles	1	8%
	Total Proceso Gestión Contractual		**5**	**38%**
Total Hallazgos		**13**	**100%**	

Algunas de las **principales causas de las Observaciones de auditoría** pueden responder a:

a. 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.
b. La SDAE como cargo requiere incluir en su perfil funcional aquellos conocimientos y competencias relacionados con TI.
c. Ausencia de un Oficial de Seguridad de la Información, no obstante, se asignó desde marzo de 2018 esta función a un profesional de nivel universitario del Equipo de Sistemas de la SDAE.
d. El Equipo de Sistemas de la SDAE se encuentra integrado por 4 funcionarios: 2 de nivel profesional especializado, 1 de nivel profesional universitario y 1 técnico, el liderazgo lo asume el profesional universitario, con antigüedad en IPES de 12 años, lo que dificulta una gestión de cambio.
e. 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, por cuanto al depender de la calificación por parte del usuario para su cierre, no hay evidencia del cumplimiento de los tiempos establecidos, lo que impide conocer la suficiencia en la capacidad y disponibilidad del servicio de mesa de ayuda.
f. Inadecuada aplicación de las políticas de seguridad de la información, por desconocimiento.
g. Falta de documentación de políticas o desactualización de las mismas frente al marco normativo vigente y relacionada con la operación informática de la Entidad.
h. Falta de evidencias y/o registros de las pruebas efectuadas a los mantenimientos.
i. Debilidad en el levantamiento de requerimientos funcionales de los sistemas de información.
j. Desconocimiento y falta de aplicación de buenas prácticas en el respaldo de los sistemas de información.

k. Ausencia de un plan de contingencia actualizado contra daños que puedan ser ocasionados por incendios, inundaciones, terremotos, explosiones, perturbación del orden, y otras formas de desastre natural o artificial.
l. Desactualización del plan de contingencia, que incluye la sede alterna en alquiler denominada Sede Barichara para recuperación del servicio, cuyo contrato de arrendamiento terminó el 17-nov-2015 (Contrato 265 de 2014).
m. Fallas y debilidades en gestión de soporte informático respecto a la mesa de servicio.
n. Falta de documentación, desconocimiento o aplicación inadecuada de las políticas de seguridad de la información a través de los procesos.
o. Debilidades en el monitoreo, pruebas y valorización de las acciones preventivas frente a la revisión y reparación sobre los equipos de TI.
p. Falla en la infraestructura tecnológica.
q. Falta en la estrategia y los controles en la capacitación a los usuarios y concientización adecuados.
r. Daños en los equipos activos de la infraestructura tecnológica.
s. La entidad no está plasmando en los estudios previos un cálculo real de la necesidad que efectivamente requiere satisfacer independientemente de si cuenta o no con los recursos su satisfacción.
t. Ausencia y/o inoportunidad de publicación de documentos en SECOP.
u. La inaplicación de las obligaciones en la etapa pos contractual.
v. La entidad realizó el estudio de mercado del contrato de arrendamiento de las sede administrativa, sin tener en cuenta la uniformidad que debían tener las cotizaciones en cuanto el valor de las mismas.
w. Las actividades de supervisión y/o interventoría de la ejecución contractual no se realizaron de acuerdo a los parámetros establecidos en el Procedimiento de supervisión del IPES en MIPG ni los parámetros establecidos en la ISO 27001: 2013 en su control A.15.2.1 Seguimiento y Revisión de los servicios de los proveedores.

8. DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA

HALLAZGOS

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

No: 1

DEFICIENCIAS EN GESTIÓN DE ATENCIÓN EN MESA DE AYUDA

Responsable de las acciones de mejora: SDAE

En la revisión de una muestra de reportes de Mesa de Ayuda, no se observó el cumplimiento de los KPI (Key Performance Indicator, Indicador clave de rendimiento), y la gestión del

conocimiento obtenida sobre una muestra de los reportes. En particular, no fue posible establecer en auditoría:

- 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 escalamiento de una solicitud,
- El monitoreo por parte del Técnico del Equipo de Sistemas
- La evaluación periódica del cumplimiento de ANS y OLA aplicados a los servicios tecnológicos,
- El plan de contingencia en caso de poca disponibilidad del personal,
- La ejecución rigurosa del plan de mantenimiento de infraestructura tecnológica.
- La realización de pruebas para evidenciar que los requerimientos son seguros en el momento de pasar a producción.

Las situaciones observadas respecto a los reportes de la mesa de ayuda de febrero y marzo del 2020; enero, abril, julio y marzo del 2019; marzo, agosto, noviembre y diciembre del 2018, fueron:

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

a. La gestión de la mesa de ayuda presentó carencias en la optimización de los procesos y los KPI (Key Performance Indicator, Indicador clave de rendimiento) debido a que existe una brecha entre las diferentes metodologías, normas, frameworks existentes en el mercado, porque en la descripción del proceso PR-136 ATENCIÓN MESA DE AYUDA se omitieron conceptos, buenas prácticas y recomendaciones de marcos definidos como: ITIL, CMMI y COBIT, así evidenciar el cumplimiento del servicio de atención, medible para la gestión que realizan los agentes de la mesa de ayuda.

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.

En el MS-013 MANUAL DE SEGURIDAD DE LA INFORMACIÓN que da origen al artefacto DE-047 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, se aplica el control *A.16.1.1. Responsabilidades Y Procedimientos* de la ISO 27001:2013.

Sin embargo, en la revisión efectuada al servicio de Mesa de Ayuda y Atención de Incidentes, la SDAE confirma que no existe una gestión de capacidad y disponibilidad de los agentes que prestan el servicio, sino que se presta por cualquier profesional o técnico del Equipo de Sistema, lo que denota la importancia de definir los roles y responsabilidades de cada agente y medir la disponibilidad del servicio.

b. A partir de la contingencia por COVID-19, no se obtuvo evidencia de un control de cambios en el procedimiento PR-136 ATENCIÓN MESA DE AYUDA, ya que por la emergencia sanitaria presentada a nivel mundial se estaba realizando por medio de chat ante la realidad del trabajo en casa por parte de los colaboradores del IPES que ingresan por el siguiente enlace:

https://chat.google.com/room/AAAAdwmpQ40.

c. No se obtuvo evidencia del control contenido en el SoA (Aplicabilidad definida por el IPES para el modelo de Seguridad y Privacidad de la Información - MSPI): *A.16.1.7. Recolección de evidencia.* En la gestión de conocimiento de acuerdo a la casuística de cada servicio solicitado mediante Mesa de Ayuda, no hay un repositorio de conocimiento, quedando éste en el agente que atendió el caso. Este conocimiento y los KPI (Key Performance Indicator, Indicador clave de rendimiento) permite la toma de decisiones para realizar inversión correcta en los recursos y la toma de decisiones para el plan estratégico.

Es importante establecer una buena práctica para gestionar las tecnologías de la información de manera eficaz, dándole un enfoque capaz de ofrecer ventajas que van mucho más allá de las tecnologías de la información y así incrementar exponencialmente el desempeño general del negocio de ITSM (Information Technology Service Management/gestión de servicios de tecnologías de la información), la cual sirve como guía para orientar la atención del servicio, un ejemplo de ellas son ITIL v3 que está actual y ya se encuentra ITIL 4.

2. Ausencia de un Protocolo de la gestión de capacidad y disponibilidad

a. 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 la muestra de reportes de Mesa de Ayuda se pudo observar 300 casos abiertos entre enero de 2018 y febrero de 2020 de usuarios que tardaron en calificar los servicios, por más de 200 días, lo cual no cual no permite conocer la efectividad en la gestión de la Mesa de Ayuda. Ver detalle **ANEXO 7.**

La gestión de mesa de ayuda debe enfocarse en alinear los servicios de TIC, por lo tanto, es importante definir una metodología de trabajo como puede ser ITIL, para establecer los ANS/SLA (Acuerdos de niveles de servicio/ Service Level Agreement) más precisos a la disponibilidad y capacidad, y se puede realizar gestión del cocimiento ITSM. Al definir la gestión de capacidad y disponibilidad para atender incidentes y

desarrollar e implementar estrategias para realizar atención de la operación, logrando mejorar la generación de valor a los clientes a través de productos y servicios óptimos. Con el ITSM obtener datos de la gestión realizada para definir estrategias que generen valor a las partes interesadas.

b. 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, Indicador clave de rendimiento) son elementos de la gestión de procesos de negocio, por medio de esto se puede medir el rendimiento desarrollar un plan capacidad y disponibilidad para la gestión de mesa de ayuda, porque así se puede medir la cantidad de recursos y tiempos de respuesta para establecer atención oportuna y asegurar también la continuidad del negocio.

Acorde a la respuesta de la SDAE del radicado 00110-817-004574 del 27-ago-2020, se indicó [8]:

> *"No se observa la existencia de una definición mediante documento en el SIG que indique un plan de gestión capacidad y disponibilidad de como el personal se dividen los roles y responsabilidades y de cómo se encargan de asumir las responsabilidades y el apoyo para la gestión de soporte. La gestión de la capacidad y la disponibilidad se encargaría de optimizar y monitorizar los servicios TI para que funcionen de manera correcta e ininterrumpida por un valor razonable y soportado por recursos correctamente dimensionados. Además, permite automatizar la creación y cierre de incidencias ante indisponibilidades y/o capacidades comprometidas, controlando el KPI de cumplimiento de los SLAs y OLAs pactados con las partes interesadas. logrando la mejora continua para el PR-136 ATENCIÓN DE MESA DE AYUDA.*

Las anteriores situaciones se presentaron por 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, por cuanto al depender de la calificación por parte del usuario para su cierre, no hay evidencia del cumplimiento de los tiempos establecidos, lo que impide conocer la suficiencia en la capacidad y disponibilidad del servicio de mesa de ayuda.

Lo que podría ocasionar a la entidad la materialización de tipo riesgos operativos y reputacionales ya que los usuarios pueden indicar que no se está prestando el servicio de forma óptima y como se describe en el procedimiento de mesa de ayuda, así mejorar los KPI (Key Performance Indicator, Indicador clave de rendimiento)de atención a las fallas y debilidades en gestión de soporte informático respecto a la mesa de servicio. Demora, dilatación, interrupción o atrasos en la gestión institucional.

3. Ejecución de mantenimientos sin documentar las pruebas realizadas

[8] RESPUESTA A RAD 4574 SDAE radicado 00110-817-004574

Cuando se observó la rigurosidad del plan de mantenimientos se evidenció el cumplimiento de los planes de mantenimiento por parte de los proveedores ETB y FAMOC DE PANEL a los diferentes elementos tecnológicos y eléctricos de la Sede Administrativa, Plazas de Mercado y Puntos Comerciales, pero no se obtuvo evidencia de la ejecución del plan de pruebas.

Se observó la existencia de un plan de mantenimientos establecido para las vigencias 2018, 2019 y 2020, pero no se obtuvo evidencia de ejecución mediante actas, certificados y/o documentos que indiquen que todo lo programado se ha realizado a cabalidad o que justifiquen que se han modificado los planes establecidos.

Ver detalle en **ANEXO 8.**

Logrando la mejora continua para el PR-136 ATENCIÓN DE MESA DE AYUDA, tener un servicio optimizado y monitoreado para que los servicios TIC funcionen de manera eficiente y efectiva a un costo razonable y soportados por recursos correctamente dimensionados.

Esta situación puede presentarse por la falta de evidencias y/o registros de las pruebas efectuadas a los mantenimientos, lo que puede ocasionar incidentes en la continuidad de la operación del Instituto Para La Economía Social - IPES.

4. Falta metodología para desarrollo de requerimientos con seguridad

En el SoA (Statement of Aplicability, Declaración de Aplicabilidad)se observa que no se tienen metodologías de desarrollo de software seguro como puede ser OWASP afectando el control *A14.2.1 Política de desarrollo seguro: Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la entidad*, recordando que ningún componente es confiable hasta demostrar lo contrario como lo indica la ISO 27002.

En el PR-136 ATENCIÓN DE MESA DE AYUDA describen incidente y requerimiento, es importante recalcar que el concepto de requerimiento en ITIL se describe como: "*Este proceso se refiere a todas las solicitudes que generan los usuarios y que no están asociadas a un incidente en un servicio*", por lo tanto, es importante aclarar conceptos en el proceso.

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.

Un ejemplo de esta situación, lo evidenció la Contraloría de Bogotá en su informe de regularidad de la vigencia 2018 entregado en 2019 respecto a la implementación del Módulo de Cartera en el ERP-GOOBI sin llevar un paralelo de la base de datos de cartera en Access, donde observó (p. 120 a 139):

> ***"3.3.1.5 Hallazgo administrativo con presunta incidencia disciplinaria por cuanto al migrar la información de cartera a GOOBI no se surtieron los controles necesarios para garantizar su calidad y fiabilidad y no se realizaron todos los tratamientos contables señalados por la CGN para aplicar el NMNC y en especial lo relacionado con el traslado de cuentas de orden al no tener en cuenta la capacidad de pago de los deudores basados en el histórico del recaudo:***
>
> *(…) También se evidenció que el IPES, cambió directamente su sistema de información financiero de SIAFI a GOOBI, sin surtir el proceso paralelo que le permitiera garantizar la confiabilidad y realidad de sus reportes, adicionalmente la conciliación de la información de cartera con contabilidad se hizo hasta junio de 2018, como se estableció según acta de visita administrativa.*
>
> *En razón de lo expuesto, a falta de ver la importancia de la transición al nuevo marco normativo de regulación contable, no haber hecho el paralelo para implementar GOOBI, no tener desarrollo este aplicativo del módulo de cartera, no existir conciliación entre contabilidad y cartera, no haber tenido en cuenta el histórico de recaudo de los acuerdos de pago, se concluye que las cifras que reporta Cuentas por cobrar, no están garantizando las características fundamentales de la información financiera, como son confiabilidad, relevancia, comprensibilidad y comparabilidad."*

Donde el IPES debió controlar los requerimientos al proveedor IT-GOP y efectuar las pruebas de lo entregado según lo solicitado antes de pasar a producción, con la aplicación de metodologías como PMI, PRINCE2, SCRUM, XP, entre otras.

Por otro lado, el no establecer controles para desarrollos seguros con el fin de evitar amenazas y vulnerabilidades de seguridad sobre las aplicaciones pueden comprometer el *Core* del negocio llegando a materializar incidentes económicos y operativos por ataques como: SQL injection, Pérdida de autenticación y gestión de sesiones, Secuencia de comandos en sitios cruzados (XSS), puertas traseras, Redirecciones y reenvíos validados y otros más.

Estas situaciones pueden relacionarse con la debilidad en el levantamiento de requerimientos funcionales de los sistemas de información, lo que puede ocasionar sanciones administrativas, disciplinarias, deficiencias en la calidad de la información e insatisfacción por parte de los usuarios.

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 - Matriz de Riesgos y Controles: El líder del proceso de gestión de seguridad de la información verifica mensualmente, la ejecución de planes de mantenimiento por parte del equipo de sistemas, apoyado en los reportes de atención generados por la mesa de ayuda. Al presentarse fallas en la ejecución de tareas de mantenimiento, se realiza reasignación de soportes de usuario.

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.

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.

Control A.14.1.1 Análisis y especificación de requisitos de seguridad de la información: 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.

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 donde los resultados de las revisiones deberían ser llevadas al comité bajo la descripción, el proceso de mesa de ayuda requiere actualización en la terminología utilizada porque al utilizar el término: "requerimientos funcionales" que hace referencia a desarrollo de software y no a la toma de incidentes para mesa de ayuda.

Control 3: 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 4. Gestión de Activos.

Control A.8.1.1 Inventario de Activos. Revisión del inventario de Activos: Se debe llevar a cabo la revisión del inventario de activos tipo información y software, hardware y servicios. Validar la definición de estrategias para el etiquetado de activos de información. Verificar con gestión documental si están aplicando o exigiendo a los usuarios la aplicación del nivel de seguridad de los documentos.

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 porque realizando la validación de las vigencias, el Grupo Administración de Sistemas argumenta que no se les han presentado Incidentes de Seguridad, además los mantenimientos que se han realizado no se les evidencia que se realizaran planes de pruebas con el fin de conocer que en caso de tener que activar el plan de contingencia y de continuidad del negocio se asegure que todo se encuentre funcionando de manera correcta cuando se requiera.

Valoración comentarios del Auditado

El auditado argumenta que:

> *"Considerando los marcos de referencia para el Gobierno de TI, o metodologías para diferentes procesos misionales, administrativos o de gestión, las entidades públicas cuentan con la libertad para apropiar lineamientos, directrices, en general buenas prácticas de diferentes autores, bajo un entendido de mejora continua y optimización y de conformidad con necesidades específicas. Dicha apropiación no establece la OBLIGATORIEDAD frente a autores específicos. El IPES establece, y adopta el PR-136 Atención de Mesa de Ayuda, en el cual establece directrices para la atención de requerimientos a los usuarios, e incluye ANS que atiende la referencia del auditor a tiempos y medición. Dicho procedimiento no define conceptos como KPI que obedece a una metodología particular (No obligatoria).*
>
> *El PGSIRT remitió el procedimiento mencionado, métricas de atención a partir de reportes del sistema de información de atención de mesa de ayuda.*
>
> - *El PR-136 en su flujograma (característica de la metodología adoptada) establece la forma en que se escalan solicitudes. Se recomienda revisar el procedimiento.*

- *La información remitida de tiempos, en medio de la auditoría, evidencia el cumplimiento de ANSs, registrando los diferentes estados y momentos de un requerimiento con los tiempos de ingreso de la solicitud, asignación, gestión técnica, finalización a través de encuesta de satisfacción de usuario.*
- *La encuesta de satisfacción de usuarios fue socializada a la auditoría. A través de la encuesta se pretende evaluar el cumplimiento de ANS, así como la percepción de la atención brindada. OLA no es un término adoptado por la metodología del IPES en la definición del procedimiento.*
- *Plan de contingencia en caso de poca disponibilidad de personal: No es clara la apreciación, tal como se expuso en la presentación de observaciones del día 09 de octubre de 2020, El PGSIRT cuenta con 4 funcionarios vinculados a través de carrera administrativa, con diferentes roles, adicionalmente un equipo de contratistas que varía en su cantidad a través del tiempo, los requerimientos de mesa de ayuda surten un nivel de escalamiento según los recursos disponibles y la criticidad de cada caso en el momento de recepción del requerimiento. Por lo anterior se evidencia que existe suficiente capacidad instalada de recursos en donde un recurso humano del proceso puede suplir otro según la necesidad y el rol de cada cargo, sin embargo, no se considera oportuno que el IPES cuente con un BackUp o respaldo a nivel de personal para cada uno de los integrantes del equipo, para atender la observación, se debería duplicar la contratación de personal, en contra del principio de austeridad en el gasto de la función pública.*

La disponibilidad de los activos de infraestructura tecnológica y de usuario final (equipos de cómputo y periféricos) establece un claro cumplimiento de los planes de mantenimiento. A su vez se remitieron en los diferentes requerimientos los planes de mantenimiento tanto de equipos finales de usuario como de la infraestructura tecnológica, así como de los elementos propios del arrendador de la sede administrativa del Instituto.

- *Por último, "La realización de pruebas para evidenciar que los requerimientos son seguros en el momento de pasar a producción", el PGSIRT aclaró que los requerimientos asociados a cambios en sistemas de información o plataformas operativas en el IPES, no se atienden a través de la mesa de ayuda, por lo que no se podría observar como deficiencia en la atención de mesa de ayuda.*

No es clara la descripción de la observación y se mezclan diferentes conceptos que atienden necesidades diferentes.

Como se menciona en la observación 1, la entidad cuenta con una metodología específica para la definición de sus procedimientos, y es la entidad quien define qué aspectos de buenas prácticas adopta o no conforme a sus necesidades, no es determinante que se adopten estas metodologías y sean de obligatorio cumplimiento.

La adopción de una metodología requiere la apropiación importante de recursos técnicos, financieros y humanos, donde el contexto Institucional y el cumplimiento de su misionalidad prima sobre la destinación de recursos para cumplir requerimientos no exigidos por la normatividad vigente.

No se puede afirmar que no se tienen en cuenta las buenas prácticas, en la construcción de los elementos de gestión de calidad, tales como los procedimientos, planes, manuales, ya que como se ha evidenciado que por ejemplo en el procedimiento de mesa de ayuda se cuenta con acuerdos de niveles de servicio, roles, estados, en cada una de las diferentes actividades se materializan las buenas prácticas de diferentes metodologías.

La observación parece estar destinada al criterio de medición a partir del cierre de encuestas por parte de los usuarios, aspecto que no está establecido en el MS-013 o PETIC. En socialización del PGSIRT se indicó que el cierre de una encuesta no está ligado a la ejecución de tareas de mantenimiento o atención de requerimientos, sin embargo, se establecerán mecanismos para fomentar una cultura institucional para el cierre de casos de mesa de ayuda (tickets)

Como se menciona anteriormente el flujograma del PR-136 define el escalamiento de requerimientos, modelo que operan las diferentes soluciones de mesa de ayuda. No es clara la conclusión que confirma que no existe una gestión de capacidad y disponibilidad de los agentes que prestan el servicio, y no se entiende cómo se determina esta conclusión a partir del procedimiento, esta tarea debe ser producto de un análisis de cumplimiento de ANS, el cual

evidencie un inconformismo de usuarios por la NO ATENCIÓN generada por falta de disponibilidad y capacidad de respuesta.
Vale la pena aclarar que el MS-013 MANUAL DE SEGURIDAD DE LA INFORMACIÓN NO da origen al DE-047 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.
El Plan Estratégico de las Tecnologías de la Información y Comunicaciones es el artefacto que se utiliza para expresar la Estrategia de TI. Incluye una visión, unos principios, unos indicadores, un mapa de ruta, un plan de comunicación y una descripción de todos los demás aspectos necesarios para la puesta en marcha y gestión del plan estratégico. El PETI hace parte integral de la estrategia de la institución. Tiene como objetivo asegurar que las metas y objetivos de tecnologías de la información estén vinculados y alineados con las metas y objetivos de la Entidad.
La SDAE no ha confirmado que no existe una gestión de capacidad y disponibilidad de los agentes que prestan el servicio, por lo contrario, en diversas ocasiones se ha mencionado que existe y se ejecuta, sin embargo es posible que se encuentre una debilidad frente a la documentación de los roles.
Las medidas de contingencia no indican una necesidad para cambiar determinantemente un procedimiento, precisamente atienden a una Contingencia. Contingencia que como se comprende a nivel mundial, no tiene antecedentes en las últimas décadas donde se ha visto enmarcada el desarrollo de las tecnologías de la Información y las Comunicaciones -TIC-; En contraposición El PGSIRT adoptó medidas inmediatas para preservar la continuidad del servicio, donde estableció y divulgó los lineamientos (Circular 16 y 23 de 2020) en aras de preservar el acceso y servicios de TI para funcionarios y contratistas de la entidad; en la cual se pone a disposición de la entidad diferentes escenarios para el trabajo en casa y los canales de comunicación dispuestos para atención de requerimientos.
La base de conocimiento que genera valor en la atención de requerimientos, está contemplada al momento de documentar el cierre del requerimiento y es susceptible de reporte desde la base de datos. En medio de la auditoria se remitió informe de mesa de ayuda en donde se evidencia la gestión de cada caso, la cual queda en un repositorio único (En la base de datos de la herramienta mesa de ayuda), adicionalmente el usuario puede visualizar todo el tiempo la trazabilidad de la gestión realizada a su requerimiento (…).
Es importante establecer una buena práctica para gestionar las tecnologías de la información de manera eficaz, dándole un enfoque capaz de ofrecer ventajas que van mucho más allá de las tecnologías de la información y así incrementar exponencialmente el desempeño general del negocio de ITSM (Information Technology Service
Management/gestión de servicios de tecnologías de la información), la cual sirve como guía para orientar la atención del servicio, un ejemplo de ellas son ITIL v3 que está actual y ya se encuentra ITIL 4.
Se intenta descifrar el mensaje que se pretende dar con esta apreciación por parte de la ACI, en el sentido de buscar la Gestión de TIC´s más allá de las TIC´s, y la manera en que podemos incrementar exponencialmente el desempeño general del negocio a partir de la base de conocimiento en la atención de mesa de ayuda.
Una vez más se indica que la calificación de la mesa de ayuda mide la satisfacción del usuario en diferentes aspectos como oportunidad, amabilidad, efectividad entre otros, sin que esto permita establecer la atención o no por parte del personal del PGSIRT, estado que se evidencia en el momento del cierre del reporte por parte de la persona que realizó la atención. El estado atendido, no depende de la calificación brindada por el usuario.
En la actual herramienta de mesa de ayuda se cuenta con los diferentes tiempos y estados de solicitud, asignación, gestión técnica y cierre a través de encuesta de satisfacción, elementos suficientes para "conocer el estado del servicio solicitado, por cuanto al depender de la calificación por parte del usuario para su cierre, no hay evidencia del cumplimiento de los tiempos establecidos, lo que impide conocer la suficiencia en la capacidad y disponibilidad del servicio de mesa de ayuda."
Según los acuerdos de niveles de servicio estipulados en el Procedimiento de mesa de ayuda con la evaluación de tiempos en la herramienta de mesa de ayuda no se evidencia que se puedan materializar demoras, dilatación, interrupción o atrasos en la gestión institucional.

Existe una interpretación errónea en la observación frente al criterio por el cual se da cierre a un caso en la mesa de ayuda. El cierre de un caso en la mesa de ayuda, no depende de la calificación del usuario, el personal del PGSIRT realiza el cierre del caso una vez atendido el requerimiento y realiza la documentación respectiva, esto puede ser evidenciado en la plataforma.

Tal como se ha mencionado anteriormente, el proceso SI lleva un registro de tiempos de mesa de ayuda, remitidos en su momento al auditor, con los tiempos de la solicitud, asignación, gestión técnica y cierre del caso, por lo que la afirmación "esto conlleva a que la mesa de ayuda no lleve un récord del cumplimiento de los tiempos establecidos" no es cierta.

La gestión de mesa de ayuda no se enfoca en alinear servicios de TIC, afirmación que resulta algo preocupante ya que denota una visión equivocada frente a este procedimiento y que direccionara en otro sentido las conclusiones de la auditoría.

No es un requisito normativo y de obligatorio cumplimiento la apropiación de metodologías específicas y sus componentes como OLA o KPI. La gestión de capacidad y recursos no necesariamente parten de este tipo de componentes, para el caso de las entidades públicas y del IPES en particular el PETIC, los planes de acción y sus respectivos indicadores, así como la administración centralizada, mantenimiento, monitoreo y mejora de los activos de infraestructura tecnológica y de información institucionales, permiten la toma de decisiones frente a necesidades de TI.

Frente a "Acorde a la respuesta de la SDAE del radicado 00110-817- 004574 del 27-ago2020, se indicó 8: controlando el KPI de cumplimiento de los SLAs y OLAs pactados con las partes interesadas. logrando la mejora continua para el PR-136 ATENCIÓN DE MESA DE AYUDA..." esta no corresponde a una respuesta emitida desde la SDAE.

En el marco de la mejora continua y el desarrollo de MIPG, el proceso recibe retroalimentación de las necesidades de los procesos de la entidad que permiten tomar correctivos frente a la ejecución de actividades propias de los procesos. Así mismo la supervisión de procesos que incluyan terceros relacionados con TI, generan correctivos durante su ejecución, de ser necesario. El plan de acción y su seguimiento permite la toma de decisiones para el fortalecimiento de los procesos del Sistema Integrado de Gestión.

El PGSIRT aportó a lo largo del desarrollo de la auditoría, los soportes de la ejecución de planes en las diferentes vigencias, encontrando siempre, por parte del equipo auditor un requerimiento nuevo que denote un incumplimiento o la no ejecución de tareas puntuales. Es importante precisar que el SGSI toma como base el modelo PHVA que busca ajustar componentes del ciclo de vida del sistema de gestión, modelo que no sería operativo bajo el esquema de auditoría, ya que se fija un cumplimiento de 0% o 100%, dependiendo del aporte de una totalidad subjetiva de los soportes de cumplimiento.

Como se explicó en el desarrollo de la auditoría, el sistema de información administrativo y financiero Goobi, es un servicio tercerizado, el cual cuenta con ANS y condiciones técnicas para su soporte y mantenimiento, razón por la cual el establecimiento de una metodología de desarrollo seguridad al interior de la entidad, no minimiza los riesgos mencionados, los cuales son controlados desde la entidad a partir de obligaciones específicas, condiciones técnicas y ANS pactados con el proveedor.

Es importante aclarar a la auditoría un aspecto importante, considerando los hallazgos citados en la observación y que hacen relación a procesos FUNCIONALES, del sistema de información, procesos que no corresponden a un componente técnico responsabilidad del PGSIRT. En desarrollo de la auditoría se suministraron los soportes de las condiciones contractuales asociadas con Goobi.

Las metodologías citadas por el auditor, no corresponden a esta etapa del plan de pruebas del sistema de información, las cuales se enmarcan en lo funcional y son responsabilidad de los procesos ejecutados.

Se concuerda con la conclusión relacionada con el levantamiento de requerimientos, aclarando que este es un proceso que nace en lo funcional.

Se precisa que las metodologías de desarrollo solo aplican para desarrollos propios, en el caso de GOOBI, el proveedor debe tener su metodología que no depende del instituto, lo que solicita la entidad son los productos finales.

Adicionalmente la migración de datos se encuentra fuera de las metodologías expresadas en la observación, es muy diferente el desarrollo que la administración de los datos."

La Auditoría efectúa el análisis de los comentarios del auditado así:

Respecto a la réplica de la observación 1, se indica que, en la Guía Metodológica de Pruebas de Efectividad, Guía No.1: *"6 OBJETIVOS: La presente guía tiene como finalidad, indicar los procedimientos de seguridad que pueden generarse durante el proceso de evaluación en los avances en la implementación del modelo de seguridad y privacidad de la información**. Se procura que las entidades tengan un enfoque de seguridad en el cual se incluya el desarrollo y mantenimiento de la misma, realizando mejoras en las áreas que se requiera. Dependiendo de la entidad, dichos procedimientos pueden variar o si la entidad desea puede generar más procedimientos si lo considera conveniente."*** Negrita fuera de texto.

Por lo cual el IPES no se debe limitar a la normatividad básica, porque es obligación de cada entidad realizar mejoras en las áreas que se requiera, habilitando a las entidades del gobierno a generar más procedimientos si se requiere o es conveniente, por ello en base a la guía de MINTIC señala, no basta con la inclusión únicamente de las ANS en el PR-136.

En la misma Guía se lee: *"7 METODOLOGÍA DE PRUEBAS DE EFECTIVIDAD, La metodología de pruebas de efectividad **es una serie de actividades, que tienen por finalidad comprobar o medir la eficiencia de la implementación** del modelo de seguridad en las entidades. Esta metodología ha sido diseñada para ayudar a las entidades a entender y comprender, la realización de unas pruebas, los objetivos de las mismas y el beneficio que se obtiene al identificar sus etapas y gestionarlas."* Negrita fuera de texto.

Como se indica en el punto *"7 METODOLOGÍA DE PRUEBAS DE EFECTIVIDAD**, (…) toda entidad debe comprobar o medir la eficiencia de implementación** del modelo de seguridad, si el modelo desarrollado no se mide, se vuelve imposible conocer si se dan resultados positivos."*

En el punto *"8 ALCANCE, La metodología busca desde el primer momento **de la ejecución, crear una línea base del estado de seguridad de la entidad, es decir, facilitar la identificación de la brecha en la implementación del modelo de seguridad, entiéndase como línea base la primera medición**; las siguientes mediciones darán a la entidad la percepción de seguridad que manifiestan en la implementación del modelo de seguridad."* Negrita fuera de texto.

Por lo tanto, como se indica en el numeral 8 "ALCANCE", toda entidad debe detectar las brechas que van respecto a la seguridad de la información, lo cual incluye la continuidad de las operaciones. Por estas mismas razones se requiere la gestión de capacidad y disponibilidad del recurso humano del instituto, lo que no significa "duplicar la contratación de personal", sino establecer los roles de cada persona y como éstos roles pueden ser suplidos por otra persona durante la ausencia del titular.

En la información suministrada no se evidenció el cumplimiento de ANS debido a que los registros observados solo indicaron cuando inicio la solicitud, omitiendo los diferentes estados, el tiempo de finalización que fue cuando el usuario calificó la encuesta de calidad del servicio, por esta razón, el proceso utilizado en el IPES no permite evidenciar realmente cuando se cerró el caso.

EL IPES no es una entidad que crea consultorías, normas, frameworks y/o metodologías para la prestación del servicio, por lo tanto, el deber ser es adoptar las que han desarrollado entidades especializadas, una metodología de servicio es ITIL, la cual define ANS o SLA describe el nivel de servicio que un cliente espera de su proveedor y el OLA describe el nivel de servicio de la operación interna, igualmente, él área en su réplica manifiesta la adopción de buenas prácticas, sin embargo, no fueron ni mencionadas ni aportadas las prácticas a las que se refieren.

Respecto al plan de contingencia en caso de poca disponibilidad de personal, como lo indica el numeral 7 METODOLOGÍA DE PRUEBAS DE EFECTIVIDAD, de la guía 1 del MINTIC se debe indicar las pruebas y realizarlas con el fin de poder conocer su efectividad.

Respecto del numeral 1 literal a: Se recalca en la guía 1 de MINTIC “7 METODOLOGÍA DE PRUEBAS DE EFECTIVIDAD***, toda entidad debe comprobar o medir la eficiencia de implementación*** del modelo de seguridad, si el modelo desarrollado no se mide, se vuelve imposible conocer si se dan resultados positivos.” Por lo tanto, de la lectura de la norma citada, se evidencia la importancia de comprobar o medir la eficiencia, por cuanto al no medirse no se puede apreciar la gestión, razón por la cual, para la presente auditoria no es posible asegurar que el cumplimiento en el plan de mantenimiento sea suficiente para corroborar que los recursos disponibles son los suficientes para afrontar una situación de contingencia. Así mismo se aclara que la observación se adjudica al proceso de “mesa de ayuda” por cuanto, al no estar separado, es en este procedimiento donde únicamente se encuentra la actividad de “atención de incidentes”. En este mismo sentido, se señala que, la Auditoria toma como criterio de medición el cierre de encuestas por parte de los usuarios, por cuanto en el procedimiento PR-163 es el único índice que permite establecer que el caso se ha cerrado y teniendo que el área no aportó ni mencionó otro tipo de medición, se mantiene el criterio.

Respecto del numeral 1 literal b: La Circular 16 y 23 de 2020 indicaron los nuevos lineamientos para dar respuesta, pero al tener que cambiar la forma de prestación del servicio bajo los lineamientos del Sistema Integrado de Gestión del IPES y bajo lineamientos de ISO 27001:2013, requiere la generación de control de cambios.

Respecto del numeral 1 literal c y numeral 2 literal a: Respecto a la evidencia aportada, 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 162 del 30 de mayo de 2018. Por lo cual respecto a la evidencia aportada no es de recibo para esta auditoría, pues de la misma no es posible establecer su fuente por medio de una imagen, menos aun cuando en ejecución de la auditoría no fue suministrada dicha información, no obstante, haber suscrito una Carta de Representación. Igualmente, la auditoria basa su observación en las evidencias aportadas, por ello, no es posible afirmar que existe de manera adecuada una gestión de capacidad y disponibilidad de los agentes que prestan el servicio, toda vez que la misma, no se reposa en documento alguno.

Respecto del numeral 2 literal b: Se recalca en la guía 1 de MINTIC "*7 METODOLOGÍA DE PRUEBAS DE EFECTIVIDAD, toda entidad debe comprobar o medir la eficiencia de implementación del modelo de seguridad, si el modelo desarrollado no se mide, se vuelve imposible conocer si se dan resultados positivos*." En donde se indica la importancia de comprobar o medir la eficiencia, por cuanto al no medirse no se puede apreciar la gestión.

A continuación se relaciona imagen del contenido de la respuesta al radicado 00110-817-004574 del 27-ago-2020, conforme a lo aportado por la SDAE:

BOGOTÁ | DESARROLLO ECONÓMICO Instituto para la Economía Social

MEMORANDO

110301

Bogotá D.C.,

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

DE: CARMEN ELENA BERNAL ANDRADE, Asesora de Control Interno

ASUNTO: Respuesta a radicado 00110-817-004574 del 27-ago-2020

Respetada doctora,

De acuerdo a su requerimiento 4490, 4491 y 4493 del 25-ago-2020, se efectuó una revisión de su respuesta, toda vez que el texto justifica situaciones que se presentan en SDAE pero no concreta la existencia o no de los controles requeridos en el marco de la auditoría regular al proceso de GSRT, en la fase correspondiente a la aplicación de la norma 27001:2013 Seguridad de la información.

Sin embargo, en confirmación con el profesional YAMEL ORLANDO MARTINEZ BALAGUERA (como delegado de SDAE) mediante conversación telefónica el día 31 de agosto, se efectúan las siguientes aclaraciones por parte de la ACI y confirmaciones por parte de SDAE:

- Punto 1 y 2): SDAE confirma que el servicio de soporte se lleva a cabo en equipo entre toda el área de recursos tecnológicos, pero no se tiene documentado un plan de capacidad y disponibilidad de como el personal se dividen los roles y responsabilidades.
- Punto 10): punto c): SDAE confirma que se cumple con las directrices de MINTIC y la ACOTIC, el PGSIRT realiza la formulación de proyectos y objetivos estratégicos para los vigencias de cada plan de desarrollo. ACI evidencia la ausencia de una metodología para la gestión de los proyectos y además no se realiza el análisis del retorno de inversión de los proyectos (ROI/ROSI), lo cual es reconocido por la SDAE.
- En el punto 17): SDAE aclara que los sistemas de información: HEME, Portal Web IPES, Intranet IPES, CHIE, correo electrónico, herramientas hacedarias, mesa de ayuda, carteles digitales, Nagios cuentan con una arquitectura que

POR FAVOR ALL CONTESTAR CITE EL No. DEL MEMORANDO

BOGOTÁ | DESARROLLO ECONÓMICO Instituto para la Economía Social

permiten, el desarrollo de web service para integrar con otros sistemas de información.

- IPES 00110-817-004491 y IPES 00110-817-004492, SDAE aclara que el IPES no cuenta con un dispositivo dedicado únicamente para realizar balanceo de cargas, pero si genera balanceo de cargas de algunos servicios con otros dispositivos que se tienen integrados con la infraestructura para servicios como Internet y otros.

A propósito de su respuesta por haber una definición de Wikipedia a la solicitud de información radicado 4491 por parte de la ACI, a continuación, se aclara el concepto de dispositivos de balanceador de cargas:

  - Broadcom (Antiguo Blacoa ahora propiedad Symantec): Control de Tráfico Global Inteligente. https://www.broadcom.com/
  - IBM (Solución Cloud en conjunto con Citrix): distribuir el tráfico entre los servidores de aplicaciones que residen actualmente en un centro de datos. https://cloud.ibm.com/catalog/infrastructure/load-balancer-group
  - F5 y Su solución se llama plataforma BIG-IP, Local Traffic Manager (LTM): permite controlar el tráfico de la red, seleccionando el destino correcto en función del rendimiento, la seguridad y la disponibilidad del servidor. https://www.f5.com/pdf/products/big-ip-local-traffic-manager-ds.pdf

- Por último, el concepto de HIPEROPERABILIDAD comprende la disponibilidad empresarial para integrar una organización entre sus procesos y sistemas de información.

Cualquier inquietud o comentario, por favor contactarme con el Auditor Rafael Eduardo Ortiz al celular: 3004977771.

Cordialmente,

CARMEN ELENA BERNAL ANDRADE

	NOMBRE, CARGO O CONTRATO	FIRMA	FECHA
Elaboró	Rafael Eduardo Ortiz Gómez – CPS 1110341-2020 ACI	Original Firmado	31/08/2020
Revisó / Aprobó	Carmen Elena Bernal Andrade – Asesora de Control Interno	Original Firmado	31/08/2020

Los antes 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.

En el caso del control de cambios respecto de las medidas de contingencia, se señala que en el instructivo **IN-001 ELABORACIÓN, MODIFICACIÓN O ANULACIÓN DE DOCUMENTOS DEL IPES/ 6.1.7 Seguimiento y control de cambios** en donde establece que "El control de los documentos se encuentra bajo la responsabilidad de Gestión Documental y los **Líderes de proceso y/o subproceso**" y se solicita actualizar los documentos en una vez al año, cuando **no se realiza la actualización se debe realizar un control de cambios**", circunstancia que no se llevó a cabo en el PR-136,

durante la vigencia 2020 con ocasión de la emergencia sanitaria el cual corresponde al servicio de mesa de ayuda.

Respecto del numeral 3: Se recuerda que toda información solicitada por el equipo auditor debió ser suministrada de manera oportuna, en caso que sea información relacionada, el auditado tiene el compromiso de suministrarla. Se suscribió por parte de la SDAE carta de representación al inicio de la auditoría 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 162 del 30 de mayo de 2018.

Respecto del numeral 4: Al omitir controles de la ISO 27001:2013 como es el Control *A.14.1.1 Análisis y especificación de requisitos de seguridad de la información*, **en donde se** deben incluir en los requisitos para para mejoras a los sistemas de información existentes se estaría ofreciendo la oportunidad de puertas traseras e ignorando las posibles amenazas y vulnerabilidades que pueden tener cualquier sistema de información, la ausencia de una gestión de proyectos deja al IPES a voluntad de los proveedores las implementaciones de los proyectos.

En mérito de lo expuesto, el hallazgo se mantiene.

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.*

Manual MS-013 Manual de Seguridad de la Información. 12.6. Políticas Específicas de Usuario. Detalle de la Política. *Cualquier incidente o posible evento que afecte la seguridad de la información debe ser reportado inmediatamente al equipo de sistemas, o a la mesa de ayuda o al área designada para este fin*.

7.1 TABLA EXPLICATIVA DEL PROCEDIMIENTO. *BPMN (Business Process Model and Notation Business Process Model and Notation) Procedimiento.*

ISO: 27001:2013: A9.1.1. Política de control de acceso: *Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. //* **A.16.1.1. Responsabilidades y procedimientos:** *Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. //* **A.16.1.3 Reporte de debilidades de Seguridad de la Información:** *Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. //* **A.16.1.7. Recolección de evidencia:** *La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.*

2. Desconocimiento de la gestión de capacidad y disponibilidad

MANUAL OPERATIVO DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN – MIPG: 2ª. Dimensión: Direccionamiento Estratégico y Planeación: *Las capacidades organizacionales a diagnosticar pueden ser vistas desde dos perspectivas: estratégicas o*

funcionales. Las primeras enfocadas al ciclo de gestión: si se poseen o no sistemas de seguimiento y evaluación, sistemas de información estadística, si existen evaluaciones de la gestión gubernamental, entre otras, pueden dar cuenta de cuán robusta puede ser la institucionalidad.
Las segundas se refieren a los recursos que tiene a disposición la entidad para entregar productos y servicios en unas condiciones de calidad predeterminadas. Entre ellas se encuentra la infraestructura física, la tecnología existente, los equipos, la misma planta de personal y el talento humano que la compone, entre muchas otras.

Es imprescindible revisar todas las fuentes de información de las que disponga la entidad a fin de garantizar un mejor diagnóstico, entre los que se destacan los informes de gestión, estudios técnicos, informes de auditorías practicadas, resultados de medición de indicadores, resultados de medición de servicio al ciudadano o satisfacción, análisis de riesgos. Lo cierto aquí es que, para poder potenciar a una entidad, se requiere una mirada de 360° y analizarla, para identificar y determinar cuáles son las capacidades con que cuenta para entregar los resultados previstos, y calcular la eficiencia operacional actual que permita identificar cuál(es) capacidades son necesario fortalecer para conseguir lo planificado.

Lista Índices de Gestión y Desempeño, 6: Gestión del Conocimiento, Índice de Gestión del Conocimiento-D6, Política 15: Gestión del Conocimiento, Índice de Gestión del Conocimiento- POL15. *Mide la capacidad de la entidad pública de implementar acciones, mecanismos o instrumentos orientados a identificar, generar, capturar, transferir, apropiar, analizar, difundir y preservar el conocimiento para fortalecer a las entidades públicas, facilitar procesos de innovación y mejorar la prestación de productos y servicios a los grupos de valor.*

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)*

ISO 27001:2013: A.16.1.1. Responsabilidades y procedimientos: *Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.*

3. Ejecución de mantenimientos sin documentar las pruebas realizadas

Matriz de Riesgos y Controles: *El líder del proceso de gestión de seguridad de la información verifica mensualmente, la ejecución de planes de mantenimiento por parte del equipo de sistemas, apoyado en los reportes de atención generados por la mesa de ayuda. Al presentarse fallas en la ejecución de tareas de mantenimiento, se realiza reasignación de soportes de usuario.*

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.*

ISO: 27001:2013: A.8.1.1. Inventario de activos: *Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.*

4. Falta metodología para desarrollo de requerimientos con seguridad

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.*

ISO 27001:2013: A.16.1.7. Recolección de evidencia: *La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. //* **A.16.1.1. Responsabilidades y procedimientos:** *Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. //* **A.16.1.3 Reporte de debilidades de Seguridad de la Información**

Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

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, 2018).
- 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 la gestión de capacidad y disponibilidad para conocer las necesidades para cubrir el servicio y optimizar el tiempo de cumpliendo de las funciones de cada uno de los agentes y del área de seguridad de la información y recursos tecnológicos.
- Documentar la ejecución de los mantenimientos realizados y a los dispositivos de infraestructura tecnológica realizar un protocolo y documentar las pruebas a realizar para conocer el estado de todos los dispositivos tanto activos como pasivos.
- 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".*
- Actualizar el proceso PR-136 ATENCIÓN MESA DE AYUDA en donde se definiendo incidente de servicio.

Connotación: Administrativa.

Proceso: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS
Procedimientos: ***PR-123 Gestión de Incidentes de Seguridad***

N° 2:

VULNERABILIDADES PARA SEGURIDAD DE LA INFORMACIÓN POR LIMITANTE DEL ALCANCE ENFOCADO A SEGURIDAD DIGITAL

Responsable de las acciones de mejora: SDAE

En la revisión efectuada al manejo dado a los incidentes, documentación de controles sobre este tema en el Manual de Seguridad de la Información, se observaron debilidades en el enfoque hacia un SGSI, así como el incumplimiento de actividades de control definidas en el SIG frente a las siguientes situaciones:

- Enfoque de políticas, procedimientos e instructivos para la gestión de incidentes de seguridad de la información.
- Identificación y medición de los tiempos de respuesta ante incidentes de seguridad.
- Informes de gestión de incidentes de seguridad en la entidad
- Conformación de un equipo calificado para dar respuesta a los incidentes de Seguridad.
- Método de recolección de evidencias y pruebas forenses digitales.
- Revisión de las políticas complementarias a la seguridad de la información
- Aprobaciones de los cambios realizados a la política por parte del Comité de Sistemas y Seguridad de la Información.

1. Falta cobertura transversal del enfoque del SGSI

En el *A.5.1.2. Revisión de las políticas para seguridad de la información,* Se evidenció que la revisión que se realizó por parte del comité de seguridad no está evaluando como para desarrollar un SGSI (Sistema de Gestión de Seguridad de la Información), ya que el *MS-013 MANUAL SEGURIDAD DE LA INFORMACIÓN vigencia 2019, 5 POLITICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:*

> *"La Dirección del INSTITUTO PARA LA ECONOMÍA SOCIAL – IPES,* ***consciente del crecimiento de los riesgos de seguridad digital, derivados del uso*** *y masificación de las tecnologías de información y comunicaciones y considerando que la información es un activo esencial para la toma de decisiones encaminadas al cumplimiento de su misionalidad, se compromete a definir, implementar, mantener y mejorar un sistema de gestión de seguridad de la información que le permita contar con niveles apropiados de integridad, confidencialidad y disponibilidad de sus activos de información, en el marco del cumplimiento de las leyes, decretos, normas y lineamientos del orden Distrital y Nacional."* Negrilla fuera de texto.

Ha sido aprobado de la misma forma en las vigencias 2018 y 2019 limitante orientado a la seguridad digital.
Los objetivos del manual encontrados:

- *Establecer lineamientos, directrices, controles y en general la intención de la Dirección del Instituto para la Economía Social de consolidar el uso apropiado de los servicios de procesamiento de información, que permitan la protección de los activos de información institucional.*
- *Definir la responsabilidad en la definición, operación, seguimiento y mejora de las políticas institucionales relacionadas con la seguridad de la información en la entidad, al Comité Sistemas y Seguridad de la Información.*
- *Orientar a los funcionarios, contratistas y terceros sobre la responsabilidad de uso y buen manejo de los activos de información y de la infraestructura tecnológica que soporta la operación informática de la entidad.*

- *Definir aspectos a ser tenidos en cuenta por la entidad, relacionados con el talento humano y su responsabilidad en el uso de la información institucional antes, durante y en la terminación del vínculo laboral.*
- *Establecer directrices para la protección física de los activos de infraestructura tecnológica de la entidad.*
- *Establecer responsabilidades, controles y lineamientos en procura de proteger los sistemas y servicios informáticos por medio de los cuales se procesa la información institucional, que garanticen la operación informática de la entidad.*
- *Fomentar la conciencia alrededor de la importancia en el aseguramiento de la información institucional, la cual debe ser adoptada como una cultura organizacional.*

El MS-013 MANUAL SEGURIDAD DE LA INFORMACIÓN vigencia 2018-2019, no contenía métricas que indicaran el cumplimiento de sus objetivos.

Con las amenazas y las vulnerabilidades que se podían presentar cada día, es importante pensar en un sistema de gestión de seguridad de la información (SGSI) para tener un diseño, implantación y mantenimiento organizados en un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de los activos de la información.

Para la generación de valor en seguridad de la información es importante tener en cuenta que se debe seguir en una mejora continua y es importante ir creciendo hacia un SGSI (Sistema de Gestión de Seguridad de la Información) que cubra toda la organización. Al pasar de un esquema de seguridad digital a un sistema de Gestión de Seguridad de la Información (SGSI) tiene el objetivo asegurar que las organizaciones implemente todos los controles adecuados sobre la confidencialidad, integridad y disponibilidad de la información, para proteger la información de las partes interesadas (se deben incluir clientes, empleados, aliados estratégicos y la comunidad en general).

2. Debilidad en medición gestión de incidentes de seguridad de la información

a. Al revisar el PR-123 GESTION DE INCIDENTES DE SEGURIDAD V3, MS-013 MANUAL SEGURIDAD DE LA INFORMACIÓN no se obtuvo la suficiente evidencia para verificar que se estuviera realizando tal cual como se describe, y además no se han establecido KPI (Key Performance Indicator, Indicador clave de rendimiento), lo describe el proceso.

Cuando se revisaron las hojas de vida de los profesionales del Equipo de Sistemas asignado a la SDAE, se evidenció que hay personal que tiene conocimiento académico y competencias para cubrir los temas de seguridad de la información y seguridad informática, lo cual es un apoyo para sus funciones, pero no se evidencia que desde sus cargos no puedan potencializar su perfil orientado a madurar un SGSI. Ver **ANEXO 4.**

b. En el procedimiento PR-123 GESTION DE INCIDENTES DE SEGURIDAD V3 se observó que falta madurar y desarrollar una metodología para evaluar y definir de manera periódica los tiempos de respuesta, comunicaciones para el servicio.

En el punto 6. DESCRIPCIÓN DEL PROCEDIMENTO no se observó la actividad relacionada con la manera de comunicar a las partes interesadas los incidentes la continuidad del negocio, así como la definición de quién(es) cubren el incidente según ocurra.

Los *Logs* explican el comportamiento de nuestros sistemas o programas, no son útiles para la restauración. Son adecuados para un análisis forense como apoyo para poder definir alguna falla.

3. Falta procedimiento de manejo de información forense

En el MS-013 MANUAL SEGURIDAD DE LA INFORMACIÓN se nombraba el Procedimiento de Manejo de Información Forense y el Instructivo de Manejo de Información Forense, pero en el SIG no se identifica la elaboración de este documento.

4. Incumplimiento de funciones asignadas al Comité de Sistemas y Seguridad de la Información

En la revisión de las actas del Comité de Sistemas y Seguridad de la Información creado mediante Resolución IPES N° 615/2013, respecto a las vigencias 2019 y 2020, se observó el incumplimiento de la periodicidad de las reuniones definida para efectuarse cada dos meses. Se tuvo acceso a 2 actas del 2018, 1 del 2019 y 3 del 2020.

En el mismo sentido se observó el incumplimiento en las funciones correspondientes a la Secretaría Técnica a cargo de la SDAE, pues era su deber convocar a los integrantes al comité. En consecuencia, no se observó el cumplimiento de las siguientes funciones asignadas a este comité:

Artículo 4° de la Resolución 615/2013:

En la vigencia 2018:

> *1) Aprobar el plan estratégico de las Tecnologías de la Información y las comunicaciones.*
> *4) Fijar acciones específicas que ayuden a proveer un ambiente seguro y estable de recursos de información, que sea consistente con las metas, políticas y objetivos.*
> *8) Evaluar los requerimientos tecnológicos en materias TIC.*
> *9) Definir roles y responsabilidades que se relacionen con la seguridad de la información.*
> *10) Aprobar el uso de metodologías y proceso específicos para la seguridad de la información.*
> *11) Establecer las estrategias para la divulgación y comunicación de las políticas y normas que el IPES dicte en materia de seguridad de la información.*

Vigencia 2019:

1) Aprobar el plan estratégico de las Tecnologías de la Información y las comunicaciones.
9) Definir roles y responsabilidades que se relacionen con la seguridad de la información.
10) Aprobar el uso de metodologías y proceso específicos para la seguridad de la información.
11) Establecer las estrategias para la divulgación y comunicación de las políticas y normas que el IPES dicte en materia de seguridad de la información.
12) Las demás funciones inherentes a la naturaleza del comité.

Vigencia 2020:

1) Aprobar el plan estratégico de las Tecnologías de la Información y las comunicaciones.
2) Definir políticas de desarrollo y seguridad de la información.
3) Establecer acciones que mitiguen riesgos de pérdida que comprometan los recursos de información.
6) Impulsar la implementación del sistema de seguridad de la información.
9) Definir roles y responsabilidades que se relacionen con la seguridad de la información.
10) Aprobar el uso de metodologías y proceso específicos para la seguridad de la información.
11) Establecer las estrategias para la divulgación y comunicación de las políticas y normas que el IPES dicte en materia de seguridad de la información.

Ver detalle **ANEXO 9**.

5. Ausencia del rol Oficial de Seguridad de la Información

Se observó que en el Comité de Sistemas y Seguridad de la Información que sesionó del 13-mar-2018 se aprobó el cambio del Oficial de Seguridad de un profesional a un profesional de planta de la SDAE, sin embargo, la presente auditoria, verificó los siguientes CPS de la SDAE:

- 060/2018 por $ 51.500.000
- 720/2018 por $ 11.000.000
- 134/2019 por $ 50.985.000
- 705/2019 por $ 16.995.000
- 178/2020 por $ 11.330.000
- 311/2020 por $ 32.500.000
- 935/2020 por $ 18.200.000
- 311/2020 por $ 13.867.000
-

Para un total de $206.377.000 y cuyo objeto general era: *"Prestación de servicios profesionales especializados, para el fortalecimiento, implementación, mantenimiento y mejora de controles, lineamientos y directrices de seguridad de la información (…)".*

Por lo que, al revisar las obligaciones de dichos contratos asignados a un profesional externo, se describieron funciones propias del Oficial de Seguridad de la Información (se toma como muestra el CPS de 2019, pero los demás son iguales):

> *"1. Realizar un análisis y evaluación sobre el estado del sistema de seguridad de la información conforme a la normatividad distrital y nacional vigente, y proponer el plan de implementación y seguimiento del sistema de gestión de seguridad de la información de la entidad para el año 2019.*
>
> *2. Elaborar la propuesta del Sistema de Gestión de Seguridad con los dominios aplicables a la entidad de acuerdo con la norma NTC-ISO/IEC 27001-2013.*
>
> *3. Elaborar los indicadores de gestión y cumplimiento que permitan medir el grado de implementación del sistema de gestión de seguridad de la información.*
>
> *4. Realizar un análisis y revisión de los procedimientos y políticas correspondientes al sistema de gestión de seguridad de la información de la entidad, y proponer mejoras conforme a las necesidades de la entidad y la normatividad vigente.*
>
> *5. Realizar seguimiento y participar en el desarrollo de actividades correspondientes a la gestión de incidentes de seguridad de la información institucional.*
>
> *(…)*
>
> *7. Realizar la validación sobre el estado actual de los controles de seguridad de la información NTC-ICO/IEC 27001:2013 y apoyar a la entidad en el sostenimiento y maduración de su estado de avance en implementación conforme la normatividad distrital y nacional vigente."*

No se entiende la justificación de este contrato, habiendo sido asignada la función de Oficial de Seguridad del IPES a un funcionario, como se evidenció en el acta del 13-mar-2018:

Imagen 1. Nombramiento Oficial de Cumplimiento – 13-mar-2018

	FORMATO
	ACTA DE REUNIÓN
Tema: COMITÉ DE SISTEMAS Y SEGURIDAD DE LA INFORMACION	**Hora inicial: 8:30 A.M.** **Hora Final:**
Lugar y fecha: Sala de capacitaciones, Marzo 13 de 2018	
Objetivo: **Socialización Política de Seguridad de la Información**	
Agenda:	

	FORMATO
	ACTA DE REUNIÓN

Información y Responsable del tratamiento de los datos. Se plantea la posibilidad de modificar la resolución 715 de 2016 previa revisión del área jurídica de la necesidad.

Se acuerda en el Comité la delegación de los roles de la siguiente forma:

- Oficial de Seguridad de la Información: Se delega al profesional especializado del proceso de gestión de seguridad de la información y recursos tecnológicos, John Jair Garzón Delgado.
- Responsable del tratamiento de los datos: Se delega a la Subdirectora Jurídica y de Contratación.

El funcionario designado como Oficial de Seguridad de la Información, corresponde al nivel profesional Universitario desde octubre de 2018, el cual presentó los siguientes compromisos laborales para las vigencias 2018, 2019 y 2020:

2018-2019:

1) Diseñar el plan de trabajo de verificación de las bases de datos y servidores de bases de datos de acuerdo a las políticas institucionales.
2) Actualizar el inventario de aplicaciones utilizadas por las diferentes dependencias.
3) Elaborar diagnóstico de funcionalidades e interfaces del sistema de información misional HEMI y desarrollar plan de acción de mejora y nuevas funcionalidades.
4) Efectuar y proyectar políticas, estrategias, planes y programas para el funcionamiento de las tecnologías de información y comunicación.
5) Analizar la factibilidad técnica para y operativa para brindar el uso adecuado de sistemas de información en la entidad.

2019-2020:

1) Desarrollar plan de soporte en el funcionamiento de las bases de datos de acuerdo a las políticas de la entidad.
2) Analizar las alternativas de articulación de aplicaciones tecnológicas del inventario de herramientas usadas por las diferentes dependencias.
3) Ajustar el inventario de manuales de servicios informáticos y aplicaciones utilizadas en las diferentes dependencias.
4) Orientar las políticas para el mejoramiento del funcionamiento de las tecnologías de información y comunicación.

2020-2021:

1) Desarrollar y fortalecer estrategias de mejoramiento a la herramienta misional HEMI.
2) Diseñar, implementar y hacer seguimiento del plan de monitoreo y soporte en el funcionamiento de las bases de datos de acuerdo con la política de la entidad.
3) Analizar y elaborar el plan de contingencia a fin de mitigar los riesgos identificados.

No se observaron compromisos relacionados con las funciones de Oficial de seguridad de la Información.

El rol de Oficial de Seguridad de la Información debe contar con un alcance amplio al interior de una organización y debe estar directamente relacionado con la alta dirección, de manera estratégica. En los compromisos funcionales del profesional universitario de la SDAE designado para este rol, no fue posible establecer las actividades adelantadas en el marco de un SGSI, en el mismo sentido, la SDAE contrató desde 2018 hasta la fecha, a un profesional con asignación de obligaciones contractuales que desarrollan el rol de Oficial de Seguridad e la Información, que desarrolla las funciones asignadas a un profesional nombrado en carrera administrativa en el IPES.

Es evidente la deficiencia de gobierno del SGSI, debido a que no se observó la ejecución de esta responsabilidad con la autoridad e independencia requeridas, con relacionamiento directo con el más alto nivel de la Dirección y reporte periódico de actividades al Comité de Sistemas: ni por el profesional designado, ni por el profesional contratado, ni por la SDAE, de acuerdo a lo confirmado por el mismo auditado en sus comentarios de réplica.

Se incumplieron las funciones establecidas en el MS-MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 8.2 Oficial de Seguridad de la Información:

> *"El comité de sistemas y seguridad de la información, designará al oficial de seguridad de la información, el cual tiene como obligaciones principales:*
> *- Liderar el diseño de políticas, directrices y lineamientos encaminados a fortalecer la seguridad de la información.*
> *- Identificar el grado de madurez en la implementación del Modelo de seguridad y privacidad de la información en la entidad.*
> *- Socializar ante el comité de sistemas y seguridad de la información, los incidentes de seguridad de la información presentados, así como las acciones tomadas para reducir su impacto.*
> *- Coordinar las actividades correspondientes a la gestión de incidentes de seguridad, con la finalidad de contar con un enfoque estructurado y planificado que permita manejar adecuadamente los incidentes de seguridad de la información.*
> *- Establecer estrategias de defensa proactivas y reactivas.*
> *- Consolidar los procedimientos de seguridad informática y someterlos a decisión del comité de sistemas y seguridad de la información.*
> *- Desarrollar, mantener y comunicar las políticas, estándares y guías de seguridad de la información, especialmente, aquellas con un enfoque tecnológico.*
> *- Coordinador el análisis de riesgos de seguridad de la información y coordinar el plan para la mitigación de los mismos.*
> *- Elaborar o coordinar campañas de sensibilización.*
> *- Realizar capacitación y socialización del SGSI.*
> *El rol de Oficial de Seguridad de la Información, <u>será asumido por el/la subdirector (a) de Diseño y Análisis Estratégico, hasta tanto el comité haga oficial la designación del responsable a través de los medios dispuestos por la entidad."</u>* Subraya fuera de texto.

Las situaciones descritas anteriormente, tienen su origen en el desconocimiento o en la aplicación inadecuada de las políticas de seguridad de la información y a la falta de documentación de políticas o desactualización de las mismas frente al marco normativo vigente y relacionada con la operación informática de la Entidad, lo que podría ocasionar la

materialización de riesgos operativos, financieros y reputacionales ya que afecta directamente a la disponibilidad de los usuarios internos y externos al IPES.

Pueden existir vulnerabilidades y amenazas que se encuentran por fuera las políticas de seguridad de la información, que finalmente resulten en incidentes de seguridad de la información no identificados.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR-123 GESTION DE INCIDENTES DE SEGURIDAD, presentó el siguiente Diseño de Control:

Control 1: PR-123 Matriz de Riesgos y Controles: Los profesionales y técnicos de sistemas formulan anualmente un Plan de Capacitación en el marco institucional de Capacitación y realizan seguimiento mensual al cumplimiento de las actividades programadas, en caso de no desarrollarse alguna actividad se realiza la reprogramación en el Plan.

PR-123 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.

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 la atención de Incidentes para la prevención y corrección de posibles fallas de seguridad, el registro de los incidentes debe tener el alcance de la seguridad de la información para que sea transversal a toda la organización porque el registro de incidentes de seguridad no es únicamente a nivel tecnológico y/o digital, y en el manejo de excepciones de la estrategia de la capacitación a los usuarios de la entidad, asociados con Incidentes de Seguridad y como los deben reportar.

Control 2: 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.

ISO 27001:2013 - Dominio A.5 Políticas de seguridad de la información. Control A.5.1.2 Revisión de las políticas para seguridad de la información: Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas. (Subdirección de Diseño y Análisis Estratégico). // A.11.2.4. Mantenimiento de equipos:

Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas. (SAF/SADE - Sistemas).

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 excepción en donde si la revisión de la política se llevó a cabo tal como lo estipula la actividad, dicha revisión tuvo que pasar por el comité para su aprobación, además falta definir KPI (Key Performance Indicator, Indicador clave de rendimiento), y en la evidencia del cumplimiento de la política de seguridad revisar cumplimiento igualmente con Key Performance Indicator, Indicador clave de rendimiento), y documentar las actas de reunión en donde se pueda realizar seguimiento los compromisos.

Valoración comentarios del Auditado

El auditado argumenta que:

"La observación en su redacción no permite dar claridad sobre la idea que pretende ilustrar el auditor. Por una parte la observación habla del manejo de incidentes de seguridad de la información, a la vez se habla del límite en el enfoque del SGSI, y se finaliza con un incumplimiento de actividades de control definidas en el Sistema Integrado de Gestión - SIG.

Es importante aclarar que la entidad cuenta con una metodología para la gestión de incidentes de seguridad de la información, más allá de lo contenido en el MS-013:

- *PR-123 PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*
- *IN-069 INSTRUCTIVO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*
- *FO-625 DOCUMENTACIÓN DE INCIDENTES*
- *FO-626 LECCIONES APRENDIDAS RESPUESTA A INCIDENTES"*

"Es necesario que la auditoría aplique los principios que rigen la seguridad de la información, considerando que el establecimiento de un ALCANCE es de obligatorio cumplimiento para los sistemas de gestión de seguridad de la información alineados a la ISO 27001. El PGSIRT realiza la definición del alcance basado en buenas prácticas donde se indica que se debe iniciar por una parte de la organización para madurar el SGSI, lo cual no implica un acotamiento a los controles de seguridad y por ende limitar su accionar. Los controles de seguridad informática impactan de manera trasversal a toda la entidad y miden su efectividad en el aseguramiento de la información institucional.

El establecimiento de un SGSI que cubra la totalidad de la organización es una apuesta de la administración distrital, que debe ser escalable en el tiempo, atendiendo las necesidades primarias del quehacer misional, y estableciendo un equipo interdisciplinario que de cumplimento a los requerimientos globales propios del Sistema de Gestión de Seguridad de la Información.

La definición de un alcance depende del proceso, no es una exigencia normativa."

"Los requerimientos normativos van encaminados al establecimiento de metodologías para la gestión de incidentes de seguridad de la información, actividad que no implica un número mínimo de incidentes en un periodo de tiempo. Se pudo establecer en la presente auditoría que la falta de documentos que evidencien la materialización de incidentes de seguridad, está relacionada con la NO existencia de la metodología, es decir que se debe contar con un gran número de incidentes para poder establecer el cumplimiento de este componente.

Respecto al enunciado, "Cuando se revisaron las hojas de vida de los profesionales del Equipo de Sistemas asignado a la SDAE, se evidenció que hay personal que tiene conocimiento académico y competencias para cubrir los temas de seguridad de la información y seguridad informática, lo cual es un apoyo para sus funciones, pero no se evidencia que desde sus cargos no puedan potencializar su perfil orientado a madurar un SGSI", Si bien no son claras las ideas

que pretende exponer el auditor, y de acuerdo a la "interpretación" que fue posible realizar, es importante aclarar que el perfil del recurso humano que compone el PGSIRT está acorde a las funciones u obligaciones de acuerdo a la naturaleza de cada cargo, por lo cual el término empleado "apoyo" desmerita la competencia que tiene el recurso humano frente los empleos y sus funciones. Desconociendo el manual de funciones y los procesos de selección de meritocracia realizados a través de organismos públicos como la Comisión Nacional del Servicio Civil.

Así mismo, en lo que compete al comentario "pero no se evidencia que desde sus cargos no puedan potencializar su perfil orientado a madurar un SGSI"; Se interpreta subjetividad respecto a la apreciación que se realiza, ya que ni la norma MSPI o la ISO27001, establece cuales son los requisitos académicos y de experiencia con el cual debe contar el recurso humano que tiene a su cargo funciones dentro de un SGSI.

Adicionalmente se aclara que un Sistema de Gestión de Seguridad abarca todos los procesos de una organización, para lo cual, debe consolidarse un equipo interdisciplinario que aporte, desde su competencia, lo necesario para madurar un SGSI."

"En el numeral 3 se establece la responsabilidad al comité de sistemas y seguridad de la información, la responsabilidad en la aplicación de la metodología para la gestión de incidentes. El PGSIRT realiza las actividades operativas del comité y ejecuta las tareas de gestión de incidentes de seguridad asociados a la plataforma tecnológica."

"Dentro de las actividades de mantenimiento y mejora del SGSI, se deben ejecutar tareas de actualización y control de documentos soporte, el procedimiento existe, se desconocen las razones por las cuales no se encontró en la carpeta compartida."

"Como es de conocimiento de la Asesoría de Control Interno, durante las vigencias 2018 y 2019, se adelantaron numerosas sesiones del comité de sistemas y seguridad de la información, en el marco de las sesiones de comité directivo, en donde se incluida dentro del orden del día y la respectiva convocatoria, temas de seguridad de la información, para la toma de decisiones, como por ejemplo el proyecto de adquisición, implementación y puesta en operación de una solución integral de BackUp. Dichas actas reposan en la Dirección General.

Como se aprecia en la conclusión de la auditoría, no se podía adelantar la contratación de un recurso humano, para cumplir con unas obligaciones específicas, si se cuenta con el Oficial de Seguridad de la Información dentro de la planta del Instituto; fundamento que carece de certezas considerando factores como:

El rol de oficial de seguridad de la información cuenta con un alcance amplio al interior de una organización y debe estar directamente relacionado con la alta dirección, de manera estratégica.

- *Las obligaciones objeto de comparación por parte del auditor distan en su alcance y especificidad, pero concuerdan en el objetivo de buscar niveles apropiados de seguridad de la información en la entidad.*
- *La seguridad de la información es un proyecto que requiere una alta apropiación de recursos humanos, técnicos y financieros.*
- *Los objetos contractuales del recurso humano cuestionado por la ACI, definen su alcance al PGSIRT, con impacto transversal a la entidad, a diferencia del rol de Oficial de Seguridad de la Información que cubre las necesidades generales de la entidad."*

La Auditoría efectúa el análisis de los comentarios del auditado así:

Respecto de la parte introductoria de la observación y Numeral 1:

Se aclara que la observación *VULNERABILIDADES PARA SEGURIDAD DE LA INFORMACIÓN POR LIMITANTE DEL ALCANCE ENFOCADO A SEGURIDAD DIGITAL,* hace referencia que el IPES se encontraba con una brecha entre seguridad de la información y seguridad digital, como indica la Guía Metodológica de Pruebas de Efectividad, Guía No.1. En *"8 ALCANCE, La metodología busca desde el primer momento* ***de la ejecución, crear una línea base del estado de seguridad de la entidad, es decir,***

facilitar la identificación de la brecha en la implementación del modelo de seguridad, entiéndase como línea base la primera medición; *las siguientes mediciones darán a la entidad la percepción de seguridad que manifiestan en la implementación del modelo de seguridad"* , es deber del IPES identificar las necesidades para desarrollar un SGSI que se integre al SGI.

Si bien la entidad cuenta con el PR-123 PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN; IN-069 INSTRUCTIVO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN; FO-625 DOCUMENTACIÓN DE INCIDENTES; FO-626 LECCIONES APRENDIDAS RESPUESTA A INCIDENTES, éstos se han limitado a la seguridad digital creando una brecha entre el área de Seguridad de la Información y Recursos tecnológicos.

Respecto del numeral 2 literal a: Se reitera, como se indicó en la observación No.1, que tal como indica la Guía Metodológica de Pruebas de Efectividad, Guía No.1. En *"8 ALCANCE, La metodología busca desde el primer momento* ***de la ejecución, crear una línea base del estado de seguridad de la entidad, es decir, facilitar la identificación de la brecha en la implementación del modelo de seguridad, entiéndase como línea base la primera medición****; las siguientes mediciones darán a la entidad la percepción de seguridad que manifiestan en la implementación del modelo de seguridad"* , por lo anterior, es deber del IPES identificar las necesidades para desarrollar un SGSI que se integre al SGI.

Respecto del literal b: El PR-123 GESTION DE INCIDENTES DE SEGURIDAD V3 se orienta únicamente a la parte tecnológica, se evidencio como se debía actuar en casos de incidentes que no correspondan a infraestructura tecnológica y como sería el plan de comunicaciones para el interior del IPES; medios de comunicación y diferentes interesados.

Respecto del numeral 3: No se evidenció en el SIG la existencia del Procedimiento de Manejo de Información Forense y el Instructivo de Manejo de Información Forense y tampoco fue suministrado en la réplica.

Respecto del numeral 4: No se suministró evidencia de que el comité de comité de sistemas y seguridad de la información estuviera cubriendo sus funciones y sus mesas de trabajo.

El auditado indica: "*Como se aprecia en la conclusión de la auditoría, no se podía adelantar la contratación de un recurso humano, para cumplir con unas obligaciones específicas, si se cuenta con el Oficial de Seguridad de la Información",* hubo un contratista para realizar actividades de oficial de seguridad y al mismo tiempo de planta existe un designado como seguridad de la información como se evidenció en el acta del 13-mar-2018.

El rol de Oficial de Seguridad de la Información debe contar con un alcance amplio al interior de una organización y debe estar directamente relacionado con la alta dirección, de manera estratégica. En los compromisos funcionales del profesional universitario de la SDAE

designado para este rol, no fue posible establecer las actividades adelantadas en el marco de un SGSI, en el mismo sentido, la SDAE contrató desde 2018 hasta la fecha, a un profesional con asignación de obligaciones contractuales que desarrollan el rol de Oficial de Seguridad e la Información, que desarrolla las funciones asignadas a un profesional nombrado en carrera administrativa en el IPES. Es evidente la deficiencia de gobierno del SGSI, debido a que no se observó la ejecución de esta responsabilidad con la autoridad e independencia requeridas con relacionamiento directo con el más alto nivel de la Dirección y reporte periódico al Comité de Sistemas ni por el profesional designado, ni por el profesional contratado, ni por la SDAE, de acuerdo a lo confirmado por el mismo auditado en sus comentarios de réplica.

En mérito de lo expuesto, el hallazgo se mantiene.

Riesgo Asociado: Implementación inadecuada de las políticas públicas de Seguridad Digital: Aspectos como el desconocimiento o aplicación inadecuada de las políticas de seguridad de la información, al igual que la falta o desactualización de la documentación relacionada con la operación informática de la Entidad, pueden conllevar Implementación inadecuada de las políticas públicas de transparencia de la información y de protección de datos.

Normatividad o Criterio:

1. Falta cobertura transversal del enfoque del SGSI

Manual MS-013 Manual de Seguridad de la Información. 12.8. Política de Gestión de Incidentes de Seguridad de la Información: Objetivo. *Proteger la integridad, disponibilidad y confidencialidad de los activos de información de la entidad, prevenir la perdida de servicios y cumplir con requerimientos legales. Esta política establece los mecanismos de coordinación para dar respuesta a los incidentes de seguridad y habilita a la entidad para una remediación rápida, recopilación de datos y reporte de los eventos que afectan la infraestructura de información y tecnología.*

ISO 27001:2013: A.5.1.2. Revisión de las políticas para seguridad de la información: *Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas. // A.16.1.1* **Responsabilidad y procedimientos**: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. // A.16.1.3. **Reporte de debilidades de seguridad de la información:** Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

Glosario de ITIL/ITSM:
Disponibilidad:

- Meta: Garantizar que los niveles de disponibilidad que se entreguen en todos los servicios cumplen o superan las necesidades actuales y futuras acordadas con el negocio, de manera eficiente en costos.

Objetivos:

- Crear y Mantener un plan actualizado de disponibilidad (AP) que refleje las necesidades presentes y futuras
- Brindar asesoría en asuntos relacionados con la disponibilidad
- Garantizar la disponibilidad de los Servicios con base a lo esperado por el negocio
- Evaluar el impacto de los cambios referentes al Plan de Disponibilidad
- Garantizar la adopción de medidas proactivas para mejorar la disponibilidad de servicios.

2. Ineficiente gestión de incidentes de seguridad de la información

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.*

ISO 27001:2013: A.5.1.2. Revisión de las políticas para seguridad de la información: *Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas. //* **A.16.1.1 Responsabilidad y procedimientos**: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. // **A.16.1.3. Reporte de debilidades de seguridad de la información:** Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

3. Falta procedimiento de manejo de información forense

MS-013 MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 14 LEVANTAMIENTO DE INFORMACIÓN FORENSE: *La entidad establece, a través del procedimiento los lineamientos para contar con capacidades para realizar análisis de información forense para poder determinar que incidentes han ocurrido sobre los sistemas de información y servicios, así como orientar en el manejo de la evidencia forense digital y su integración con la gestión de incidentes de seguridad de la información. Se ha definido el siguiente procedimiento e instructivo:*

- *Procedimiento de Manejo de Información Forense.*
- *Instructivo de Manejo de Información Forense.*

ISO 27001:2013: A.5.1.2. Revisión de las políticas para seguridad de la información: *Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.*

4. Incumplimiento de funciones asignadas al Comité de Sistemas y Seguridad de la Información

Matriz de Riesgos y Controles: *Los profesionales de Sistemas realizan mínimo una vez al año y de acuerdo a las necesidades operativas y normativas, los cambios y ajustes a las políticas que hacen parte del proceso "SEGURIDAD INFORMACIÓN Y RECURSOS TECNOLÓGICOS", teniendo como referencia el marco normativo de las políticas públicas del sector de las TIC y los lineamientos distritales y Nacionales.*

Resolución N° 615 de 2013, por la cual se crea el Comité de Sistemas y Seguridad de la Información en el IPES: Artículo 4. Funciones del comité:

1. *Aprobar el plan estratégico de tecnologías de la información y las comunicaciones.*
2. *Definir políticas de desarrollo y seguridad de la información.*
3. *Establecer acciones que mitiguen riesgos de perdida que comprometan los recursos de información.*
4. *Fijar acciones específicas que ayuden a proveer un ambiente seguro y estable de recursos de información, que sea consistente con las metas, políticas y objetivos del instituto para la Economía Social – IPES.*
5. *Garantizar que se promueva los recursos humanos, técnicos y financieros, para asegurar que la información del instituto se encuentre protegida apropiadamente sobre los presupuestos de la confidencialidad y de los recursos informáticos y físicos que lo soportan.*
6. *Impulsar la implementación del sistema de gestión de seguridad de la información - SGSI.*
7. *Revisar Diagnostico del estado de la seguridad de la entidad.*
8. *Evaluar los requerimientos tecnológicos en materia de TIC's.*
9. *Definir roles y responsabilidades que se relacionen con la seguridad de la información.*
10. *Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.*
11. *Establecer las estrategias para la divulgación y comunicación de las políticas y normas que el IPES, dicte en materia de seguridad de la información.*
12. *Las demás funciones inherentes a la naturaleza del Comité.*

Artículo 5. funciones de la secretaria técnica:

1. *Convocar a las reuniones ordinarias y extraordinarias del comité, como mínimo con tres (3) días de antelación.*
2. *Elaborar la agenda de los temas a tratar en la reunión para que se coloquen a consideración del comité para su respectivo estudio y aprobación.*

3. *Elaborar actas producto de las reuniones de cada comité los cinco (5) días siguientes de la realización para su respectiva aprobación.*
4. *Preparar los informes que le sean solicitados.*
5. *Los demás que le asigne el comité.*

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.*

Ley 1753 de 2015, ARTÍCULO 45. Estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano. Director de Tecnologías y Sistemas de Información: *b) Director de Tecnologías y Sistemas de Información. Las entidades estatales tendrán un Director de Tecnologías y Sistemas de Información responsable de ejecutar los planes, programas y proyectos de tecnologías y sistemas de información en la respectiva entidad. Para tales efectos, cada entidad pública efectuará los ajustes necesarios en sus estructuras organizacionales, de acuerdo con sus disponibilidades presupuestales, sin incrementar los gastos de personal. El Director de Tecnologías y Sistemas de Información reportará directamente al representante legal de la entidad a la que pertenezca y se acogerá a los lineamientos que en materia de TI defina el MinTIC.*

MS-MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 8.2 Oficial de Seguridad de la Información: *El comité de sistemas y seguridad de la información, designará al oficial de seguridad de la información, el cual tiene como obligaciones principales:*
- Liderar el diseño de políticas, directrices y lineamientos encaminados a fortalecer la seguridad de la información.
- Identificar el grado de madurez en la implementación del Modelo de seguridad y privacidad de la información en la entidad.
- Socializar ante el comité de sistemas y seguridad de la información, los incidentes de seguridad de la información presentados, así como las acciones tomadas para reducir su impacto.
- Coordinar las actividades correspondientes a la gestión de incidentes de seguridad, con la finalidad de contar con un enfoque estructurado y planificado que permita manejar adecuadamente los incidentes de seguridad de la información.
- Establecer estrategias de defensa proactivas y reactivas.
- Consolidar los procedimientos de seguridad informática y someterlos a decisión del comité de sistemas y seguridad de la información.
- Desarrollar, mantener y comunicar las políticas, estándares y guías de seguridad de la información, especialmente, aquellas con un enfoque tecnológico.
- Coordinador el análisis de riesgos de seguridad de la información y coordinar el plan para la mitigación de los mismos.
- Elaborar o coordinar campañas de sensibilización.
- Realizar capacitación y socialización del SGSI.
El rol de Oficial de Seguridad de la Información, será asumido por el/la subdirector (a) de Diseño y Análisis Estratégico, hasta tanto el comité haga oficial la designación del responsable a través de los medios dispuestos por la entidad.

FORTALECIMIENTO DE LA GESTIÓN TI EN EL ESTADO[9]

PERFIL: *¿Cómo deben ser los CIO colombianos? ¿Qué competencias y habilidades deben desarrollar? ¿A qué se enfrentan los CIO en Colombia, cuáles son sus retos? La Estrategia TI define cinco competencias, ocho habilidades y cinco retos que deben satisfacer como mínimo los CIO públicos del país:*

1.1. **Competencias**

Se enmarcan en 5 áreas de conocimiento:

1. *Conocimiento y experiencia en TI: que desarrollan por medio de la educación formal y continua en TI y la práctica laboral en gerencia de proyectos de tecnología.*
2. *Sector público:*
   a) *Deben conocer el valor de lo público*
   b) *Procedimientos del gobierno*
   c) *Deben tener orientación al servicio al ciudadano*
   d) *Deben conocer los procedimientos de la contratación pública*
3. *Capacidad gerencial:*
   a) *Experiencia en gerencia de proyectos de TI*
   b) *Pensamiento estratégico*
   c) *Liderazgo*
   d) *Gestión de riesgos*
   e) *Manejo de las partes interesadas o afectadas (stakeholders)*
   f) *Control y seguimiento*
   g) *Trabajo en equipo*
   h) *Gestión del cambio*
4. *De cada sector: deben tener conocimiento y experiencia de los procesos y la misión de su sector: salud, educación, vivienda, finanzas, etc.*
5. *Innovación: capacidad para incorporar tendencias o estrategias tecnológicas innovadoras que tengan impacto en el desarrollo de su sector.*

1.2. **Habilidades**

1. *Entendimiento: capacidad de entender y estar al día con las nuevas tendencias tecnológicas.*
2. *Análisis: análisis de diferentes aproximaciones y enfoques de TIC y su impacto en la organización.*
3. *Decisión: justificar y tomar decisiones de TI y sobre su impacto actual y futuro para la organización.*
4. *Liderazgo: capacidad de introducir innovaciones e iniciativas de TI en la organización, de administrar los resultados del cambio y de dirigir los equipos.*
5. *Negociación: relacionarse con otros actores para establecer alianzas, acuerdos y para fijar prioridades en pro de objetivos comunes.*
6. *Solución de problemas: entender y diagnosticar problemáticas y trazas soluciones.*
7. *Comunicación: capacidad para transmitir las ideas y de interactuar con actores de diferentes disciplinas en un lenguaje no técnico, para lograr objetivos comunes.*

[9] https://www.mintic.gov.co/gestion-ti/CIO/Perfil/

8. *Trabajo en equipo: capacidad para articular esfuerzos con otras personas, dentro y fuera de la entidad.*

1.3. **Retos**

1. *La información como valor estratégico:*
   a) *Deficiencias en gestión de proyectos y duplicidad de esfuerzos y recursos.*
   b) *No hay cadenas de valor concebidas.*
   c) *Inconsistencias y baja percepción de la calidad.*
   d) *No hay voluntad para compartir e intercambiar información.*
   e) *Problemas de seguridad y privacidad.*
2. *Gestión de información y servicios en línea:*
   a) *No todas las entidades han habilitado trámites y servicios en línea.*
   b) *La oferta de datos abiertos o información libre aún es limitada.*
   c) *La gestión pública debe ser POR el ciudadano, PARA el ciudadano y CON el ciudadano.*
3. *Gestión de tecnología como agente transformador:*
   a) *Carencia de planes.*
   b) *Fallas en coordinación de soluciones y desarrollos.*
   c) *Baja e incorrecta percepción sobre las oficinas de TI.*
   d) *Pérdida de tiempo en los procesos de contratación.*
   e) *Baja capacidad de negociación.*
   f) *Rezago de las innovaciones.*
   g) *Falta una concepción de servicio.*
4. *Liderazgo de los CIO:*
   a) *Deficiente capacitación.*
   b) *Bajo bilingüismo.*
   c) *Bajo conocimiento especializado.*
   d) *Existe el talento, pero no hay estrategas tecnológicos.*
   e) *Falta trabajar en Investigación + Desarrollo + Innovación.*
   f) *Se debe generar confianza y legitimidad sobre la tecnología.*
5. *Arquitectura Organizacional:*
   a) *Frente a la estructura organizacional, por la disparidad de ubicaciones dentro de la estructura de cada entidad.*
   b) *Frente al talento humano, se concentran en temas operativos y de soporte técnico, las discrepancias salariales son altas y no hay oportunidades para desarrollar competencias.*

ISO 27001:2013: A.5.1.2. Revisión de las políticas para seguridad de la información: *Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.*

Lista Índices de Gestión y Desempeño, Política 14: Gestión Documental: <u>Componente administración de archivos</u>: *Mide la capacidad de la entidad pública de implementar un conjunto de estrategias dirigidas a la planeación, dirección y control de los recursos físicos, técnicos, tecnológicos, financieros y del talento humano, necesarios para*

la realización de los procesos de la gestión documental y el eficiente funcionamiento de los archivos. // **Componente tecnológico:** *Mide la capacidad de la entidad pública de implementar actividades para la administración electrónica de documentos, la seguridad de la información y la interoperabilidad en cumplimiento de las políticas y lineamientos de la gestión documental y administración de archivos.*

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, 2018).
- Identificar las brechas del MS-013 MANUAL SEGURIDAD DE LA INFORMACIÓN vs la norma ISO 27001:2013
- Definir el *MS-013 MANUAL SEGURIDAD DE LA INFORMACIÓN* con un alcance orientado a la seguridad de la información y no limitarlo a la seguridad digital.
- Definir los controles de seguridad de la información de manera transversal en toda el Instituto con el fin de que cubra todas las necesidades, asociados a la identificación de riesgos y las medidas para su mitigación.
- Definir la seguridad de la información como un proceso estratégico independiente de los demás subdirecciones del IPES.
- Generar una metodología para la gestión de incidentes de seguridad de la información que sea transversal a todo el Instituto Para La Economía Social – IPES.
- Definir una directriz para el Manejo de Información Forense y el Instructivo de Manejo de Información Forense para ser activado cuando se requiera.
- Nombrar un Oficial de Seguridad de la Información en propiedad como responsable que cumpla las funciones asignadas a este rol y reporte de manera directa a la Alta Dirección, con total independencia a todos los procesos del Instituto Para La Economía Social – IPES.
- Garantizar desde la Secretaría Técnica del comité, las funciones del comité de seguridad de la información, al igual que el seguimiento a los reportes periódicos del cumplimiento de las funciones del Oficial de Seguridad, quien debe velar la mejora continua, el monitoreo de controles y el cumplimiento de un esquema de seguridad de la información transversal al Instituto Para La Economía Social - IPES.

Connotación: Administrativa y con posible connotación disciplinaria en lo relacionado con los numerales 4 y 5.

N° 3:

DEFICIENCIAS EN LA GESTIÓN DE LOS ACTIVOS DE LA INFORMACIÓN

Responsable de las acciones de mejora: SDAE

En la revisión efectuada sobre los diferentes documentos que dan cuenta de la gestión de: 1) riesgos de seguridad digital, 2) controles a la gestión de comunicaciones y operaciones,

3) capacidad y 4) controles de seguridad física, no se obtuvo evidencia respecto a las siguientes actividades de control:

- Definición de un procedimiento para la identificación y valoración de Activos de la entidad.
- Seguimiento a los planes de tratamiento de riesgo definidos.
- Informe a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital de la entidad.
- Definición de políticas o procedimientos relacionados con los procesos de monitoreo encaminados a brindar seguridad física de los Recursos Tecnológicos (Servidores, equipos de Red, equipos de Cómputo)
- Identificación de los mecanismos de seguridad, así como los niveles de servicio y los requisitos de gestión de todos los servicios de red de la entidad.
- Análisis de la capacidad y el desempeño de la Infraestructura Tecnológica para satisfacer las necesidades actuales y futuras de la entidad.
- Evaluación de la optimización del rendimiento de la red, la disponibilidad de recursos, la optimización y aumento del almacenamiento periódicamente.
- Existencia de actas o informes de actividades de medición que permitan realizar proyecciones de los requisitos sobre la capacidad futura.

1. *Deficiencia en la identificación y valorización de los activos de información*

Se evidenció que la valoración de activos de la entidad se realizó a nivel cuantitativo basado en el valor comercial del bien, sin tener en cuenta el valor cualitativo de la información.

Se evidenció que la valoración de activos de la entidad se realizó a nivel cuantitativo basado en el valor comercial del bien, sin tener en cuenta el valor cualitativo de la información.

Lo anterior sustentado en lo siguiente:

a. La ISO 27001:2013, establece en su control "A.*8.1.1. Inventario de activos: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos; A.8.2.1 clasificación de la información: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada"*.

b. La Guía Para la Administración del Riesgo y el Diseño de controles en entidades públicas del DAFP, establece en el numeral "2.1.5 Identificación de activos de seguridad de la información: Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, **información física o digital**, tecnologías de información -TI, tecnologías de operación TO".

c. La ISO 27001:2013, establece en su control "*A.8.2.1 clasificación de la información: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.*"

d. La Guía Para la Administración del Riesgo y el Diseño de controles en entidades públicas del DAFP, establece:" **"¿Qué es tratamiento del riesgo?** Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo **cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio** de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo."

e. Guía para la Gestión y Clasificación de Activos de Información – guía 5- MINTIC, establece:

> "***6.1. DEFINICIÓN:*** *La definición consiste en determinar qué* ***activos de información van a hacer parte del inventario****, para esta tarea debe existir un equipo que realice la gestión de activos de información al interior de la entidad y por medio del líder del cada proceso (o quien haga sus veces. Líder requerido en gestión de calidad) ayude en realización de la actividad. En segunda instancia los líderes de procesos deben, solicitar la revisión de la definición de los activos por parte del propietario del activo de información designado, custodio y usuario del mismo, para que validen si son las partes interesadas o la parte de la entidad adecuadas para tener este rol. Es recomendable que la definición del inventario se lleve a cabo por lo menos una vez al año.*
>
> *<u>Información básica:</u> La información básica hace referencia a aquellas características del activo y para realizar la etapa de definición podría incluir como mínimo la siguiente:*
> - *Identificador: Número consecutivo único que identifica al activo en el inventario.*
> - *Proceso: Nombre del proceso al que pertenece el activo.*
> - *Nombre Activo: Nombre de identificación del activo dentro del proceso al que pertenece.*
> - *Descripción/Observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.*
> - *Tipo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:*
> - *Información: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de*

soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.

- *Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.*
- *Recurso humano: Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información. o Servicio: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.*
- *Hardware: Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.*
- *Otros: activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso*

Ubicación: Describe la ubicación tanto física como electrónica del activo de información.
Clasificación: Hace referencia a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad.
Justificación: Para cada valoración, describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad), o el argumento del porque se asignó dicha valoración.
Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información:

- *Alta. Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.*
- *Media. Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio.*
- *Baja. Activos de información en los cuales la clasificación de la información en todos sus niveles es baja."*

Por lo tanto, de la lectura de las normas y guías señaladas, se establece la necesidad por parte de las entidades de valorar la información, pues la misma, desde la visión de la Seguridad de la información es un ACTIVO, por lo tanto no es suficiente la valoración comercial del repositorio y de los elementos lógicos donde reposa la información sino también darle un valor a la misma como a cualquier activo, con lo cual la entidad puede establecer con mayor exactitud y eficiencia estrategias para definir los controles a implementar para la protección de dicha información y la inversión que se debería realizar para tal fin, situación que en este momento la entidad no tiene establecida en ninguno de sus manuales y procedimientos.

2. *Falta definición de políticas o procedimientos relacionados con los procesos de monitoreo para la seguridad física*

Los profesional de la SDAE han omitido el apoyo requerido para la seguridad física en el IPES, en el *PO-013 CARACTERIZACIÓN PROCESOS, GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS y* en la GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS se omitió la caracterización *"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" para dar el apoyo respectivo al control de acceso a las diferentes áreas correspondientes a la entidad y se pudiera orientar el IPES a un SGSI (Sistema de Gestión de Seguridad de la Información); se observó el apoyo que se debió brindar a nivel administrativo para el acceso físico de la entidad y no limitar las funciones a dar soporte a los sistemas de acceso ya establecidos, era importante ir a un modelo de defensa que cubra la organización para madurar el SGSI y no limitarse al alcance de seguridad digital.

MICROSOFT en su modelo de defensa, proporciona un alcance con claridad para modelar la seguridad de la información por medio de capas, como un concepto valido aplicable a cualquier organización:

- Nivel de directivas, procedimientos y concienciación: programas educativos de seguridad para los usuarios
- Nivel de seguridad física: guardias de seguridad, bloqueos y dispositivos de seguimiento
- Nivel perimetral: servidores de seguridad de hardware, software o ambos, y creación de redes privadas virtuales con procedimientos de cuarentena
- Nivel de red de Internet: segmentación de red, Seguridad IP (IPSec) y sistemas de detección de intrusos de red
- Nivel de host: prácticas destinadas a reforzar los servidores y clientes, herramientas de administración de revisiones, métodos seguros de autenticación y sistemas de detección de intrusos basados en hosts.
- Nivel de aplicación: prácticas destinadas a reforzar las aplicaciones y el software antivirus
- Nivel de datos: listas de control de acceso (ACL) y cifrado.[10]

3. *Debilidades de control de acceso los sistemas de información*

Cuando se realizó recorrido verificando el acceso de los usuarios:

- reortizg
- vmartinezo
- mcperream
- mlbenjumeap
- nmontealegrec
- larodriguez
- saguzmano
- dsjimenezm
- basuarezp
- jhrojasc
- girinconb

[10] Modelo de defensa de Microsoft.

- cavalenciac
- nkmachadon
- ymartinezl

El usuario *dsjimenezm* se encontraba siendo usado por el usuario Nancy Gutiérrez, porque no se le había asignado usuario para iniciar sus labores.

Respecto al control *A18.1.2 Derechos de propiedad intelectual,* se evidenció en el Microsoft Volume Lincensing Service Center Suministrado, que solo se tenía 210 CAL afectando el licenciamiento de los usuarios que pueden estar conectado de forma simultánea. Se tienen aproximadamente 400 usuarios en la Entidad.

Imagen 2. *Microsoft Licensing Service Center*

4. *Deficiencia en la organización de los recursos tecnológicos*

Durante un recorrido en el DATACENTER del IPES realizado el 07-sep-2020 se observó que los racks no se encontraban debidamente peinados (organizado el cableado), se evidenció cables cruzados con un monitor y elementos que pueden producir incidentes de tipos operativos, de seguridad y salud en el trabajo, materiales inflamables, como se observa en el siguiente registro fotográfico de ese día:

Imagen 3. Condiciones Datacenter – Visita de auditoría 07-sep-2020

Al realizar visita al punto comercial de Kennedy y la plaza de mercado la Perseverancia el 28-sep-2020 se evidenciaron las siguientes deficiencias:

El punto Vive Digital de Kennedy:

Existencia de cableado sin canaleta y en mal estado, generando riesgos tanto de seguridad para los transeúntes, como posibles riesgos eléctricos:

Imagen 4. Condiciones Cableado – Punto Vive Digital Kennedy

En la Plaza de Mercado de la Perseverancia: dentro de la Oficina Administrativa, el punto de Datos presentaba existencia de cableado sin peinar, lo que puede generar un riesgo operativo para dificultar la atención del soporte en el momento en que se requiera:

Imagen 5. Condiciones Cableado – PDM La Perseverancia

5. *Deficiencias en el aseguramiento de la capacidad, desempeño y optimización de la infraestructura tecnológica*

Para asegurar el funcionamiento de la infraestructura tecnológica no se realizan pruebas de control de acceso no autorizado a los sistemas que componen la seguridad digital y para evitar la aparición de bugs (defectos), vulnerabilidades o brechas de seguridad en aplicaciones en producción, el IPES, se realizaban pruebas anuales de seguridad de Etical Hacking, análisis de vulnerabilidades y/o pruebas de penetración, y otros tipos de pruebas como la ingeniería social.

MINTIC promueve la guía 8 que define CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN/ bajo la ISO 27001:2013, en donde definen su aplicabilidad para entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de TI en el marco de la Estrategia de Gobierno en Línea.

6. *Falta de proyección en la optimización del rendimiento de la red, la disponibilidad de recursos, la optimización y aumento del almacenamiento periódicamente*

El DE-047 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES indicaban que se tenía planeado orientar al cumplimiento de un Sistema Integrado de Seguridad de la Información (SGSI), lo cual va en contradicción del MS-013 MANUAL DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, el cual era limitado al alcance de seguridad digital. El PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN se definirá durante la fase II en donde se evaluará GOBIERNO TIC bajo el marco de COBIT.

MINTIC promueve la guía 8 que define CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN/SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN bajo la ISO 27001, en donde definen su aplicabilidad para e*ntidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de TI en el marco de la Estrategia de Gobierno en Línea.*

Ver comparativo Matriz de Aplicabilidad vs ISO 27001:2013, **ANEXO 10.**

7. *Falta de información de actividades de medición que permitan realizar proyecciones de la estrategia TIC y SISG*

La mejora continua requiere de un monitoreo de los activos de infraestructura tecnológica para definir planes de disponibilidad y crecimiento para realizar proyectos que agreguen valor conociendo el retorno de inversión.

Aunque procedimientos, instructivos y evidencias sobre la realización de acciones preventivas de un monitoreo y/o mantenimiento, no se identificó la realización de pruebas

de que se encontraran de manera correcta para el caso de tener que cubrir una contingencia.

Se logró identificar accesos no autorizados a los sistemas de información y manipulación indebida de información de los mismos, en donde un usuario estaba ingresando a los equipos de cómputo con las credenciales de otro compañero debido a que no le habían suministrado su autenticación; al verificar el acceso de autenticación con las CAL del directorio activo (Como se detalla en el **ANEXO 11**) existe menos licencias de la cantidad de usuarios activos en el sistema (cuando no se encontraban el planeta en emergencia sanitaria si alcanzaba a superar la cantidad de usuarios autenticados).

Se presenta manejo inapropiado de las plataformas tecnológicas, sistemas y servicios informáticos por parte de los colaboradores, en cuanto la gestión de capacidad y disponibilidad. El no definir la gestión capacidad y disponibilidad puede originar sanciones administrativas y disciplinarias según la responsabilidad y las acciones de la operación de los recursos.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR-123 GESTION DE INCIDENTES DE SEGURIDAD, presentaron el siguiente Diseño de Control:

Control 1: Matriz de Riesgos y Controles: Los profesionales de sistemas realizan seguimiento trimestral a la implementación de los controles de seguridad informática a los que se refiere la norma ISO 27001 y el Modelo de Seguridad y Privacidad de la Información -MSPI-.

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 y una gestión transversal a toda la organización.

Control 2: 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 6. Seguridad Física y del Entorno: A.11.1.1 Perímetro de seguridad física // A.11.1.2 Controles físicos de entrada // Actividad 1: Controles de Acceso a áreas seguras. Verificar controles de Acceso a áreas seguras, las cuales deben estar protegidas para asegurar que solo se permite el acceso a personal autorizado

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 prioridad que se encontraba en actualización para el año 2020, pero no es claro con

qué frecuencia se va a ejecutar, en el manejo de las excepciones no se especifica cómo se va a desarrollar esta estrategia, y en el manejo de la evidencia no se encontraron evidencias. Para poder definir la capacidad, desempeño y optimización de la infraestructura tecnológica es importante poder realizar pruebas que apoyen a realizar pruebas de control de acceso no autorizado a los sistemas de información y descubrir y evitar la aparición de bugs (defectos), vulnerabilidades o brechas de seguridad en aplicaciones en producción, el IPES no se realizaban pruebas periódicas de seguridad de Etical Hacking, análisis de vulnerabilidades y/o pruebas de penetración, y otros tipos de pruebas como la ingeniería social, además para la estrategia de control de acceso y la cultura corporativa en temas de seguridad de la información, además definir los recursos de control de acceso ya que las CAL del directorio activo superan a la cantidad de usuarios registrados activos.

Control 3: 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 8. Control de Acceso: A.9.2.2 Suministro de acceso de usuarios // Actividad 2: Controles de Acceso a medios de procesamiento.
Acceso a medios de procesamiento de información, los usuarios solo deben tener acceso a los medios para cuyo uso están específicamente autorizados.

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 las excepciones no se están diligenciando debidamente los formatos de solicitud.

Control 4: 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 11. Gestión de la Continuidad del Negocio: A.17.2.1 Disponibilidad de instalaciones de procesamiento de información. // Actividad 3: Desarrollo de Estrategias. Desarrollo de las Estrategias para garantizar la continuidad de las actividades de negocio. // Actividad 5: Prueba y Aprobación. Prueba y aprobación del Plan de Continuidad de Negocio.

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 del propósito se plantea una fecha prevista para el primer trimestre de 2020, el cual no se tiene evidencia de su cumplimiento, en el procedimiento y la evidencia el control se apoya en el DE-039 el cual se encuentra obsoleto.

Valoración comentarios del Auditado

El auditado argumenta que:

> *"Como se evidencia en la presente observación, no fueron tenidas en cuenta las aclaraciones producto de la sesión de socialización del pasado 9 de octubre de 2020, lo cual deriva en el presente proceso de explicación, actividad repetitiva en la presente auditoría en donde se hizo necesario ilustrar en todos los aspectos al equipo auditor, sin alcanzar el resultado esperado.*

- *Se explicó en medio de la auditoría la razón de ser de los instrumentos FO-699, FO362, IN-085 e Índice de Información clasificada y reservada publicados en la página web de la entidad. El instructivo para la clasificación de activos de información muestra el procedimiento para clasificar los activos de información, atendiendo lineamientos del Lineamiento 11 de la Norma Técnica Distrital de Calidad. Dentro de la sesión de socialización, la ACI hace una reflexión sobre la necesidad de asignar un valor económico a la información creada, procesada y almacenada en la entidad, bajo una norma o lineamiento que no pudo ser explicada, probablemente al tratarse de una afirmación errónea. La valoración de activos de información obedece a un análisis de impacto y criticidad de la información.*
- *El PGSIRT suministro en la presente auditoría la matriz de riesgos que incluye el plan de tratamiento de riesgos. Así mismo, esta información reposa en la página web del Instituto. por otra parte se socializo y entregó el DE-038 Plan de tratamiento de riesgos de seguridad y privacidad de la información.*
- *"Informe a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital de la entidad", no es claro el incumplimiento. Un informe debería partir de un cambio significativo.*
- *No todos los controles de ISO 27001 e ISO 27002, son susceptibles de elevar a Procedimiento o Política, precisamente para eso existe la declaración de aplicabilidad, complementado con roles y responsabilidades. El PGSIRT cuenta adicionalmente con contratos con terceros para el mantenimiento y soporte de las tecnologías de información y comunicaciones. Característica informada también a la ACI.*
- *Existen tareas propias de la administración, mantenimiento y monitoreo de los activos de infraestructura tecnológica, que pueden ser evidenciados en consolas de administración de los mismos activos y que dan los insumos para la toma de decisiones a partir de la gestión de la capacidad y rendimiento. "*

  "No se pueden mezclar particularidades asociadas a los activos de información. La elaboración de un inventario de activos de información busca definir controles que garanticen su aseguramiento en términos de disponibilidad, diferente de la tarea propia de los procesos de recursos físicos para el tratamiento de bienes muebles e inmuebles en una organización. Sin embargo y como se aclaró en sesión de socialización del 9 de octubre, que la entidad realiza proceso de valorización de activos en términos de dinero, para el establecimiento de pólizas a través de los procesos administrativos y financieros."

  "Se contemplan los riesgos de seguridad sobre los activos de IT en el mapa de procesos (MR-013)

  Se socializó con la ACI el FO-699 Inventario de activos de información tipo software, hardware y servicios."

  "Se explicó al auditor la razón de ser de los instrumentos FO-699, FO-362, IN-085 e Índice de Información clasificada y reservada publicados en la página web de la entidad. El instructivo para la clasificación de activos de información muestra el procedimiento para clasificar los activos de información, atendiendo lineamientos del Lineamiento 11 de la Norma Técnica Distrital de Calidad. Dentro de la sesión de socialización, la ACI hace una reflexión sobre la necesidad de asignar un valor económico a la información creada, procesada y almacenada en la entidad, bajo una norma o lineamiento que no pudo ser citado, probablemente al tratarse de una afirmación errónea. La valoración de activos de información obedece a un análisis de impacto y criticidad de la información."

  "Se contemplan los riesgos de seguridad sobre los activos de IT en el mapa de procesos (MR013), en cumplimiento de la política de Administración del Riesgo del IPES, la cual se encuentra alineada y en concordancia con el DAFP."

  "En desarrollo de la sesión de socialización del 9 de octubre, el PGSIRT explicó al auditor la razón de ser de los instrumentos FO-699, FO-362, IN-085 e Índice de Información clasificada y reservada publicados en la página web de la entidad. El instructivo para la clasificación de activos de información muestra el procedimiento para clasificar los activos de información, atendiendo lineamientos del Lineamiento 11 de la Norma Técnica Distrital de Calidad.

El índice de información clasificada y reservada cuenta con las variables asociadas a los activos y requeridas por normatividad. De igual manera el FO-699, resume las características de los activos tipo software hardware y servicios."

"Bajo la estructura de un Sistema Integrado de Gestión y la operación de la entidad basada en procesos, no se puede hablar de una omisión en la socialización y operación de controles de seguridad de la información. El PGSIRT participa activamente en mesas de trabajo en las cuales se adoptan medidas como la seguridad física y realiza los conceptos requeridos frente a necesidades específicas. Los anteriormente conocidos Subsistemas, interrelacionan entre sí para definir requerimientos institucionales, en el marco del Modelo de Planeación y Gestión MIPG.

El SGSI contempla roles y responsabilidades en diferentes niveles de la entidad, es así como la operación de controles físicos de acceso a áreas seguridad, corresponde a la operación administrativa, o la gestión de bienes a los procesos de recursos físicos, sin esto desligarse de un modelo basado en procesos."

De acuerdo al Formato FO-325 Entrega de credenciales a usuario, las condiciones de uso las cuales acepta el usuario al recibir los servicios se estipula " Una vez recibidos los recursos y/o servicios informáticos el usuario se compromete a: Conocer y dar cumplimiento a las políticas de seguridad de la información, lineamientos, procedimientos, protocolos y demás instrumentos establecidos por la entidad, para preservar la confidencialidad, integridad y disponibilidad de la información institucional. Cooperar con los esfuerzos de la entidad para proteger la información. Actualizarse en temas relacionados con la seguridad de la información, seguridad informática y seguridad digital. Consultar con el responsable del Subsistema de Seguridad de la Información de la Entidad, en caso de duda o desconocimiento de un procedimiento formal, ya que el desconocimiento normativo no exonera de la aplicación de una acción disciplinaria frente a posibles violaciones a las políticas de seguridad de la información. Dar uso adecuado de los recursos asignados (equipos de cómputo, impresoras, software, entre otros) y/o servicios informáticos (cuentas de usuario, recursos compartidos, correo electrónico institucional, datos e información, sistemas de información, entre otros) de acuerdo con las normas y procedimientos establecidos por la Entidad. Proteger y no transferir el usuario y la contraseña asignada por la Entidad a otra persona o funcionario, ni utilizar otra cuenta de usuario para el ingreso a los recursos de la Entidad. Responder por todas las operaciones efectuadas y la información registrada con la cuenta de usuario. Cualquier incumplimiento en los compromisos relacionados previamente, será reportado como un incidente de seguridad de la información de acuerdo con el procedimiento definido por la entidad, para cuya atención deberá convocarse, como parte del equipo de respuesta, a la Oficina de Control Interno Disciplinario, quien indicará las acciones a realizar para cada caso."

Consideramos que es responsabilidad de cada usuario el uso de sus credenciales de acceso a los sistemas de información, toda vez que desde el PGSIRT se adelanta capacitaciones y campañas a todos los funcionarios en materia de seguridad de la información, realmente es un tema muy difícil de controlar si no se cuenta con la colaboración y la cultura de proteger la información.

El acceso al centro de datos, como es de conocimiento de la auditoría, se encuentra limitado al personal de TI, bajo controles físicos como puerta electromagnética de seguridad con acceso biométrico por reconocimiento de huella, que limita el acceso a esta área restringida, minimizando los riesgos mencionados en la observación.

Frente a uno de los activos (planta telefónica) el PGSIRT adelanta la organización de los cables que generan la alerta.

No es clara la observación. La administración en sí de un dispositivo de seguridad perimetral, indica la constante prueba de intentos de acceso no autorizado a los sistemas que componen la seguridad digital.

Frente a la ejecución de pruebas especializadas, el no realizar de manera anual este componente no indica una brecha mayor en este tipo de vulnerabilidades, principalmente si no se realizan cambios sobre los sistemas de información que establezcan vulnerabilidades.

Al ser repetitiva la apreciación frente a la definición del alcance del SGSI.

Se considera que la observación " Se logró identificar accesos no autorizados a los sistemas de información y manipulación indebida de información de los mismos, en donde un usuario

estaba ingresando a los equipos de cómputo con las credenciales de otro compañero debido a que no le habían suministrado su autenticación; al verificar el acceso de autenticación con las cal del directorio activo (Como se detalla en el ANEXO 10)existe menos licencias de la cantidad de usuarios activos en el sistema (cuando no se encontraban el planeta en emergencia sanitaria si alcanzaba a superar la cantidad de usuarios autenticados)." ya que fue descrita en el numeral "3. Debilidades de control de acceso los sistemas de información" por tanto no debería ser incluida en esta sección con la cual se considera no tiene relación."

La Auditoría efectúa el análisis de los comentarios del auditado así:

Respecto de la parte introductoria de la observación y Numeral 1, literales b, c, d y e: Se tuvieron en cuenta los comentarios durante la socialización, lo cual no significa su aceptación, tal como se indicó a los presentes en esa mesa del 09-oct-2020, sin embargo, se realiza el análisis de lo aumentado y evidenciado por escrito por parte de los auditados.

Respecto de la asignación de un valor económico de la información, es un aspecto esencial para definir un análisis de riesgos pues se requiere dicha valorización correcta de los activos de la información para poder definir los controles a implementar y poder establecer retorno de la inversión de cada control; la metodología para llevar a cabo este ejercicio, la deben definir los líderes de cada proceso como dueños de los activos a valorar y no la ACI en auditoria.

Ahora bien, el **MS001 MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN** define de manera clara cuales son los activos de la información, como se indica en el numeral "**10 SUBSISTEMA DE SEGURIDAD DE LA INFORMACIÓN:**

"El subsistema de seguridad de la información, busca preservar la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo que brinde confianza a los usuarios y partes interesadas de la entidad, acerca de que los riesgos sean gestionados adecuadamente.

La información es un activo que como otros activos importantes de la institución, es esencial para las actividades del IPES, la cual se puede manejar en diferentes medios como: impresa, almacenada electrónicamente o transmitida por correo electrónico, en consecuencia, necesita una protección adecuada, esto es especialmente importante en un entorno de operación cada vez más interconectado.

La seguridad de la información se logra implementando un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Los controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que se cumplan los objetivos de seguridad y de la entidad.

La documentación del subsistema se consulta en compartido sitio de publicación de la Documentación del SIG."

Todos los controles requieren estar documentados en un procedimiento o política con la inclusión de los 6 elementos de control de acuerdo a la Guía para la Administración de Riesgos y Diseño de Controles (DAFP, 2018), precisamente para garantizar su

cumplimiento en el marco del SIG. Los controles de Seguridad de la Información deben ser transversal a todas las áreas del IPES, y a algunos procesos como Gestión Documental, Gestión del Talento Humano, Gestión de Recursos Físicos y no solo limitarse a la seguridad digital, para mostrar un cumplimiento meramente normativo.

Se aclara que no se desconoce que existe equipos activos de infraestructura tecnológica para monitorear varios activos de la información, se vuelve a recalcar que los activos de la información no son únicamente su repositorio y toda la información no se encuentra en un repositorio tecnológico.

Si bien la auditoria evidenció la existencia del instructivo para la clasificación de activos de información, la observación versa sobre la deficiencia existente en la valorización de los activos respecto de la información contenida en los repositorios de la misma.

Respecto del numeral 2: si bien es cierto, durante la auditoría se evidenció la existencia de roles y responsabilidades por parte del área de Seguridad de la Información y recursos tecnológicos, los mismos, desde el procedimiento se encuentran enfocados a la seguridad digital, dejando de lado los demás aspectos de seguridad de la información, tales como control de archivo, control de acceso físico, etc. Igualmente, respecto de la participación del área en las mesas de trabajo por ellos mencionados, no se aportó en la réplica evidencias de las mismas.

Respecto del numeral 3: Es responsabilidad de cada usuario el uso de sus credenciales de acceso a los sistemas de información, pero también es responsabilidad del comité de seguridad de la información y al oficial de seguridad de la información el definir controles para mitigar el riesgo que se presente un incidente por el inadecuado uso de los recursos tal como lo indica la resolución IPES N° 615/2013.

Dentro de la información suministrada en la carpeta compartida, se evidenció un plan de mantenimiento del SGSI correspondiente a la vigencia 2020, pero no se evidenció las actividades que se estuvieran realizando, no se tuvo evidencia del plan de mantenimiento del SGSI durante las vigencias 2018 y 2019.

Respecto del numeral 4: Se reconoce que el acceso al datacenter, se encuentra limitado al personal de TI, bajo controles físicos como puerta electromagnética de seguridad con acceso biométrico por reconocimiento de huella, que limita el acceso a esta área restringida, sin embargo, la observación versa sobre el estado en que se encontraron los elementos allí mencionados y además, los controles que indicó el área, no eliminan el riesgo que se presente incidentes de tipo operativo.

La misma situación se evidenció también en el punto comercial de Kennedy: existencia de cableado sin canaleta y en mal estado, generando riesgos tanto de seguridad para los transeúntes como posibles riesgos eléctricos y en la Plaza de mercado de la Perseverancia: dentro de la Oficina Administrativa, el punto de Datos presentaba existencia de cableado sin peinar, lo que puede generar un riesgo operativo para dificultar la atención del soporte en el momento en que se requiera.

Respecto del numeral 5: Es importante establecer diferentes formas de verificar y comprobar la efectividad del control de acceso, un dispositivo de seguridad perimetral puede indicar una cantidad de alarmas, la infraestructura que posee el IPES, no es lo suficientemente robusta. Debido a que: no se realizan pruebas de control de acceso no autorizado a los sistemas que componen la seguridad digital y para evitar la aparición de bugs (defectos), vulnerabilidades o brechas de seguridad en aplicaciones en producción, pruebas anuales de seguridad de Etical Hacking, análisis de vulnerabilidades y/o pruebas de penetración, y otros tipos de pruebas como la ingeniería social. Según como indica el control ISO **A9.1.1. Política de control de acceso:** *Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información;* ***11.1.1 Perímetro de seguridad física:*** *Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información;* ***11.1.2 Controles de acceso físicos:*** *Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.;****11.1.3 seguridad de oficinas, recintos e instalaciones:*** *Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.*

En mérito de lo expuesto, el hallazgo se mantiene.

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 de Auditoría:

1. Deficiencia en la identificación y valorización de los activos de información

GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS. 2.1.4. Identificación de activos de seguridad de la información: *Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación TO.*

MS001 MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN; "10 SUBSISTEMA DE SEGURIDAD DE LA INFORMACIÓN: *El subsistema de seguridad de la información, busca preservar la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo que brinde confianza a los usuarios y partes interesadas de la entidad, acerca de que los riesgos sean gestionados adecuadamente.*
La información es un activo que como otros activos importantes de la institución, es esencial para las actividades del IPES, la cual se puede manejar en diferentes medios como: impresa, almacenada electrónicamente o transmitida por correo electrónico, en

consecuencia, necesita una protección adecuada, esto es especialmente importante en un entorno de operación cada vez más interconectado.

La seguridad de la información se logra implementando un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Los controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que se cumplan los objetivos de seguridad y de la entidad.

La documentación del subsistema se consulta en compartido sitio de publicación de la Documentación del SIG."

IN-085 CLASIFICACIÓN DE LOS ACTIVOS DE LA INFORMACIÓN: Inventario de activos: *Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.*

Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones: Artículo 13. Registros de Activos de Información. *Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información haciendo un listado de:*
a) Todas las categorías de información publicada por el sujeto obligado;
b) Todo registró publicado;
c) Todo registro disponible para ser solicitado por el público.

Activo de Información: *En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.*
Riesgo*: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).*

Lista Índices de Gestión y Desempeño. Política 14: Gestión Documental, Modelo de Seguridad y Privacidad de la Información – MINTIC, Índices desagregados por política: Componente estratégico – I65: *Mide la capacidad de la entidad pública de implementar actividades relacionadas con el diseño, planeación, verificación, mejoramiento y sostenibilidad de la función archivística, mediante la implementación de un esquema gerencial y de operación a través de planes, programas y proyectos que apalancan los objetivos estratégicos de la institución, además de articularse con otras políticas de eficiencia administrativa. //* **Componente cultural-I69:** *Mide la capacidad de la entidad pública de implementar acciones relacionados con la interiorización de una cultura archivística por el posicionamiento de la gestión documental que aporta a la optimización de la eficiencia y desarrollo organizacional y cultural de la entidad y la comunidad de la cual hace parte, mediante la gestión del conocimiento, gestión del cambio, la participación ciudadana, la protección del medio ambiente y la difusión.*

MinTIC: Guía No 5 - Gestión De Activos- Guía para la Gestión y Clasificación de Activos de Información. 5. INTRODUCCIÓN: *Esa guía entrega los lineamientos básicos que deben ser utilizados por los responsables de la seguridad de la información, para poner en marcha la gestión y clasificación de activos de información que son manejados por cada entidad del estado, con el fin de determinar que activos posee la entidad, de cómo deben ser utilizados, los roles y responsabilidades que tienen los funcionarios sobre los mismos y, reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe dársele. La realización de un inventario y clasificación de activos hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información con respecto a la seguridad de los activos de información de los procesos de una entidad, y cuyo objetivo es dar cumplimiento a cuatro puntos principales descritos en el Ítem 8 de la Tabla 2 – de la guía Controles del Anexo A del estándar ISO/IEC 27001:2013: //* ***6.1. DEFINICIÓN:*** *La definición consiste en determinar qué activos de información van a hacer parte del inventario, para esta tarea debe existir un equipo que realice la gestión de activos de información al interior de la entidad y por medio del líder del cada proceso (o quien haga sus vece de Líder requerido en gestión de calidad) ayude en realización de la actividad. En segunda instancia los líderes de procesos deben, solicitar la revisión de la definición de los activos por parte del propietario del activo de información designado, custodio y usuario del mismo, para que validen si son las partes interesadas o la parte de la entidad adecuadas para tener este rol. Es recomendable que la definición del inventario se lleve a cabo por lo menos una vez al año.*

Información básica

La información básica hace referencia a aquellas características del activo y para realizar la etapa de definición podría incluir como mínimo la siguiente:

- *Identificador: Número consecutivo único que identifica al activo en el inventario.*
- *Proceso: Nombre del proceso al que pertenece el activo.*
- *Nombre Activo: Nombre de identificación del activo dentro del proceso al que pertenece.*
- *Descripción/Observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.*
- *Tipo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:*
    - *Información: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.*
    - *Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.*
    - *Recurso humano: Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información. o Servicio: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.*

- *Hardware: Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.*
- *Otros: activos de información que no corresponden a ninguno de los tipos descritos anteriormente pero deben ser valorados para conocer su criticidad al interior del proceso*

Ubicación: Describe la ubicación tanto física como electrónica del activo de información.
Clasificación: Hace referencia a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad.
Justificación: Para cada valoración, describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad), o el argumento del porque se asignó dicha valoración.
Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información:

- *Alta. Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.*
- *Media. Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio.*
- *Baja. Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.*

Guía Para la Administración del Riesgo y el Diseño de controles en entidades públicas del DAFP: ¿Qué es tratamiento del riesgo? *Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo* ***cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio*** *de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo. //* **3.2.3 Nivel de riesgo (riesgo residual): EVITAR EL RIESGO:** *Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple,* ***la menos arriesgada y menos costosa****, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.*

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.

7.4. Políticas informáticas:

La directiva 005 de 2005 define las políticas generales de tecnologías de información comunicaciones aplicables a las entidades del distrito capital, las cuales se resumen es:

- *Planeación de informática*
- *Estandarización*
- *Seguridad y control*
- *Democratización de la información*
- *Marco legal*
- *Calidad*
- *Relación del gasto*
- *Cultura informática*

ISO 27001:2013: 6.1.1 Roles y responsabilidades para la seguridad de la información: *Se deben definir y asignar todas las responsabilidades de la seguridad de la información. //* **A.12.1.3. Gestión de capacidad:** *Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema. //* **A.11.2.2 Servicios de suministro:** *Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. //* **18.1.2 Derechos de propiedad intelectual:** *Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.*

PO-013 CARACTERIZACIÓN PROCESOS: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS: 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.*

CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN/SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – Guía 8 – MINTIC: 3 introducción: *El Modelo de Seguridad y Privacidad de la Información en la fase de Planificación se realiza la selección de controles, y durante la fase Implementación se ejecuta la implementación de controles de seguridad de la información, por lo cual se cuenta con el anexo de controles del estándar ISO 27002.*

2. <u>Falta definición de políticas o procedimientos relacionados con los procesos de monitoreo para la seguridad física</u>

ISO 27001:2013: A.5.1.2. Revisión de las políticas para seguridad de la información: *Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas. //* **A.9.1.1 Política de control de acceso:** *Se debe establecer documentar y*

revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. // **11.1.1 Perímetro de seguridad física:** *Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. //* **11.1.2 Controles de acceso físicos:** *Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. //* **11.1.3 seguridad de oficinas, recintos e instalaciones:** *Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. //* **11.1.4 protección contra amenazas externas y ambientales:** *Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. //* **A.16.1.1 Responsabilidad y procedimientos**: *Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. //* **A.16.1.3. Reporte de debilidades de seguridad de la información:** *Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.*

3. <u>Debilidades de control de acceso los sistemas de información</u>

MS-013 SUBSISTEMA DE GESTIÓN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 6 OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: *- Establecer directrices para la protección física de los activos de infraestructura tecnológica de la entidad. //* **6.3. Política de Control de Acceso. Objetivo:** *Controlar el acceso físico y lógico a la información, a los servicios de procesamiento de información, a los sistemas y servicios informáticos y de red del Instituto para la Economía Social, así como evitar la exposición de activos de información y medios de procesamiento de información a daño, perdida, robo o modificación accidental o intencional. El personal de la entidad debe ser consciente que debe tomar las precauciones necesarias para no revelar información no pública cuando se hace una llamada telefónica que puede ser interceptada mediante acceso físico a la línea o al auricular o escuchada por personas que se encuentren cerca. Lo anterior debe aplicar también cuando el empleado se encuentre en sitios públicos como restaurantes, transporte público o ascensores. //* **9.1.1 Política de control de acceso:** *Se debe establecer documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. //* **9.1.2 Acceso a redes y a servicios de red:** *Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. //* **9.2.1 Registro y cancelación del registro de usuarios:** *Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. //* **9.2.2 Suministro de acceso usuarios:** *Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios. //* **9.2.6 Retiro o ajuste de los derechos de acceso:** *Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.*

4. *Deficiencia en la organización de los recursos tecnológicos*

ISO 27001:2013: 8.1.3 Uso aceptable de los activos. *Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con la información e instalaciones de procesamiento de información. //* **11.1.1 Perímetro de seguridad física:** *Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. //* **11.1.3 seguridad de oficinas, recintos e instalaciones:** *Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. //* **11.1.4 protección contra amenazas externas y ambientales:** *Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.*

5. *Deficiencia asegurando la capacidad, desempeño y optimización de la infraestructura tecnológica*

CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN/ Guía 8-MINTIC: A.8.1.3 Uso aceptable de los activos: *Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. //* **A.11.1.3. Seguridad de oficinas, recintos e instalaciones:** *Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. //* **A.11.1.4. Protección contra amenazas externas y ambientales:** *Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. //* **A.11.1.5. Trabajo en áreas seguras:** *Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras. //* **A.11.2.1 Ubicación y protección de los equipos:** *Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.*

6. *Falta de proyección en la optimización del rendimiento de la red, la disponibilidad de recursos, la optimización y aumento del almacenamiento periódicamente*

CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN/ Guía 8-MINTIC
Aplicabilidad para entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de TI en el marco de la Estrategia de Gobierno en Línea (COBIT). // **6.2.1.2 Cubrir la Empresa de Extremo a Extremo:** *Las buenas prácticas contemplan el gobierno y la gestión de la información y la tecnología relacionada desde una perspectiva extremo a extremo y para toda la empresa. Esto significa que:»*
Se debe Integrar el gobierno de TI en el gobierno corporativo. Es decir, el sistema de gobierno para la empresa TI propuesto se integra sin problemas en cualquier sistema de gobierno.»» Se deben cubrir todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. Dado este alcance corporativo amplio, las buenas prácticas contemplan todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos. La información es una de las categorías de catalizadores de COBIT. El modelo mediante el que la metodología sugerida define los catalizadores permite a cada grupo de interés definir requisitos completos para la

información y el ciclo de vida de procesamiento de la información, conectando de este modo el negocio y su necesidad de una información adecuada y la función TI para soportar el negocio. El enfoque de gobierno debe ser extremo-a-extremo y está representado en la siguiente gráfica, mostrando los componentes clave de un sistema de gobierno. Además del objetivo de gobierno, los otros elementos principales del enfoque de gobierno incluyen catalizadores, alcance y roles, actividades y relaciones.

7. *Falta de información de actividades de medición que permitan realizar proyecciones de la estrategia TIC y SISG*

PLAN ESTRATÉGICO DE TIC: Un Enfoque Hacia la arquitectura Empresarial 2018-2021: *Aplicar los siete pasos del proceso de la mejora persigue los siguientes objetivos:*

- *Identificar oportunidades de mejora en servicios, procesos y herramientas.*
- *Reducir el costo de proveer servicios.*
- *Asegurar que TI apoya al negocio en sus metas.*
- *Identificar necesidades de medición, analizarlas y reportar oportunidades de mejora.*
- *Asegurar el cumplimiento de los requerimientos del negocio.*
- *Entender qué medir, qué se está midiendo y definir, cuidadosamente, el resultado exitoso.*

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, 2018).
- Mejorar la valorización de activos bajo el lineamiento del "MS001 MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN, 10 SUBSISTEMA DE SEGURIDAD DE LA INFORMACIÓN, La información es un activo que como otros activos importantes de la institución, es esencial para las actividades del IPES, la cual se puede manejar en diferentes medios como: impresa, almacenada electrónicamente o transmitida por correo electrónico, en consecuencia, necesita una protección adecuada, esto es especialmente importante en un entorno de operación cada vez más interconectado"
- El valor de la información debe ser definido por cada dueño de proceso.
- Ampliar el MS-013 SUBSISTEMA DE GESTIÓN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN para que sea transversal a todos los procesos del Instituto Para La Economía Social – IPES y así establecer políticas y/o procedimientos relacionados con los procesos de monitoreo para la seguridad física.
- Establecer controles y directrices para el cumplimiento de las políticas de control de acceso a los sistemas de información y áreas físicas.
- Realizar un plan de gestión de capacidad y disponibilidad de los recursos tecnológicos para cubrir las necesidades del recurso humano del Instituto Para La Economía Social – IPES.
- Realizar mantenimiento y organización al cableado estructura de datos y eléctrico a todas las sedes que hacen parte del del Instituto Para La Economía Social – IPES.

- Realizar diferentes pruebas para verificar la eficiencia de los diferentes controles de acceso a los sistemas de información para explotar las vulnerabilidades existentes en los sistemas críticos valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores y otros. Con el propósito de tomar las medidas preventivas en contra de posibles intrusiones malintencionados.
- Definir un plan de gestión de capacidad y disponibilidad para los diferentes recursos tecnológicos, repositorios de la información y canales de comunicación, el cual se define bajo los requerimientos de Gobierno TIC.
- Realizar actividades de medición que permitan efectuar proyecciones de la estrategia TIC y SGSI y así auditar el eficiencia de los objetivos trazados por el gobierno TIC.

Connotación: Administrativa.

Proceso: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS
Procedimientos: ***PR-033 Back Up, Generación y Recuperación***

No: 4

DESACTUALIZACIÓN PROCEDIMIENTO DE BACK UP, GENERACIÓN Y RECUPERACIÓN

Responsable de las acciones de mejora: SDAE

Se observó en el proceso para PR-033 BACK UP, GENERACIÓN Y RECUPERACIÓN que la SDAE realizó un cambio significativo en la realización del mismo durante las vigencias 2018, 2019 y 2020, debido a que se modificó el proceso de Back Up realizado 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.

Así mismo y de acuerdo al requerimiento de información para la auditoría mediante radicado 3854 del 10-jul-2020, no se obtuvo evidencia de los registros FO-319 de los Back Up que soportan la ejecución de respaldo de manera estricta de las vigencias 2018 y 2019 (solo desde noviembre de 2019 se evidencian respaldos hasta la fecha), con la siguiente periodicidad de los servicios:

- HEMI: diario, semanal, mensual
- GOOBI: diario, semanal, mensual
- File Server: diario, semanal, mensual
- Directorio Activo: diario, semanal
- Página Web: diario, semanal

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* ".

En la información suministrada no se evidencia en donde se realiza el respaldo correspondiente a la página web, por lo que no se pudo evidenciar que se esté ejecutando. Así mismo el área entregó información de back up identificados de la siguiente forma: SRV2K8IPES01, BackUp CheckUp-ecommerce, Logs SQL, SQL, los cuales no se encuentran descriptos en el proceso: PR-033 BACK UP, GENERACIÓN Y RECUPERACIÓN.

La información sobre los registros de los Back Up suministrada va desde el mes de noviembre de la vigencia 2019 hasta de junio de la vigencia 2020; en la bitácora suministrada (Herramienta que reemplazo los respaldos en cintas) del software VEEAM BACK UP va desde el 30 de enero de la vigencia 2020, el cual evidenció que no se realizó el registro de control de cambios en el proceso PR-033 BACK UP, GENERACIÓN Y RECUPERACIÓN; no sé suministraron las pruebas del monitoreo de la correcta realización de los respaldos, como lo indica el control de la ISO 27001:2013, ***A.12.3.1 Respaldo de 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.*

Tabla 8. *Análisis histórico de Back Up, realizados 2019 y 2020*

Servicio	Ultimo Registro de Back Up	Primer Registro de Back Up	Frecuencia
SRV2K8IPES01	27/11/2020		Único Back Up
BackUp CheckUp-ecommerce	26/11/2020		Único Back Up
DATAVM SRV2K18IPES25	14/07/2020	11/06/2020	Diario
HEMI	15/07/2020	11/05/2020	Diario
Intranet	26/11/2019	15/11/2020	Diario
GOOBI	15/07/2020	15/11/2019	Diario
Intranet nuevo portal	15/07/2020	26/11/2019	Diario
Antivirus Kaspersky	15/07/2020	26/11/2020	Diario
Directorio Activo	15/07/2020	21/11/2019	Diario
Directorio Activo de respaldo	14/07/2020	25/06/2020	Diario
Logs SQL	15/07/2020		Único Back Up
SQL	14/07/2020		Único Back Up
Back Up SQL	14/06/2020	11/07/2019	Diario
Pruebas Back Up SQL	26/06/2020	7/111/2019	Diario
Back Up Unidad D	15/07/2020	30/11/2019	Diario
Unidad F	07/11/2020	30/11/2019	Diario

Servicio	Ultimo Registro de Back Up	Primer Registro de Back Up	Frecuencia
Bitácora de Beem Back Up	Registrar los eventos, incidentes o acciones relacionadas con la gestión del servidor de BackUp		
	Fecha de creación de bitácora: 30-01-2020		

No se actualizó el proceso o un control de cambios, lo que denota la falta al principio ISO 27001: 2013, ***A12.1.2 gestión de cambios:*** *Se deben controlar los cambios en la entidad, en los procedimientos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.* En donde en el SoA (Statement of Aplicability, Declaración de Aplicabilidad) se afirma que está actividad se está cumpliendo al 100%.

Lo anterior debido al desconocimiento y falta aplicación de buenas prácticas en el respaldo de los sistemas de información lo que podría ocasionar que ante una falla en la infraestructura tecnológica o elementos que afecten los datos y al no realizar pruebas pueden generar inconvenientes al restablecer servicios.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR-132 - PROTECCIÓN DE INTERCAMBIO DE INFORMACIÓN, presentaron el siguiente Diseño de Control:

Control 1: PR-033 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.

El proceso PR-033 BACK UP, GENERACIÓN Y RECUPERACIÓN se encontraba desactualizado, aunque se reconoce que el proceso ha mejorado, también se evidencia la falta de actualizar el proceso, la conservación de las copias y realizar pruebas a los respaldos realizados tanto a nivel lógico como físico.

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 del procedimiento de cómo se ejecuta las tareas de BackUp de los activos de información institucional, con las excepciones se debe actualizar el procedimiento, ya que en el último trimestre de 2019 se realizó un cambio en la herramienta de BackUp, lo cual repercute en el manejo de la evidencia en la políticas de BackUp, Formato FO-319 solicitud recuperación de Información, por lo tanto generar evidencias de las pruebas a los sistemas de Back Up que no se encuentra en la descripción de la actividad de control.

Valoración comentarios del Auditado

El auditado argumenta que:

> *"En el marco de las actividades de definición, mantenimiento y mejora de los controles de seguridad de la información, que consolidan el SGSI, el PGSIRT adelantó el proyecto para establecer escenarios de contingencia y continuidad, por medio de la plataforma Veeam BackUp, que permite aumentar niveles de seguridad de la información. En ese sentido, el procedimiento de BackUp PR-033 es susceptible de actualización en una parte menor del documento, ya que las políticas de protección de la información mantienen su estructura."*

La Auditoría efectúa el análisis de los comentarios del auditado así:

Se reconoce que la plataforma Veeam BackUp puede aumentar niveles de seguridad de la ***información*** en cuanto respaldo de la información en los repositorios tecnologicos, pero al observar el procedimiento de BackUp PR-033-BACKUP GENERACIÓN Y RECUPERACIÓN, se evidencia que no corresponde al proceso en la actualidad, por lo que se reitera la necesidad de incluir está actividad en el procedimiento de acuerdo al se señala en el instructivo **IN-001 ELABORACIÓN, MODIFICACIÓN O ANULACIÓN DE DOCUMENTOS DEL IPES/ 6.1.7 Seguimiento y control de cambios** en donde establece que "*El control de los documentos se encuentra bajo la responsabilidad de Gestión Documental y los l**íderes de proceso y/o subproceso**" y se solicita actualizar los documentos en una vez al año, cuando **no se realiza la actualización se debe realizar un control de cambios***", circunstancia que no se llevó a cabo en el PR-033-BACKUP GENERACIÓN Y RECUPERACIÓN, durante la vigencia 2020 con ocasión de la emergencia sanitaria el cual corresponde al servicio de mesa de ayuda.

En mérito de lo expuesto, el hallazgo se mantiene.

Riesgo Asociado: Pérdida de Disponibilidad de la información por daños en la Infraestructura Tecnológica de la Entidad: Indisponibilidad de la información, Daños o funcionamiento inadecuado de la plataforma tecnológica de la entidad por no contar con medidas implementadas que garanticen la Continuidad de los servicios tecnológicos frente a cualquier eventualidad.

Normatividad o Criterio:

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 7. Gestión de Comunicaciones y operaciones.*
PR-033-BACKUP GENERACIÓN Y RECUPERACIÓN: 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. //* **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. (…) La ejecución de tareas de BackUp de los activos de información institucional digital, debe realizarse de manera estricta, en cumplimiento de Ios siguientes aspectos principales:*

No	***Activos de información Institucional Digital***	***Frecuencia Realizada***	***Tipo de copia***	***Almacenamiento***	***Notas Adicionales***
1	*HEMI*	- *Diaria* - *Semanal y* - *Mensual*	*Incremental*		
2	*GOOBI*	- *Diaria* - *Semanal y Mensual*	*Incremental*		
3	*DIRECTORIO ACTIVO*	- *Diaria y* - *Semanal*	*FULL*		
4	*PAGINA WEB*	- *Diaria y* - *Semanal*	*FULL*		
5	*FILE SERVER*	- *Diaria* - *Semanal y* - *Mensual*	*Incremental*		
6	*VIRTUALIZACIÓN*	*Durante su configuración y puesta en operación en el evento en que se realicen cambios significativos*	*FULL*		
7	*ACTIVOS DE INFRAESTRUCTURA TECNOLOGICA*	*Durante su configuración y puesta en operación en el evento en que se realicen cambios significativos*	*FULL*		

ISO 27001:2013: A.12.1.2 Gestión de cambios: *Se deben controlar los cambios en la entidad, en los procedimientos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. //* **A.12.3.1 Respaldo de 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.*

Guía Metodológica de Pruebas de Efectividad-Guía 1. 11 INFORMES Y RECOMENDACIONES: *En esta fase ya se cuenta con la información resultante del levantamiento de información, pruebas, análisis y evidencias recolectados, se han evidenciado las vulnerabilidades técnicas explotables y la línea base de seguridad de la entidad evaluada, su brecha frente a la norma ISO 27001 y los requisitos frente a al MSPI, Gobierno en Línea y en relación con mejores prácticas. De la misma forma en cada uno de los análisis se han documentado las recomendaciones para mejorar o subsanar las debilidades y hallazgos. Lo anterior permitirá determinar el nivel de madurez y construir los informes de las pruebas técnicas y administrativas. //* **Elaboración de la política general de seguridad y privacidad de la información-Guía 2. Disposición de los activos:** *Esta política debe determinar la obligatoriedad para la construcción y cumplimiento de un procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los activos. Esta política debe determinar la toma de BackUp de los activos evitando así el acceso o borrado no autorizado de la información, la política debe indicar quien es el responsable de emitir las correspondientes autorizaciones y debe aplicar tanto para medios removibles como activos de procesamiento y/o almacenamiento de información.*

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 procedimental 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.*

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, 2018).
- Actualizar el procedimiento PR-033.
- Realizar pruebas para conocer que los respaldos estén quedando bien realizados y disponibles cuando se requiera, y de acuerdo a las pruebas definir KPI (Key Performance Indicator, Indicador clave de rendimiento) para conocer la efectividad del proceso.

- Para realizar una mejor practica de seguridad se sugiere realizar el esquema de BackUp 3-2-1, que consiste en 3 copias de para respaldo en total, distribuidas así dos (2) soportes diferentes en donde se tiene el respaldo de la información, una (1) copia de respaldo externa u offline, que no se encuentre cerca geográficamente de la ubicación.

Connotación: Administrativa.

Proceso: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS
Procedimientos: ***PR-133 Acceso a los Medios de Procesamiento de Información***

No: 5

DEFICIENCIA EN LOS LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Responsable de las acciones de mejora: SDAE

Se evidenció que los lineamientos y protocolos de seguridad de la información de la entidad presenta deficiencias en los aspectos de la gestión y acceso de usuarios en los sistemas de información y a las áreas físicas.

Para lo cual se llevó a cabo revisión sobre los diferentes documentos:

- Análisis de políticas de control de acceso a áreas físicas mediante FO325.
- Análisis de la ejecución de mantenimientos de acuerdo al plan 2018, 2019, 2020.

Se observaron las siguientes situaciones:

1. *Ausencia de protocolos de acceso a áreas físicas*

Se evidenció que no existen procedimientos para definir el control de acceso a las diferentes áreas físicas diferentes a las tecnológicas en el IPES, a pesar que el IPES tiene consignados en sus procedimientos lo siguiente:

PR-133 OTORGAR ACCESO A LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN, indicaba en el punto 2. alcance: "*aplica para todos los medios de procesamiento de información y las* ***áreas donde se encuentran alojados los activos de infraestructura tecnológica que soportan la operación*** *informática del Instituto para la economía Social – IPES*." (página 1); en donde se evidenció que los controles para áreas seguras solo están establecidos a los recursos tecnológicos. Donde continuamente en el punto **3. RESPONSABLES**, se desplegó responsabilidades para todo tiempo de acceso de información sin importar si es digital o física.

En la página 1, el punto ***3.1. Administradores de la plataforma tecnológica (medios de procesamiento de información) de la entidad:***

- *Definir controles de seguridad física para los medios de procesamiento de información de la entidad.*

No se indicó en donde se podía validar los controles de seguridad física establecidos.

Así mismo se evidenció que a pesar de existir el formato FO-325 GESTIÓN DE PERFIL DE USUARIO, en este únicamente se registran el acceso a los usuarios a nivel informático y no en el control de acceso a áreas físicas.

Lo anterior por cuanto el enfoque que ha realizado la entidad versa sobre la seguridad digital y no una visión más amplia que integre aspecto como seguridad de la información y sus riesgos derivados. Lo que podría ocasionar un riesgo para la modificación y/o alteración de la información.

2. *Falta documentar la depuración de usuarios en la ejecución de mantenimientos de acuerdo al plan 2018, 2019, 2020*

Al solicitar información mediante radicado 4305 del 11-ago-2020 mediante el cual la Auditoría solicitó las evidencias de las pruebas a los mantenimientos realizados, fue suministrado a la presente auditoria la "*BITACORA – PLAN DE MANTENIMIENTO PARA SEGURIDAD DE LA INFORMACIÓN"* y las *"ACTIVIDADES DE MANTENIMIENTO PARA HARDWARE Y SOFTWARE".*

Por lo tanto, no se aportó registro, acta, correos y/o alguna evidencia de que aparte de los mantenimientos se realicen pruebas y al revisar los documentos aportados se concluye:

En la BITACORA – PLAN DE MANTENIMIENTO PARA SEGURIDAD DE LA INFORMACIÓN no se evidencia actividades de control de acceso para áreas físicas y para los controles de acceso públicos, no se documenta en el análisis amenazas y vulnerabilidades para el acceso de la información.

En las ACTIVIDADES DE MANTENIMIENTO PARA HARDWARE Y SOFTWARE que se ejecuta dentro de la vigencia 2020 se evidenció que en las actividades de mantenimiento en el tema: 7. CUENTAS DE USUARIOS se realizó la depuración de las cuentas de acceso de los usuarios, pero no se documenta los registros de las actividades realizadas.

Ver detalle **ANEXO 8.**

Al materializarse una falla en la infraestructura tecnológica a nivel lógico (Software) y/o físico (Hardware) en equipos activos la ausencia de pruebas para medir su eficacia. La falta de controles en áreas comunes puede presentar vulnerabilidad(es) y/o amenaza(s) pudiendo materializarse robos de elementos, fuga, manipulación, espionaje y/o secuestro de la información.

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 INFORMACION, presentaron el siguiente Diseño de Control:

Control 1: PR-133: Actividad 2: Enviar solicitud aprobada a SDAE-Sistemas. Se entrega solicitud aprobada en la SDAE-Sistemas // Actividad 4: Otorgar, modificar, o eliminar los permisos acceso a los medios. Se otorga, modifica o eliminan los permisos de acceso previamente autorizados con el rol y privilegios definidos, así mismo se activa el proceso de monitoreo de medios de procesamiento para hacerle seguimiento al acceso creado. // Actividad 5: Informar la asignación, modificación de permisos de acceso a los medios. Se informa al usuario solicitante la autorización/modificación/eliminación de acceso a medios de procesamiento de información. // Actividad 6: Informar al área solicitante la denegación de la solicitud. Se informa al solicitante que permisos NO fueron otorgados.

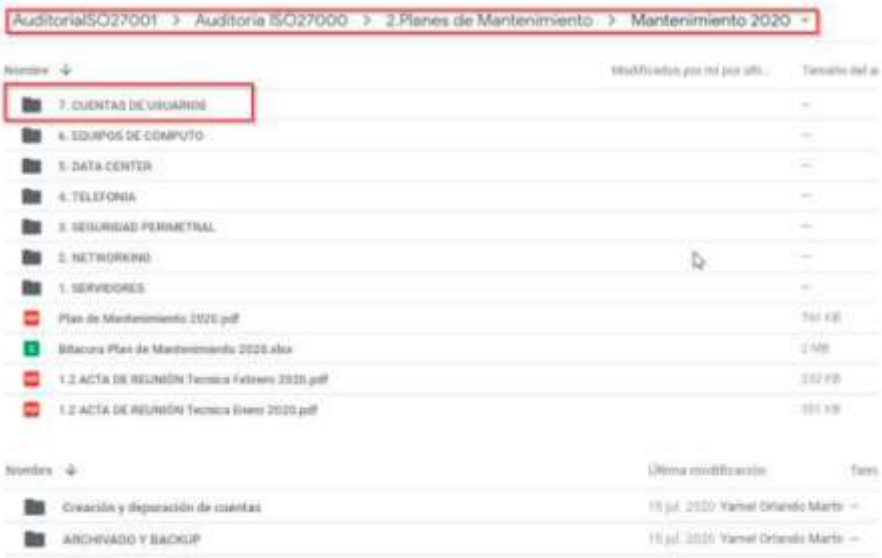
De lo anterior, al observar el flujo de control del procedimiento respecto de los 6 elementos del control: Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control, se encontró debilidad en el manejo del excepciones no se está diligenciando el formato de solicitud acceso a los medios FO-325 - GESTION PERFIL DE USUARIO, por parte de los Directivos o supervisores de contrato que aprueba los permisos de acceso a los medios de procesamiento. de como se ejecuta las tareas de BackUp de los activos de información institucional, con las excepciones se debe actualizar el procedimiento, ya que en el último trimestre de 2019 se realizó un cambio en la herramienta de BackUp, lo cual repercute en el manejo de la evidencia en las políticas de BackUp, Formato FO-319 solicitud recuperación de Información, por lo tanto, generar evidencias de las pruebas a los sistemas de Back Up que no se encuentra en la descripción de la actividad de control.

Valoración comentarios del Auditado

El auditado argumenta que:

Respecto del numeral 2:

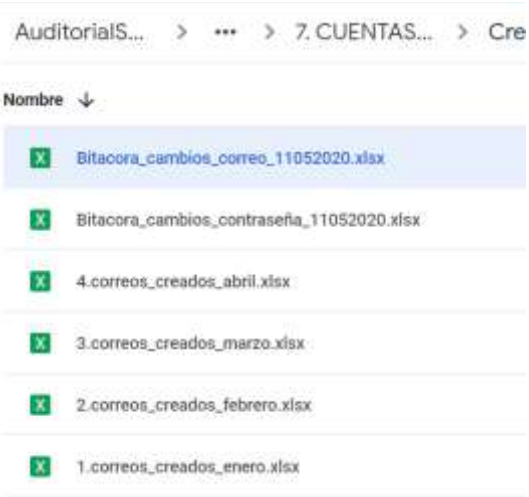
> *"Realizando la revisión de la información solicitada en el radicado 4305 del 11-ago-2020 se encuentra que se requirió la siguiente información:*
>
> - *Planes de mantenimiento preventivo y sus planes de prueba sobre los equipos y servicios tecnológicos ofrecidos por el área de TI, incluyendo el plan de mantenimiento del edificio de la sede administrativa de los dispositivos que soportan la operación del Centro de Cómputo, Centros de Cableado y todos los Pisos (Servidores, Sistemas de Back Up, dispositivos activos TI, planta eléctrica, UPS, aires acondicionados), esta información debe abarcar las vigencias 2018, 2019 y 2020.*
> - *Usuarios activos e inactivos del directorio activo.*
>
> *No se requirió información con respecto al tema de evidencias depuración de cuentas de acceso.*
>
> *No obstante, en la información entregada a Control Interno dentro de la carpeta "Auditoria ISO 27001" se encuentra la información correspondiente a la depuración, creación de cuentas y archivado a fecha 15 de Julio de acuerdo al plan de mantenimiento para el año 2020."*



Por tanto, la depuración de cuentas de usuario es una actividad que se encuentra documentada mes a mes de acuerdo a las evidencias entregadas."

La Auditoría efectúa el análisis de los comentarios del auditado así:

Cómo se mencionó en la replica, mediante el radicado 4305 del 11-ago-2020, se solicitaron los planes de mantenimiento preventivo y sus planes de prueba sobre los equipos y servicios tecnológicos soportados por el área de TIC. Al analizar nuevamente la ruta de los archivos señalada por el área en su réplica, respecto a los usuarios activos e inactivos del directorio activo, solo se evidencia la creación de cuentas de correos y cambio de contraseñas, la auditoría tuvo como alcance las vigencias 2018, 2019 y 2020, en ninguna de las 3 vigencias se pudo corroborar la depuración de cuentas como lo indica la siguiente imagen:



Igualmente se recuerda que la información solicitada, debe aportarse en su totalidad, 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 162 del 30 de mayo de 2018 por lo tanto la información no suministrada no puede ser auditada y tampoco omite el compromiso del auditado en suministrarlo al tener relación con los requerimientos de información.

En mérito de lo expuesto, el hallazgo se mantiene.

Riesgo Asociado: Afectación a la confidencialidad y/o integridad de la información por suplantación de la identidad del usuario: Puede generar a la entidad problemas de reputación, existen casos en los que se utilizan datos de terceras personas para suplantar su identidad y cometer algún tipo de delito, todas aquellas actividades realizadas por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal.

Normatividad o Criterio:

1.Ausencia de protocolos de acceso a áreas físicas

PR-133 OTORGAR ACCESO A LOS MEDIOS DE PROCESAMIENTO DE INFORMACION: Actividad 2: *Enviar solicitud aprobada a SDAE-Sistemas. Se entrega solicitud aprobada en la SDAE-Sistemas. //* **Actividad 4:** *Otorgar, modificar, o eliminar los permisos acceso a los medios. Se otorga, modifica o eliminan los permisos de acceso previamente autorizados con el rol y privilegios definidos, así mismo se activa el proceso de monitoreo de medios de procesamiento para hacerle seguimiento al acceso creado. //* **Actividad 5:** *Informar la asignación, modificación de permisos de acceso a los medios. Se informa al usuario solicitante la autorización/modificación/eliminación de acceso a medios de procesamiento de información. //* **Actividad 6:** *Informar al área solicitante la denegación de la solicitud. Se informa al área solicitante que permisos NO fueron otorgados.*

MS-013 Manual del Subsistema de Gestión de Seguridad y Privacidad de la Información: 7. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: *La desarrollo de la presente política de seguridad y privacidad de la información, así como la definición, implementación, mantenimiento y mejora de los controles de seguridad informática cubren todos los activos de infraestructura tecnológica (servidores, equipos de cómputo, equipos de comunicaciones, entre otros) y a todos los activos de información, (Bases de Datos, Documentos, SIG, Servicios Informáticos, documentos, registros), a fin de proteger la información institucional digital contra daño, pérdida, sustracción, modificación accidental o intencional, describiendo buenas prácticas en el uso de los sistemas y servicios informáticos, así como de los activos de tecnologías*

de información y comunicaciones, dispuestos por el Instituto para la Economía Social a los usuarios para el cumplimiento de sus funciones.

CARACTERIZACIÓN PROCESOS: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS. Políticas de Operación: *Políticas de seguridad y privacidad de la información establecidas en el marco de la NTC ISO- IEC 27001-2013 y la normativa vigente, contempladas en el manual de seguridad de la información de la entidad.*

PR-133 OTORGAR ACCESO A LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN: 2. ALCANCE: *El presente procedimiento aplica para todos los medios de procesamiento de información y las áreas donde se encuentran alojados los activos de infraestructura tecnológica que soportan la operación informática del Instituto para la economía Social – IPES. Aplicable a todos los funcionarios, contratistas y terceros que requieran acceder a los activos de información institucional, medios de procesamiento de información y las áreas donde se encuentran alojados. //* **3. RESPONSABLES:** *La Subdirección de Diseño y Análisis Estratégico es responsable de designar a las personas encargadas de hacer cumplir los lineamientos, otorgar permisos de acceso a los medios de procesamiento de información de acuerdo a las directrices y lineamientos dispuestos por la entidad relacionados con la seguridad y privacidad de la información. //* **3.1 Administradores de la plataforma tecnológica (medios de procesamiento de información) de la entidad:**

- *Definir controles de seguridad física para los medios de procesamiento de información de la entidad.*
- *Definir niveles de seguridad asociados a cada rol y cargo del área, así como los controles adecuados de cada nivel.*
- *Habilitar los permisos de acceso a los usuarios (funcionarios, contratistas, terceros), establecido desde las diferentes dependencias, de acuerdo al perfil y rol designado.*
- *Generar el listado de usuarios autorizados y mantenerlo actualizado con tareas predefinidas y acceso a los diferentes medios de procesamiento de información.*
- *Autorizar el traslado de equipos de computación. (Se hace con formato de traslado de elementos de almacén).*

MS-013 Manual del Subsistema de Gestión de Seguridad y Privacidad de la Información: 7. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: *La desarrollo de la presente política de seguridad y privacidad de la información, así como la definición, implementación, mantenimiento y mejora de los controles de seguridad informática cubren todos los activos de infraestructura tecnológica (servidores, equipos de cómputo, equipos de comunicaciones, entre otros) y a todos los activos de información, (Bases de Datos, Documentos, SIG, Servicios Informáticos, documentos, registros), a fin de proteger la información institucional digital contra daño, pérdida, sustracción, modificación accidental o intencional, describiendo buenas prácticas en el uso de los sistemas y servicios informáticos, así como de los activos de tecnologías de información y comunicaciones, dispuestos por el Instituto para la Economía Social a los usuarios para el cumplimiento de sus funciones.*

CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN/SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – Guía 8 – MINTIC: 3 introducción: *El Modelo de Seguridad y Privacidad de la Información en la fase de Planificación se realiza la selección de controles, y durante la fase Implementación se ejecuta la implementación de controles de seguridad de la información, por lo cual se cuenta con el anexo de controles del estándar ISO 27002.*

ISO 27001:2013: A11.1.1 Perímetro de seguridad física: *Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. //* **11.1.2 Controles de acceso físicos:** *Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. //* **11.1.3 seguridad de oficinas, recintos e instalaciones:** *Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. //* **A.8.1.1. Inventario de activos:** *Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.*

MinTIC: Guía No 5 - Gestión De Activos- Guía para la Gestión y Clasificación de Activos de Información. 7 INTRODUCCIÓN: *Esa guía entrega los lineamientos básicos que deben ser utilizados por los responsables de la seguridad de la información, para poner en marcha la gestión y clasificación de activos de información que son manejados por cada entidad del estado, con el fin de determinar que activos posee la entidad, de cómo deben ser utilizados, los roles y responsabilidades que tienen los funcionarios sobre los mismos y, reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe dársele. La realización de un inventario y clasificación de activos hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información con respecto a la seguridad de los activos de información de los procesos de una entidad, y cuyo objetivo es dar cumplimiento a cuatro puntos principales descritos en el Ítem 8 de la Tabla 2 – de la guía Controles del Anexo A del estándar ISO/IEC 27001:2013: (…).*

Lista Índices de Gestión y Desempeño, Política 6: Gobierno Digital, Índice de Gobierno Digital-POL06: *Mide la capacidad de la entidad pública de usar y aprovechar tecnologías de la información y las comunicaciones TIC para consolidar un Estado y ciudadanos proactivos e innovadores que generan valor público en un entorno de confianza digital.*

2 falta documentar la depuración de usuarios en la ejecución de mantenimientos de acuerdo al plan 2018, 2019, 2020.

ISO 27001:2013: 9.1.1 Política de control de acceso: *Se debe establecer documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. //* **9.1.2 Acceso a redes y a servicios de red:** *Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. //* **9.2.1 Registro y cancelación del registro de usuarios:** *Se debe implementar un proceso formal de registro y de cancelación de registro de*

usuarios, para posibilitar la asignación de los derechos de acceso. // **9.2.2 Suministro de acceso usuarios:** *Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios. //* **9.2.2 Suministro de acceso usuarios:** *Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios. //* **9.2.5 Revisión de los derechos de acceso de usuarios:** *Los propietarios de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares. //* **9.2.6 Retiro o ajuste de los derechos de acceso:** *Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.*

ACTIVIDADES DE MANTENIMIENTO PARA HARDWARE Y SOFTWARE: *7. CUENTASDE USUARIOS se realizaba la depuración de las cuentas de acceso de los usuarios, pero no se documenta los registros de las actividades realizadas.*

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, 2018).
- Ampliar el MS-013 Manual de Seguridad de la Información a cubrir la seguridad de la información de manera transversal a toda el
- Definir políticas, procesos y/o controles para establecer control de acceso a los sitios de interés de seguridad de la información.
- Definir auditorias para los controles establecidos para el control de acceso físico.
- Crear un control oportuno para la depuración de usuarios para controlar el acceso a todos los perfiles.

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: 6

INOPERANCIA DEL PLAN DE CONTINGENCIA DE TI

Responsable de las acciones de mejora: SDAE

En la revisión del DE-025 PLAN DE CONTINGENCIA TI se identificaron las siguientes situaciones que imposibilitan al IPES a continuar su operación en caso de desastre por la falta de un plan de contingencia ejecutable por las siguientes situaciones:

1. *No se garantiza la continuidad de las operaciones del IPES en caso de desastre*

Se evidenció que a pesar de la existencia del DE-025 PLAN DE CONTINGENCIA DE TI del 16-ene-2020/versión 2, en caso de un siniestro es imposible la ejecución del mismo, toda vez que existe una vulnerabilidad si se requiriera activar la continuidad de la operación así:

El plan contempla como sitio alterno la sede Barichara para garantizar la continuidad de la operación, de lo cual cuando se solicitó la información con evidencias fotográficas respecto de esa sede en el radicado 00110-817-004367, el área de SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLOGICOS suministró como evidencia las siguientes fotografías:

Imagen 6. Registro fotográfico suministrado por SDAE como sede alterna para plan de contingencia

Sin embargo, al realizarse pruebas de auditoría se evidenció que el ultimo contrato de arrendamiento de la Sede Barichara es el 265 de 2014 cuyo objeto es *"ARRENDAMIENTO DEL INMUEBLE UBICADO EN LA CALLE 19 No 3-16 LOCALES 301,302,303 PISO 3, PARA LA SEDE DE LA SUBDIRECCION DE FORMACION Y EMPLEABILIDAD DEL INSTITUTO PARA LA ECONOMIA SOCIAL"* el cual finalizó el 17-nov-2015, situación que igualmente fue corroborada por el auditado en visita programada para el 28-sep-2020, cuando se encontraba el auditor al frente de la edificación del supuesto punto alterno de acuerdo a lo aprobado en el Plan de Contingencia de TI para 2019 y 2020.

2. *Ausencia de control de cambios cuando se requiere*

Al revisar el PLAN DE CONTINGENCIA DE TI, se observa respecto a la ISO 270001 se encontró incumplimiento en los siguientes controles: A.12.1.2 Gestión de Cambios, A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación. El

IPES tenía el Documento Estratégico DE-025 PLAN DE CONTINGENCIA TI v2, el cual en MIPG en el **IN-001 ELABORACIÓN, MODIFICACIÓN O ANULACIÓN DE DOCUMENTOS DEL IPES/ 6.1.7 Seguimiento y control de cambios** en donde *"El control de los documentos se encuentra bajo la responsabilidad de Gestión Documental y los Líderes de proceso y/o subproceso"* y se solicita actualizar los documentos en una vez al año, cuando no se realiza la actualización se debe realizar un control de cambios, situación que no se llevó a cabo en el DE-025 PLAN DE CONTINGENCIA TI, al momento de no contar el IPES con la sede de Barichara como sede alterna.

Lo anterior debido a la ausencia de un plan de contingencia actualizado contra daños que puedan ser ocasionados por incendios, inundaciones, terremotos, explosiones, perturbación del orden, y otras formas de desastre natural o artificial al no tener un plan de contingencia actualizado no permitiría continuar el servicio a las partes interesadas del IPES.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR-131 MONITOREO ACCESO A LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN, presentaron el siguiente Diseño de Control:

Control 2: 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 11 Gestión de la Continuidad del Negocio. // Actividad 3: Desarrollo de las estrategias. Se debe llevar a cabo el desarrollo de las estrategias para garantizar la continuidad de las actividades del Negocio. // Actividad 5: Desarrollo de las estrategias. Prueba y Aprobación del Plan de Continuidad del Negocio. // A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.

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 por No se cuenta con documentación formalizada, referente a la gestión de Control de Cambios en la Infraestructura Tecnológica, además que el plan de contingencia se encuentra desactualizado hace dos (2) años a pesar de estar firmado como actualizado, en el manejo de la evidencia no se encontró que se realicen pruebas a los sistemas de Back Up ni simulacros para el plan de contingencia.

Valoración comentarios del Auditado

El auditado argumenta que:

> *"Frente a las conclusiones de la auditoría, se debe partir por precisar que el DE-025, hace referencia a la continuidad de la operación informática frente a la materialización de eventos inesperados de seguridad que comprometan total o parcialmente los sistemas y servicios informáticos que apoyan el cumplimiento de la misionalidad del IPES, a diferencia de lo mencionado por la ACI donde se afirma "En la revisión del DE-025 PLAN DE CONTINGENCIA*

DE TI se identificaron las siguientes situaciones que imposibilitan al IPES continuar con su operación…", para lo cual debió remitirse al Plan de Contingencia Institucional Actualmente se evidencia una desactualización en el documento DE-025, y debe ser actualizado conforme a las nuevas necesidades y alternativas a nivel tecnológico implementadas. El PGSIRT realizó el diseño de una solución integral de BackUp y ejecutó el proyecto para su implementación y puesta en operación, bajo la tecnología Veeam, tecnología descrita en desarrollo de la auditoría, que permite contar con escenarios de contingencia y continuidad de la operación informática."

La Auditoría efectúa el análisis de los comentarios del auditado así:

Respecto al PLAN DE CONTINGENCIA INSTITUCIONAL, mencionado en la réplica por parete del área, no fue posible su revisión por cuanto no fue aportado durante la auditoría, ni en la socialización, ni anexado en la presente réplica; si embargo, se recalca que la observación versa sobre la inoperancia del DE-025 PLAN DE CONTINGENCIA DE TI por encontrarse desactualizado en los elementos descritos en la observación y que no fueron desvirtuados en la réplica.

En mérito de lo expuesto, el hallazgo se mantiene.

Riesgo Asociado: Afectación a la disponibilidad de la información por desastres naturales (sismo, incendio, inundación): Daños o funcionamiento Inadecuado de la plataforma tecnológica de la entidad por no implementar medidas que garanticen la Integridad y Disponibilidad de la información y de las instalaciones de procesamiento de información frente a cualquier eventualidad.

1. No se garantiza la continuidad de las operaciones del IPES en caso de desastre

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 10: Garantizando la oportuna y adecuada prestación de los servicios con un soporte moderno en su infraestructura física, tecnológica, documental, administrativa y organizacional en el marco del respeto a las normas de protección ambiental.*

ISO 27001:2013: A.12.1.2 Gestión de Cambios: *Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. //* **A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación:** *Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización. //* **A. 17.1.1 Planificación de la continuidad de la seguridad de la información:** *La entidad debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. //*

A. 17.1.2 implementación de la continuidad de la seguridad de la información: *La entidad debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.*

2. Ausencia de control de cambios cuando se requiere

ISO 27001:2013: A.12.1.2 Gestión de Cambios: *Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.*

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.
6. **CONDICIONES GENERALES:**
Acorde al Modelo Integrado de Planeación y Gestión, hay una gran necesidad de procedimental 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.*

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, 2018).
- Desarrollar actualización y mantenimiento al DE-025 PLAN DE CONTINGENCIA DE TI para asegurar la continuidad del Instituto Para La Economía Social – IPES en caso de desastre o que se requiera activar la contingencia.
- Realizar la documentación y divulgar el control de cambios cada vez que se requieran realizar.

Connotación: Administrativa

No: 7

FALTA DE PRUEBAS AL SOFTWARE Y/O HARDWARE PARA ASEGURAR CONTINUIDAD EN LOS SERVICIOS CRÍTICOS

Responsable de las acciones de mejora: SDAE

En la revisión de los planes de mantenimiento de seguridad 2018, 2019 y 2020 se evidenció que la entidad no cuenta de manera documentada con las pruebas del funcionamiento software y/o hardware para asegurar los servicios críticos en caso de falla de estos, pues dicha información se solicitó mediante radicado 4305 y no fue suministrada.

Cuando se realizó la revisión de "ACTIVIDADES DE MANTENIMIENTO PARA HARDWARE Y SOFTWARE" se observó que no se contempla plan de pruebas a los elementos de Software y/o Hardware independientes de los mantenimientos realizados.

Lo anterior debido a que la entidad al no documentar las pruebas independientes a las actividades del proveedor no se registra si los mantenimientos están en correcto funcionamiento, lo que puede ocasionar que los mantenimientos no estén quedando bien realizados y/o se requiera más soporte sobre esos servicios.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR-131 MONITOREO ACCESO A LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN, presentaron el siguiente Diseño de Control:

Control 1: 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 mantenimientos de sistemas. // Actividad 3: Realizar Verificaciones de validación. Se deben incorporar verificaciones de validación en las Aplicaciones, para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados. // A.14.2.9 Prueba de aceptación de sistemas.

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 del procedimiento realizando verificaciones de validación en las aplicaciones teniendo elementos en producción sin realizar pruebas de los elementos lógicos y físicos para probar su restauración, en el manejo de las excepciones para los Sistemas de Información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados y en la evidencia no se puede evidenciar un plan de pruebas.

Valoración comentarios del Auditado

El auditado argumenta que:

> *"En desarrollo de los ejercicios de entrevista, pruebas de recorrido, respuesta a requerimientos, entre otros, se socializó a la ACI los servicios que componen el portafolio de servicios de TI, para los cuales se contemplan tareas de administración para garantizar su disponibilidad.*

La entidad cuenta principalmente con 3 sistemas de información con los cuales se soportan procesos misionales, administrativos y de gestión:
- Sistema de Información misional HEMI
- Sistema de información administrativo y financiero GOOBI
- Suite Google Apps Bussines Edition
Como se puede observar, la responsabilidad directa de los profesionales del PGSIRT en términos de desarrollo se centra sobre el sistema de información misional, el cual no ha sufrido cambios estructurales que requieren un exhaustivo protocolo de pruebas para su entrada en operación y no se cuenta con incidentes registrados que comprometan su operación.
En lo referente a GOOBI y Correo electrónico, la entidad establece ANS y condiciones contractuales para garantizar su continuidad. (ver procesos contractuales). Como eje fundamental en la operación informática institucional, el PGSIRT cuenta con roles y responsabilidades frente a la administración de los activos de infraestructura tecnológica sobre los cuales operan los sistemas y servicios informáticos, y realiza actividades permanentes de seguimiento y monitoreo."

La Auditoría efectúa el análisis de los comentarios del auditado así:

En la observación FALTA DE PRUEBAS AL SOFTWARE Y/O HARDWARE PARA ASEGURAR CONTINUIDAD EN LOS SERVICIOS CRÍTICOS, no se omite la realización de seguimientos y monitorios por parte del área a los 3 sistemas por ellos mencionados en su réplica, pero si se hace referencia es a la ausencia de pruebas a los diferentes componentes de los sistemas de información, que incluyen, entre otros, temas de verificación del estado de los servidores de respaldo, verificación la redundancia y alta disponibilidad del servicio de la Internet, la utilización en el IPES de KPIs (Key Performance Indicator, Indicador clave de rendimiento) que permitan medir la eficiencia de la operación y de sus respaldos en caso de manifestarse un incidente; situaciones estas de las que no so obtuvo evidencia alguna.

En mérito de lo expuesto, el hallazgo se mantiene.

Riesgo Asociado: Afectación a la disponibilidad de la información por fallas de origen técnico en el Software y/o Hardware: Se debe contar con un análisis de necesidades de la entidad y definir en base a estas necesidades una plataforma tecnológica con una infraestructura en hardware, software, personal operativo, etc. que soporte las operaciones de las instalaciones del centro de datos; en donde se garantice la Disponibilidad de la Información institucional.

Normatividad o Criterio:

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 mantenimientos de sistemas.** ***//*** **Actividad 3:** *Realizar Verificaciones de validación. Se deben incorporar verificaciones de validación en las Aplicaciones, para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.*

ISO 27001:2013: A.14.2.9 Prueba de aceptación de sistemas: *Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas*

de prueba para aceptación y criterios de aceptación relacionados. // **A.17.1.1 Planificación de la continuidad de la seguridad de la información:** *La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa*

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, 2018).
- Definir pruebas y sus KPI (Key Performance Indicator, Indicador clave de rendimiento) para conocer su eficacia de como funcionan y prevenir el control de acceso a los diferentes dispositivos lógicos y físicos y medir la eficacia de los mantenimientos.
- Definir quién es el responsable de cada uno de los elementos físicos y lógicos.

Connotación: Administrativa.

No: 8

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 4: Pérdida de Disponibilidad de la información por daños en la Infraestructura Tecnológica de la Entidad

1) **Actividad de Control Analizada:** PR-033-BACKUP GENERACIÓN Y RECUPERACIÓN
   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.

Diseño del Control: "en la Actividad 5: Restauración Cinta a través de herramienta de BackUp. Tarea de recuperación de Información, a partir de medios de almacenamiento". Menciona la utilización, la cual evidencia desactualización del proceso, ya que en el momento de la auditoria había una solución de software que no requiere cintas.

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 excepciones que hace referencia al Procedimiento de clasificación de la información, el cual no existe en el SIG.

RIESGO 7: Afectación a la disponibilidad, confidencialidad e integridad de la información por abuso de privilegios.

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

Actividad 1: Identificación de medios de procesamiento de información a monitorear. La gestión del riesgo o los siniestros ya materializado nos permiten identificar los procedimientos más críticos sobre los cuales se debe realizar monitoreo, si no se cuenta con un análisis de riesgos se debe generar una muestra, o una selección periódica de los medios de procesamiento que se van a monitorear.

Actividad 2: Análisis de riesgos e identificación de monitoreo a realizar. De acuerdo con los resultados de la evaluación del riesgo o de la muestra tomada de los medios de procesamiento a monitorear se deben definir los siguientes monitoreos:
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 log 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.

Actividad 4: Establecer y hacer seguimiento a actividades preventivas, correctivas y de mejora. 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 excepciones que No se tiene datos al respecto.

RIESGO 8: Afectación a la disponibilidad, confidencialidad e integridad de la información por uso no autorizado de terceros

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

Control 1: Manual MS-013 Manual de Seguridad de la Información.
12.10. Política de Tercerización.

Consideraciones de seguridad con los clientes.
Para los clientes que tienen acceso a los activos de información de la entidad se deben considerar todos los requisitos de seguridad de información internos para que sean aplicados a los clientes, dentro de estos se encuentran las políticas, convenios, acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual entre otros.

A.15.1.1 Política de seguridad de la información para las relaciones con proveedores

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 proceso y la evidencia por los informes de operación, acuerdos de niveles de servicio.

Control 2: 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 3 Organización de la Seguridad de la Información.

Actividad 6: Establecer acuerdos de Confidencialidad
Se deben establecer acuerdos de Confidencialidad con partes interesadas.

A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores

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 excepciones porque se evidenció datos al respecto

RIESGO 11: Pérdida a la Integridad de la Información por fallas en el monitoreo y/o inexistencia de los registros log (Aplicaciones, BD y plataformas tecnológicas)

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

Control 1: 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 3. Organización de la seguridad de la información.

Actividad 3: Documentación de Instrucciones de trabajo.
Controlar la documentación de instrucciones de trabajo para la operación de los componentes de Infraestructura de TI. Desarrollar manuales de responsabilidades detalladas para los administradores de los sistemas de información que incluyan las tareas específicas que debe desarrollar cada Profesional para la operación de los sistemas a su cargo.

A.6.1.1 Roles y responsabilidades para la seguridad de 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 Manejo de excepciones que no es confiable porque al viabilizar los cambios beneficiosos con un mínimo de interrupciones en la prestación de servicios de TI.

RIESGO 12: 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

5) Actividad de Control: PROCEDIMIENTO: RIESGOS DE CORRUPCION

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.

Control A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

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 Manejo de excepciones que no es confiable porque al viabilizar los cambios beneficiosos con un mínimo de interrupciones en la prestación de servicios de TI.

Control 2: Matriz de Riesgos y Controles: La entidad cuenta con Políticas de Seguridad de la Información, así mismo y a través de la SJC y SAF establece acuerdos de confidencialidad en la etapa de vinculación laboral o contractual de personas naturales y jurídicas, y adicionalmente el proceso de Gestión de Seguridad de la información y Recursos Tecnológicos cuenta con una metodología de gestión de incidentes de seguridad informática.

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 5. Seguridad de los Recursos Humanos.

Actividad 2: Elaborar Planes de Capacitación. Elaboración de planes de Capacitación y toma de conciencia en seguridad de la información.

A.7.2.2 Toma de conciencia, educación y formación en la 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 la periocidad se planteaba una fecha prevista para el primer trimestre de 2020 y debilidad en la evidencia que no se encuentra completa.

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, 2018).

Connotación: Administrativa.

Proceso: GESTIÓN CONTRACTUAL
Procedimientos:
PR - 144 Etapa de Planeación Contractual Estudios Previos y Proyecto de Pliego
PR - 145 Etapa de selección y adjudicación
PR - 154 Ejecución y Cierre del Expediente Contractual

Ver **ANEXO 6 – MUESTRA PROCESO GESTION CONTRACTUAL** en archivo Excel_ANEXOS del Informe Final donde se describe la muestra analizada.

No: 9

INOBSERVANCIA DE PRINCIPIOS QUE RIGEN LA CONTRATACIÓN ESTATAL

Responsable de las acciones de mejora: SDAE y SJC

En la muestra seleccionada se evidenció la inobservancia de los principios de planeación y publicidad que rigen la contratación pública así:

1. ***Deficiencias en la planeación que busca suplir la necesidad***

En el proceso de Contratación Directa, que originó el Contrato de prestación de servicios nro. 692 de 2018 con IT GOP S.A.S cuyo objeto es "DESARROLLO DE NUEVAS FUNCIONALIDADES Y PRESTACIÓN DE LOS SERVICIOS DE ACTUALIZACIÓN, SOPORTE, MANTENIMIENTO Y CAPACITACIÓN DEL SISTEMA ADMINISTRATIVO Y FINANCIERO QUE OPERA EL INSTITUTO PARA LA ECONOMÍA SOCIAL - IPES" adjudicado a IT GOP SAS por valor de $160.055.000; se evidenció que la Entidad no planeó adecuadamente la satisfacción de la necesidad, debido a que el sistema documental GOOBI requiere actualización, soporte, mantenimiento permanente.

En ese sentido, la entidad debió proyectar un plazo mayor a los 7 meses en la ejecución del contrato para que, con posterioridad, no se hiciere necesario prorrogar dos veces el contrato, para un total de 8 meses más a los inicialmente pactados, en desatención al principio de planeación Independientemente que el contratista una vez aprobada la adición y prórroga en el SECOP, haya desistido de la segunda prórroga y solicitado la terminación anticipada del contrato.

La anterior afirmación se soporta con base en la solicitud del 26-jun-2019 en donde el supervisor del contrato solicitó prorrogar el mismo por 4 meses más. Por lo tanto, se observa que, tal como se afirmó, la entidad requiere continuidad ininterrumpida de los servicios que presta el contratista.
Ahora bien, teniendo en cuenta que el GOOBI es el sistema de gestión documental de la entidad y este requiere de funcionamiento y atención permanente, desconoce esta auditoría

porque la entidad faltó al deber de planeación y suscribió un contrato inicial por 7 meses, cuando está claro, desde el estudio previo con fecha 23-oct-2018, que:

- *Se requiere dar continuidad al uso del software GOOBI, versión actualizada del aplicativo SIAFI, el cual soporta actualmente la operación Administrativa y Financiera del IPES.*
- *Reviste importancia contar con las versiones más recientes y las actualizaciones que realiza el proveedor.*
- *La empresa IT GOP S.A.S., es la única organización que ofrece el servicio de soporte y actualización de la plataforma GOOBI.*

Igualmente, la entidad debe tener en cuenta que el contrato viene ejecutándose desde el año 2016 de la siguiente manera:

Tabla 9. *Relación de contratos recurrentes suscritos IT-GOP de 2016 a 2020*

ITEM	NUMERO DE CONTRATO	PLAZO INICIAL	PRORROGAS	TIEMPO PRORROGADO	TIEMPO TOTAL	VALOR INICIAL	VALOR TOTAL En pesos COL
1	179 - 2016	6 MESES	6	11 MESES 18 DIAS	17 MESES, 18 DIAS	$ 110,000,000	**$ 162,916,996**
2	516- 2017	7MESES				$ 79,135,000	**$ 79,135,000**
3	692-2018	7 MESES	2	8 MESES	15 MESES	$ 160,055,000	**$ 207,655,000**
4	254-2020	10 MESES				$ 165,267,200	En ejecución

Finalmente, se debe advertir que el desconocimiento del principio de planeación conllevó a la entidad a suscribir dos prórrogas al contrato inicial. Al respecto, esta auditoría reitera que la modificación del contrato estatal, si bien puede ser una herramienta útil para el logro de los fines del Estado y aliviar el impacto fiscal que puede tener 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 las cosas, la modificación debe ser excepcional y debe justificarse en razones autorizadas por la ley y debidamente probadas y fundamentadas.

Lo anterior debido a que la entidad no está plasmando en los estudios previos un cálculo real de la necesidad que efectivamente requiere satisfacer independientemente de si cuenta o no con los recursos su satisfacción, situaciones que podrían llevar a que se realicen modificaciones al contrato previsibles desde el inicio del mismo.

2. ***Deficiencias en la aplicación del Principio de publicidad por ausencia en la publicación de documentos en la plataforma SECOP***

En 6 de 20 contratos de la muestra seleccionada, se evidenció el incumplimiento del principio de publicidad, materializado en la ausencia de la publicación que de los documentos del proceso de selección o del contrato debe realizarse en la Plataforma SECOP, así:

a) PSASI - IPES No. 11-2019, que originó el Contrato 468 de 2019 con SUMINISTROS OBRAS Y SISTEMAS SAS por valor de $157.022.976, el cual fue suscrito con SUMINISTROS OBRAS Y SISTEMAS SAS y cuyo objeto es "*ADQUISICIÓN, CONFIGURACIÓN Y PUESTA EN OPERACIÓN DE UNA SOLUCIÓN INTEGRAL DE BACKUP PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL INSTITUTO PARA LA ECONOMÍA SOCIAL – IPES*": Se evidenció que el Supervisor no publicó ningún informe de seguimiento al contrato o el informe final de supervisión del mismo.

b) En el proceso de Contratación Directa, que originó el Contrato Interadministrativo nro. 416 de 2019 con ETB cuyo objeto es *"PRESTACIÓN DEL SERVICIO DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA ORGANIZACIÓN, DIGITALIZACIÓN, ALMACENAMIENTO EN NUBE, LICENCIAMIENTO DE LA PLATAFORMA DE CONSULTA DE LAS IMÁGENES DIGITALIZADAS Y AJUSTE AL INVENTARIO DOCUMENTAL DEL FONDO DOCUMENTAL ACUMULADO (FONDO DE VENTAS POPULARES) DEL IPES"* por valor de $259.917.170; se evidenció que la Entidad no publicó todos los documentos del proceso en el SECOP. En ese sentido, la entidad debió publicar:

- Estudio previo de necesidad.
- CDP.
- Matriz de riesgos.
- Acto administrativo de justificación de la contratación directa.
- Invitación a presentar propuesta.
- Oferta del convenido.
- RP.
- Acta de aprobación de pólizas.
- Acta de inicio.
- Documento mediante el cual se justifique la adición.
- Informes de supervisión

c) En el proceso de Contratación Directa, que originó el Contrato Interadministrativo nro. 341 de 2020 con ETB cuyo objeto es *"PRESTAR EL SERVICIO INTEGRAL DE TELECOMUNICACIONES (CANALES DEDICADOS, WI-FI, TELEFONÍA) Y SERVICIOS DE TECNOLOGÍA PARA BRINDAR APOYO EN EL CUMPLIMIENTO DE LOS PROCESOS MISIONALES Y ADMINISTRATIVOS A CARGO DE LA ENTIDAD"* por valor de $374.810.350; se evidenció que la Entidad, una vez suscrita el acta de inicio del contrato (13 de mayo de 2020) no ha publicado los documentos del proceso en el SECOP. En ese sentido, la Entidad debió publicar:
- Informes de supervisión

d) En el proceso de Contratación Directa, que originó el Contrato Interadministrativo nro. 729 con ETB de 2019 cuyo objeto es *"PRESTAR EL SERVICIO INTEGRAL DE TELECOMUNICACIONES (CANALES DEDICADOS, WI-FI, TELEFONÍA) Y SERVICIOS DE TECNOLOGÍA PARA BRINDAR APOYO EN EL CUMPLIMIENTO DE LOS PROCESOS MISIONALES Y ADMINISTRATIVOS A CARGO DE LA ENTIDAD"*

por valor de $193.932.700; se evidenció que la Entidad no publicó todos los documentos del proceso en el SECOP. En ese sentido, la entidad debió publicar:

- Estudio previo de necesidad.
- CDP.
- Matriz de riesgos.
- Acto administrativo de justificación de la contratación directa.
- Invitación a presentar propuesta.
- Oferta del convenido.
- RP.
- Acta de aprobación de pólizas.
- Acta de inicio.
- Informes de supervisión

e) En el proceso de Contratación Directa, que originó el Contrato de arrendamiento nro. 297 de 2018 con FAMOC DE PANEL S.A. cuyo objeto es *"ARRENDAMIENTO DEL INMUEBLE UBICADO EN LA CALLE 73 NO. 11-66 PARA LA SEDE DEL INSTITUTO PARA LA ECONOMÍA SOCIAL- IPES, CON EL PROPÓSITO DE DESARROLLAR SUS ACTIVIDADES ADMINISTRATIVAS, OPERATIVAS Y MISIONALES"* por valor de $3.156.148.800; se evidenció que la Entidad no publicó todos los documentos del proceso en el SECOP. En ese sentido, la entidad debió publicar:

- CDP
- Matriz de riesgos
- Modelo de invitación
- RP
- Acta de aprobación de pólizas
- Acta de inicio
- Informes de supervisión

f) En el proceso de Contratación Directa, que originó el Contrato Interadministrativo nro. 729 con ETB de 2019 cuyo objeto es "PRESTAR EL SERVICIO INTEGRAL DE TELECOMUNICACIONES (CANALES DEDICADOS, WI-FI, TELEFONÍA) Y SERVICIOS DE TECNOLOGÍA PARA *BRINDAR APOYO EN EL CUMPLIMIENTO DE LOS PROCESOS MISIONALES Y ADMINISTRATIVOS A CARGO DE LA ENTIDAD"* por valor de $193.932.700; se evidenció que la Entidad no publicó todos los documentos del proceso en el SECOP. En ese sentido, la entidad debió publicar:

- Informes de supervisión.

La anterior situación debido a que, al no ser documentos necesarios para la trazabilidad en la plataforma, suele omitirse su publicación, sin embargo, el no realizarlo acarrea las posibles sanciones al funcionario pues su cumplimiento hace parte del principio de publicidad de todos los documentos de la actividad contractual que rige la contratación estatal.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR – 144 Etapa De Planeación Contractual Estudios Previos y Proyecto de Pliego, presentó el siguiente Diseño de Control:

Control 1: CONTROL 6.1.13: REVISAR ESTUDIOS Y DOCUMENTOS PREVIOS: Revisar los documentos contenidos en la carpeta contractual. Si los estudios están correctos se pasa a la actividad 15 o 16 de la elaboración del proyecto de pliegos, si no, volver a la actividad No.1. Responsable: Profesional de Jurídica y Contratación. (ESTUDIOS PREVIOS).

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 cuanto que no se encuentra documentado en el propósito del control, qué se revisa de los documentos, ni el procedimiento de cómo se hace la revisión de los mismos, así como tampoco la evidencia del control. Cabe señalar que el control indicado no es específico por cada uno de los documentos previos, tales como las cotizaciones, el estudio de sector o el estudio previo, sino que se encuentra descrito en el procedimiento de manera muy general para todos los documentos contenidos en la carpeta contractual, lo que dificulta la especificidad del control y por lo tanto la eficacia en la ejecución del mismo.

El diseño de las actividades de control señaladas en el PR- 154 EJECUCION Y CIERRE DEL EXPEDIENTE CONTRACTUAL se observó así:

Control 2: Control 6.1.8 y 6.1.9 Revisar la carpeta Contractual: Revisar los documentos contenidos en la carpeta contractual. Si los documentos cumplen lo requerido se pasa a la actividad 10. Si no, pasa a la actividad 1 o a la que corresponda Revisar la carpeta Contractual: Revisar los documentos contenidos en la carpeta contractual.
Responsable: Profesional de Jurídica y Contratación. (ESTUDIOS PREVIOS).

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 cuanto que no se encuentra documentado el procedimiento de cómo se hace la revisión de los mismos, así como tampoco la evidencia del control. Cabe señalar que el control indicado no es específico, sino que se encuentra descrito en el procedimiento de manera muy general para todos los documentos contenidos en la carpeta contractual, lo que dificulta la especificidad del control y por lo tanto la eficacia en la ejecución del mismo.

Control 3: No existe documentado en el SIG un control respecto de la publicación a realizar por parte de los supervisores de la documentación de la ejecución del contrato.

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 cuanto que al no encontrarse descrito en el SIG, se requiere establecer control

Valoración comentarios del Auditado

Por parte de la SJC, el auditado argumenta que:

*"**1. DEFICIENCIAS EN LA PLANEACIÓN QUE BUSCA SUPLIR LA NECESIDAD:***
Respecto a esta observación, es importante recordar que es la dependencia que solicita la contratación quien establece la necesidad de contratación definiendo la forma de ejecución y plazo de la misma. Por lo anterior, teniendo en cuenta que la función de la Subdirección Jurídica y de Contratación es la de validar que la misma esté acorde con la normatividad vigente y el Plan Anual de Adquisición, la estructuración de los documentos que soporta la contratación es de la dependencia solicitante. (…)
(…) En consecuencia, se reitera que si bien es cierto que los procesos y procedimientos que rigen la contratación estatal de la Entidad se encuentran en cabeza de la Subdirección Jurídica y de Contratación, la responsabilidad de la estructuración de los documentos que la soportan son responsabilidad de las dependencias solicitantes de la contratación, ya que son éstas las conocedoras de la necesidad que se busca suplir, razón por la cual se solicita se desvincule a la Subdirección Jurídica y de Contratación del presente hallazgo en el informe definitivo.

2.DEFICIENCIAS EN LA APLICACIÓN DEL PRINCIPIO DE PUBLICIDAD POR AUSENCIA EN LA PUBLICACIÓN DE DOCUMENTOS EN LA PLATAFORMA SECOP:
Respecto a la presente observación se informa que en lo referido al contrato No 729 de 2019, se encuentran publicados los siguientes documentos: ACTA DE INICIO, POLIZAS, OFERTA DEL CONVENIO, INVITACION A PROPUESTA, ACTO ADMINISTRATIVO, MATRIZ DE RIESGO, ESTUDIOS PREVIOS, CONTRATO tal y cómo se observa en el archivo en PDF adjunto.

En lo referido al contrato 416 de 2019 se encuentran publicados los siguientes documentos: ACTA DE INICIO, ACTA APROBACION DE POLIZAS, OFERTA DEL COMVENIO, ACTO ADMINISTRATIVO, MATRIZ DE RIESGOS, ESTUDIOS Y DOCUMENTOS PREVIOS, ADICION, CONTRATO INTERADMINISTRATIVO, tal y como se observa en el archivo en PDF adjunto.

Esta Subdirección, respecto a los demás contratos se allana al pronunciamiento consignado en la observación del auditor, por lo que se procederá con la revisión de la publicación de los documentos los documentos en los diferentes contratos, y se adoptaran los correctivos del caso en el plan de mejoramiento que se formulará en su debido momento"

Por parte de SDAE, el auditado argumenta que:

"2. DEFICIENCIAS EN LA APLICACIÓN DEL PRINCIPIO DE PUBLICIDAD POR AUSENCIA EN LA PUBLICACIÓN DE DOCUMENTOS EN LA PLATAFORMA SECOP
Numeral c) En el proceso de Contratación Directa, que originó el Contrato Interadministrativo nro. 341 de 2020: Realizando la verificación en SECOP II número de proceso CDIPES3342020- la información publicada desde el inicio del contrato 341 de 2020 el día 13 de mayo de 2020, a la fecha se han publicado dos facturas y sus correspondientes informes y soportes de supervisión, como se evidencia en la siguiente imagen: (se adjunta pantallazo del SECOP de las facturas de agosto y septiembre de 2020).

Por tanto, se considera que no se está incumpliendo el principio de publicidad, ya que en la medida que se realizan los pagos y la información esté disponible, se realiza la publicación por parte del proveedor y la aceptación por parte de la supervisión. Es de aclarar que si bien el Contratista tiene atrasada la publicación del tercer pago, por parte de la supervisión se han realizado los requerimientos correspondientes para lograr que la información se publique en cada reunión de

seguimiento mensual como se puede observar en las actas de reuniones publicadas en SECOPII y mediante correo electrónico.

Numeral d). En el proceso de Contratación Directa, que originó el Contrato Interadministrativo nro.729 con ETB de 2019: Por parte de la Subdirección de Diseño y Análisis Estratégico se remitieron todos los documentos necesarios en ejercicio del proceso de contratación en mención mediante el radicado 00110-817-012349 del 03/12/2019, siendo responsabilidad de la Oficina Jurídica y de contratación la publicación de los documentos dentro de la plataforma SECOP I. Realizando la revisión en SECOP I número de proceso 729-2019 donde se encuentra publicado el contrato se evidencian los siguientes soportes a la fecha: (adjunta pantallazo del SECOP I)"

Respecto de la solicitud realizada por la SJC de "se desvincule a la Subdirección Jurídica y de Contratación del presente hallazgo en el informe definitivo", es menester aclarar que no es posible acceder a dicha solicitud, por cuanto tal como lo señalo la SJC, los procesos y procedimientos que rigen la contratación estatal de la Entidad se encuentran en cabeza de la Subdirección Jurídica y de Contratación, por tanto si bien es cierto que el numeral 1 de la observación, se centra en las deficiencias encontradas en el estudio previo, el cual es responsabilidad del área que llevó a cabo su elaboración, no es menos cierto que los controles que deben existir en los procesos y procedimientos se encuentran en cabeza de la SJC, por lo tanto y en vista que la SDAE no aportó argumentación o evidencia que desvirtúe lo manifestado en el informe preliminar, respecto del presente numeral, se mantiene la observación en cabeza de ambas áreas en lo que a cada quien corresponda.

Respecto del contrato nro. 729 de 2019, una vez verificada la plataforma SECOP I se advierte que los estudios previos, el CDP, la matriz de riesgo, la resolución de justificación de la contratación directa, la invitación a presentar propuesta, la oferta del convenido, el Registro presupuestal, las garantías y el acta de inicio; fueron publicadas por la entidad con fecha 27/10/2020.

Igual situación acontece con los documentos correspondientes al contrato nro. 416 de 2019, en donde la información fue publicada en la misma fecha, es decir, en términos donde ya se encontraba la auditoria en ejecución.

Así mismo, es importante aclarar que el traslado del informe preliminar que se le brinda al auditado no es para subsanar situaciones pasadas sino, por el contrario, pronunciarse sobre las evidenciadas al momento en que la ACI hace el corte y remite el informe en comento.

Respecto del contrato Interadministrativo nro. 341 de 2020, sea lo primero resaltar que el contrato suscrito es de ejecución tracto sucesiva, es decir, que las obligaciones se cumplen mes a mes y, en ese sentido, la labor de supervisión se cumple por el mismo periodo de tiempo.

Por otro lado, afirma la entidad que "en la medida que se realizan los pagos y la información esté disponible, se realiza la publicación por parte del proveedor y la aceptación por parte de la supervisión." No obstante, es importante aclarar que, tal como se advirtió en el párrafo anterior, la labor de supervisión se realiza mes a mes y, de conformidad con el contrato, el plazo de ejecución corresponde a 10 mensualidades, razón por la cual no encuentra

justificación esta auditoría del porqué, transcurrido casi el 50 % del plazo de ejecución, la entidad no contaba con informes de supervisión aprobados.

Finalmente es importante aclarar que el traslado del informe preliminar que se le brinda al auditado no es para subsanar situaciones pasadas sino, por el contrario, pronunciarse sobre las evidenciadas al momento en que la ACI hace el corte y remite el informe en comento. Lo anterior, precisamente, debido a que con fecha 27 y 28 de octubre del presente año fueron publicados los informes nro. 3, 4 y 5.

Se adjunta evidencia:

Facturas del contrato

Id de pago	Número de factura	Código de autorización	Fecha de expedición	Fecha de recepción
2	000281984056	-	15/09/2020 12:48 PM (UTC -5 horas)	15/09/2020 12:48 PM (UTC -5
1	000280983820	-	5/08/2020 10:16 AM (UTC -5 horas)	5/08/2020 10:16 AM (UTC -5
3	7757116401	-	27/10/2020 10:22 AM (UTC -5 horas)	27/10/2020 10:22 AM (UTC -5
4	000283659924	-	28/10/2020 11:20 PM (UTC -5 horas)	28/10/2020 11:20 PM (UTC -5
5	000284121192	-	28/10/2020 11:27 PM (UTC -5 horas)	28/10/2020 11:27 PM (UTC -5

Documentos de ejecución del contrato

Descripción	Nombre del documento
Acta Inicio ETB 341-2020.pdf	Acta Inicio ETB 341-2020.pdf
Correo Soporte- REGISTRO PRESUPUESTAL 696 DE 2020 ETB.pdf	Correo Soporte- REGISTRO PRESUPUESTAL 696 DE 2020 ETB.pd
RP 696 ETB (1).pdf	RP 696 ETB (1).pdf

Por lo manifestado de forma precedente esta auditoría mantiene el hallazgo.

Riesgo Asociado: Afectación en la transparencia del proceso de contratación por la inobservancia de los principios que orientan la contratación Estatal. Adelantar procesos de contratación, suscribir y ejecutar contratos sin la observancia de los principios rectores.

1. Deficiencias en la aplicación del Principio de planeación que busca suplir la necesidad de la entidad.

Ley 80 de 1993: Artículo 26 – Del Principio de Responsabilidad. *En virtud de este principio:*
1) Los servidores públicos están obligados a buscar el cumplimiento de los fines de la contratación, a vigilar la correcta ejecución del objeto contratado y a proteger los derechos de la Entidad, del contratista y de los terceros que puedan verse afectados por la ejecución del contrato.
2) Los servidores públicos responderán por sus actuaciones y omisiones antijurídicas y deberán indemnizar los daños que se causen por razón de ellas.
3) Las Entidades y los servidores públicos, responderán cuando hubieren abierto licitaciones o concursos sin haber elaborado previamente los correspondientes pliegos de

condiciones, términos de referencia, diseños, estudios, planos y evaluaciones que fueren necesarios, o cuando los pliegos de condiciones o términos de referencia hayan sido elaborados en forma incompleta, ambigua o confusa que conduzcan a interpretaciones o decisiones de carácter subjetivo por parte de aquellos.

Ley 1437 de 2011; Artículo 3 - Principios. *(...) Las actuaciones administrativas se desarrollarán, especialmente, con arreglo a los principios del debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad.*

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.*

Corte Constitucional, Sentencia C300 de 2012. M P. Jorge Ignacio Pretelt Chaljub. Expediente D-8699: *"2.6.4. Ahora bien, como se indicó en ese concepto, el que la mutabilidad de los contratos estatales sea posible no significa que pueda llevarse a cabo por la mera voluntad de las partes o de la entidad contratante; por el contrario, la modificación del contrato debe ser excepcional en virtud de los principios de planeación y seguridad jurídica."*

CONSEJO DE ESTADO SALA DE LO CONTENCIOSO ADMINISTRATIVO SECCIÓN TERCERA SUBSECCION B Consejera ponente: 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 pre factibilidad 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.

PR-144 ETAPA DE PLANEACION CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO: CONTROL 6.1.13: REVISAR ESTUDIOS Y DOCUMENTOS PREVIOS: *Revisar los documentos contenidos en la carpeta contractual. Si los estudios están correctos se pasa a la actividad 15 o 16 de la elaboración del proyecto de pliegos, si no, volver a la actividad No.1.*Responsable: Profesional de Jurídica y Contratación. (ESTUDIOS PREVIOS).

PR-145 ETAPA DE SELECCIÓN Y ADJUDICACION: CONTROL ACTIVIDAD DE CONTROL 2 REVISAR Y APROBAR O RECHAZAR RESOLUCION DE APERTURA Y PLIEGO DE CONDICIONES DEFINITIVO: *El subdirector jurídico y de contratación revisa y aprueba o rechaza el contenido de la resolución de apertura, pliego de condiciones y su complemento a través de del flujo de aprobación en la plataforma del SECOP II.*

2. Deficiencias en la aplicación del Principio de publicidad por ausencia en la publicación de documentos en la plataforma SECOP

Ley 1437 de 2011; Artículo 3 - Principios. (...)
Las actuaciones administrativas se desarrollarán, especialmente, con arreglo a los principios del debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad.

Decreto 1082 de 2015; Artículo 2.2.1.1.1.3.1. *Definiciones.* *Los términos no definidos en el Título I de la Parte 2 del presente decreto y utilizados frecuentemente deben entenderse de acuerdo con su significado natural y obvio. (…)*

Documentos del Proceso son: *(a) los estudios y documentos previos; (b) el aviso de convocatoria; (c) los pliegos de condiciones o la invitación; (d) las Adendas; (e) la oferta; (f) el informe de evaluación; (g) el contrato; y cualquier otro documento expedido por la Entidad Estatal durante el Proceso de Contratación. (Subrayas por fuera del texto original).*

DECRETO 1082 DE 2015; Artículo 2.2.1.1.1.7.1 – Publicidad en el SECOP. La Entidad Estatal está obligada a publicar en el SECOP los Documentos del Proceso y los actos administrativos del Proceso de Contratación, dentro de los tres (3) días siguientes a su expedición.

Ley 1150 de 2007; Artículo 2, Numeral 5, Parágrafo 4 - *De las modalidades de contratación. "El procedimiento aplicable para la ejecución de cada una de las causales a que se refiere el numeral 2o del presente artículo, deberá observar los principios de transparencia, economía, responsabilidad y las siguientes reglas: 1) Se dará publicidad a todos los procedimientos y actos. (...)*

PR-145 ETAPA DE SELECCIÓN Y ADJUDICACION: *En cada etapa incluye actividades de control relacionadas con la publicación oportuna en la plataforma del SECOP II,*

señaladas en las actividades 6.1.2, 6.1.4, 6.1.8, 6.1.14; 6.1.15, 6.1.23, 6.1.27, 6.1.33, 6.1.35.

PR-154 EJECUCION Y CIERRE DEL EXPEDIENTE CONTRACTUAL: *En cada etapa de la ejecución incluye actividades de control relacionadas con la publicación oportuna en la plataforma del SECOP II, señaladas en las actividades 6.1.4, 6.1.5, 6.1.10, 6.1.13, 6.1.18, 6.1.29, 6.1.33, 6.1.34, 6.1.36.*

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, 2018).
- Incluir especialmente, en los procedimientos PR 144, PR 145, PR 146, PR 152, PR 153 y PR 154, controles que contengan los 6 elementos del diseño de control con sus respectivas explicaciones (Responsable, Periodicidad, Propósito, Cómo se hace, Excepciones o Desviaciones, Evidencia) donde se permita verificar la aplicación de los principios que rigen la contratación estatal en cada una de las etapas del proceso de contratación desde la precontractual, hasta la postcontractual; bien sea mediante la inclusión de dicha revisión como actividad en los controles ya existentes o mediante la creación de un control nuevo para tal fin
- Establecer en los estudios previos la necesidad real que la entidad desea satisfacer con la presente contratación para lo cual, se debe tener en cuenta el objeto a contratar y el histórico que contratos con el mismo objeto se han ejecutado en el IPES, de ese modo, al establecer el plazo del contrato, este debe tener relación con la satisfacción real de la entidad; si existen razones económicas, técnicas o jurídicas, que no permitan llevar a cabo la contratación satisfaciendo al 100% la necesidad, dejar plasmada esas circunstancias en el estudio previo.
- Modificar el PR -154, e incluir en el acápite 6.1 **"TABLA EXPLICATIVA DEL PROCEDIMIENTO**", los 6 elementos del diseño de control con sus respectivas explicaciones (Responsable, Periodicidad, Propósito, Cómo se hace, Excepciones o Desviaciones, Evidencia. Respecto de la revisión o verificación que debe existir en el cumplimiento por parte del Supervisor de las obligaciones establecidas en los procedimientos del IPES, en especial lo referido a la publicación de la documentación de la ejecución contractual en la Plataforma del SECOP, atendiendo para ello lo establecido en el Ciclo PHVA (Planificar, Hacer, Verificar y Actuar)
- Publicar en el SECOP todos los documentos del contrato incluyendo los relativos a la ejecución del mismo.

Connotación: Administrativa.

No: 10

INOBSERVANCIA NORMATIVA EN LA ETAPA POSTCONTRACTUAL

Responsable de las acciones de mejora: SDAE Y SJC

En la muestra seleccionada se evidenció que la entidad no ha realizado las actividades requeridas una vez vencido el plazo del contrato, tales como las liquidaciones y el cierre del expediente en los casos que aplique así:

1. ***Falta de cierre del expediente***

En 1 de 20 contratos de la muestra seleccionada, se evidenció el incumplimiento de la actividad post-contractual de cierre del expediente así:

En el proceso de Selección abreviada por Subasta Inversa Nro. PSASI - IPES No. 11-2019, que originó el Contrato 468 de 2019 con SUMINISTROS OBRAS Y SISTEMAS SAS por valor de $157.022.976, el cual fue suscrito con SUMINISTROS OBRAS Y SISTEMAS SAS y cuyo objeto es "*ADQUISICIÓN, CONFIGURACIÓN Y PUESTA EN OPERACIÓN DE UNA SOLUCIÓN INTEGRAL DE BACKUP PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL INSTITUTO PARA LA ECONOMÍA SOCIAL – IPES*, se observó que una vez finalizado el contrato y expirada la vigencia fijada en la Garantía única para el amparo de calidad, la Entidad no suscribió el Acta de Cierre de Expediente, situación que desconoce lo ordenado por el Decreto 1082 de 2015.

Esta situación se presentó por la inaplicación de las obligaciones en la etapa post-contractual, lo que pudo ocasionar sanciones para el funcionario responsable de realizar el cierre del proceso.

2. ***Inexistencia suscripción acta de liquidación***

En 3 de 20 contratos de la muestra seleccionada, se evidenció el incumplimiento de la actividad post-contractual de liquidación del contrato así:

a) En el proceso de Selección abreviada por Subasta Inversa nro. PSASI - IPES No. 11-2019, que originó el Contrato 468 de 2019 con SUMINISTROS OBRAS Y SISTEMAS SAS por valor de $157.022.976, el cual fue suscrito con SUMINISTROS OBRAS Y SISTEMAS SAS y cuyo objeto es "ADQUISICIÓN, CONFIGURACIÓN Y PUESTA EN OPERACIÓN DE UNA SOLUCIÓN INTEGRAL DE BACKUP PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL INSTITUTO PARA LA ECONOMÍA SOCIAL – IPES", se observó que el contrato finalizó el 08/01/2020, información que se confirma con la suscripción del acta de inicio . Sin embargo, cuatro (4) meses después de la finalización del contrato, la Entidad no ha suscrito el acta de liquidación correspondiente. Esta situación contraviene lo establecido en el artículo 11 de la Ley 1150 de 2007.

b) En el proceso de Contratación Directa, que originó el Contrato Interadministrativo nro. 594 de 2018 con ETB cuyo objeto es "PRESTACIÓN DEL SERVICIO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL QUE PERMITA LA ORGANIZACIÓN Y DIGITALIZACIÓN DE ARCHIVOS DEL IPES" por valor de $299.994.152; se observó que la entidad no ha realizado la liquidación del

contrato, teniendo en cuenta que el mismo finalizó el día 02 de diciembre de 2019 y acorde con el numeral 2.2.9 del Estudio previo, el término estipulado para dicho trámite era de 4 meses siguientes a la terminación del contrato.

c) En el proceso de Contratación Directa, que originó el Contrato Interadministrativo nro. 692 de 2018 con IT GOP S.A.S cuyo objeto es "DESARROLLO DE NUEVAS FUNCIONALIDADES Y PRESTACIÓN DE LOS SERVICIOS DE ACTUALIZACIÓN, SOPORTE, MANTENIMIENTO Y CAPACITACIÓN DEL SISTEMA ADMINISTRATIVO Y FINANCIERO QUE OPERA EL INSTITUTO PARA LA ECONOMÍA SOCIAL - IPES" por valor de $160.055.000, se observó que la entidad no ha realizado la liquidación del contrato, teniendo en cuenta que el mismo finalizó el día 28 de Octubre de 2019, según consta en la terminación anticipada del mismo y acorde con el numeral 2.2.9 del Estudio previo, el término estipulado para dicho trámite era de 4 meses siguientes a la terminación del contrato.

3. Acta de liquidación por fuera de término

En el proceso de Contratación Directa, que originó el Contrato de arrendamiento nro. 297 de 2018 con FAMOC DE PANEL S.A. cuyo objeto es "ARRENDAMIENTO DEL INMUEBLE UBICADO EN LA CALLE 73 NO. 11-66 PARA LA SEDE DEL INSTITUTO PARA LA ECONOMÍA SOCIAL- IPES, CON EL PROPÓSITO DE DESARROLLAR SUS ACTIVIDADES ADMINISTRATIVAS, OPERATIVAS Y MISIONALES" por valor de $3.156.148.800; se observó que la liquidación del contrato se suscribió el 12 de septiembre de 2019, cuando el plazo máximo legal era el 28 de mayo de 2019.

En todo caso, la Entidad debió ampliar el plazo que cubría la garantía, pues de conformidad con el Decreto 1082 de 2015 esta debe tener una vigencia mínima hasta la liquidación del contrato.

Esta situación se presentó por la inaplicación de las obligaciones en la etapa pos-contractual, lo que pudo ocasionar sanciones para el funcionario responsable de realizar el cierre del proceso.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el PR- 154 EJECUCION Y CIERRE DEL EXPEDIENTE CONTRACTUAL se observó así:

Control 1: ACTIVIDAD DE CONTROL 6.1 TABLA EXPLICATIVA DEL PROCEDIMIENTO 33: El/la Profesional de la SCJ diligenciará en la plataforma del SECOP II la justificación del cierre del expediente contractual en la sección "MODIFICCION DEL CONTRATO" publicando los documentos que soportan la solicitud. VER condiciones generales. El/la profesional de la Subdirección Jurídica y de Contratación. si no se aprueba la modificación, se devuelve para que el profesional jurídico justifique nuevamente el cierre del expediente.

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 que el control cumple con los parámetros para su diseño.

Control 2: PR- 154 EJECUCION Y CIERRE DEL EXPEDIENTE CONTRACTUAL ACTIVIDAD DE CONTROL No.6.1.32 REVISAR COMPONENTE JURIDICO DE LA LIQUIDACION: El /la Profesional de la SJC efectuará la Revisión del componente jurídico del acta de liquidación. Una vez se encuentre debidamente ajustada el/la profesional designado/a por la SJC dará su visto bueno en el formato y procederá a remitir el acta a él/la supervisor/a para la revisión y suscripción del contratista, el/la subdirector/a Administrativo/a y Financiero/a del contrato. Surtido lo anterior el/la Supervisor/a del contrato allegará a la SJC el acta de liquidación para la suscripción por parte de él/la Subdirector/a Jurídico/a y de contratación; posteriormente el Profesional de la SJC incorporará la fecha del acta.

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 que el control cumple con los parámetros para su diseño.

Valoración comentarios del Auditado

Por parte de la SJC, el auditado argumenta que:

> *"Respecto a este punto, es menester recordar que el artículo 11 de la Ley 1150 de 2007 establece que: (Se cita la norma)*
> *En atención a lo anterior, el primer párrafo del precitado artículo solo habla de la liquidación de mutuo acuerdo, estableciendo un término de 4 meses para la liquidación de aquellos contratos en los que no se estableció un término específico dentro del pliego de condiciones o sus equivalentes, siendo este el único término que se puede concertar con el contratista.*
>
> *De igual manera, el mismo artículo establece dos términos adicionales para la liquidación de los contratos, sin que estos puedan ser suprimidos al haberse establecido el plazo antes mencionado así:* ***a.*** *2 meses para liquidación del contrato de manera unilateral y,* ***b.*** *2 años para la liquidación de mutuo acuerdo o unilateral; estableciendo un plazo total de 30 meses para la liquidación de los contratos.*
>
> *Por lo anterior, es menester precisar que el único término que es facultativo para la Entidad y para el contratista es el establecido para realizar la liquidación de mutuo acuerdo, toda vez que los 26 meses restantes para la liquidación de los contratos son reglados y vinculante para las Entidades públicas.*
>
> *Ahora bien, dando aplicación al último párrafo del precitado artículo si vencido el plazo establecido para la liquidación de mutuo acuerdo y unilateral ésta no se ha realizado, la misma podrá ser hacer en cualquier tiempo dentro de los dos años siguientes, razón por la cual la Entidad se encuentra dentro del término legal establecido para la liquidación de los contratos auditados.*
>
> *De igual manera, se recuerda que el artículo 2.2.1.2.3.1.12 del Decreto 1082 de 2015 establece que la garantía de cumplimiento del contrato debe tener una vigencia mínima hasta la liquidación*

del contrato, siendo responsabilidad del contratista mantener vigente la garantía hasta el término antes mencionado.

En consecuencia, se solicita se retire la observación presentada y se desvincule a la Subdirección Jurídica y de Contratación del presente hallazgo en el informe definitivo.

Por parte de la SDAE:

Respecto del literal b) Contrato Interadministrativo nro.356 de 2018 con ETB: El proceso de liquidación del contrato 356 de 2018 se viene adelantando de común acuerdo con la empresa ETB, durante los 4 meses correspondientes del 13 de diciembre de 2019 al 13 de abril de 2020 realizando las siguientes acciones dentro del tiempo establecido y de acuerdo al MS-012 MANUAL DE CONTRATACION, SUPERVISIÓN E INTERVENTORIA "La liquidación de los contratos se realizará de mutuo acuerdo dentro del término fijado o dentro del que acuerden las partes para el efecto" :

- *Se realizaron las reuniones respectivas para revisar que todos los servicios se entregarán a satisfacción de las dos partes.*
- *Una vez se llegó a un acuerdo mutuo se expidió por parte del proveedor ETB la última factura de pago con Nro. de radicado 00110-812-002787 del 26/02/2020.*
- *Por parte de la supervisión del contrato se procede a elaborar el Acta de liquidación para lo cual se debe subsanar algunos temas en SECOPII y organizar toda la documentación respectiva para la revisión de SAF.*
- *Una vez se cuenta el visto bueno por parte de SAF con respecto al Acta de liquidación se procede a enviar el documento a la ETB para su respectiva firma mediante correo electrónico del 03/04/2020 al correo dispuesto por el proveedor liquidaciones_etb@etb.com.co por motivos de la contingencia.*

Cabe señalar que en el contrato que nos ocupa, una vez se terminó el plazo de ejecución contractual se dio inicio a los trámites pertinentes a fin de suscribir la liquidación bilateral del contrato con ETB, pero a raíz de las múltiples dificultades y retrasos que han sufridos las actuaciones administrativas en el país a causa de la Pandemia ocasionadas por el COVID 19 el contratista aún no ha remitido el acta de liquidación debidamente firmada.
No obstante, a lo anterior, se han sostenido varias reuniones virtuales con el objetivo de aclarar dudas y fijar aspectos fundamentales para llevar a buen fin la liquidación bilateral, pero esto no ha sido posible y por ello se les informó que se realizará la liquidación unilateral.
En constancia de lo anterior, nos permitimos remitir los soportes de las gestiones realizadas ante la ETB y nos permitimos informar que se está en la preparación de los documentos necesarios para radicar ante la SJC la liquidación unilateral.
Vale la pena aclarar que la liquidación de un contrato estatal se puede realizar sin pérdida de competencia hasta un término de 30 meses contados a partir de la suscripción del mismo, por lo que no existiría una inoperancia normativa en la etapa postcontractual debido a que en algunos casos, existen inconvenientes administrativos de facturación de consecución de firmas, de cambios en la operación de las empresas contratistas y pesé a las actuaciones administrativas adelantadas por la entidad no es posible cumplir con el plazo inicial, hay que tener en cuenta situaciones como trámites ante la secretaría de hacienda, ajustes en saldos, entre otros.
Con relación a la observación "El proceso de Contratación Directa, que originó el Contrato Interadministrativo nro. 692 de 2018 con IT GOP S.A.S cuyo objeto es "DESARROLLO DE NUEVAS FUNCIONALIDADES Y PRESTACIÓN DE LOS SERVICIOS DE ACTUALIZACIÓN,SOPORTE, MANTENIMIENTO Y CAPACITACIÓN DEL SISTEMA ADMINISTRATIVO Y FINANCIERO QUE OPERA EL INSTITUTO PARA LA ECONOMÍA SOCIAL - IPES" por valor de $160.055.000, se observó que la entidad no ha realizado la liquidación del contrato, teniendo en cuenta que el mismo finalizó el día 28 de Octubre de 2019, según consta en la terminación anticipada del mismo y acorde con el numeral 2.2.9 del Estudio previo, el término estipulado para dicho trámite era de 4 meses siguientes a la terminación del contrato", no se contempla por parte de la ACI, que el contrato fue objeto de una terminación anticipada, razón que cambia sus condiciones iniciales.

La Auditoría efectúa el siguiente análisis:

Sea lo primero advertir que la suscripción y publicación del acta de liquidación dentro de los 4 meses siguientes a la terminación del plazo de ejecución es de contenido objetivo y final, con base en las obligaciones contractuales acordadas por las partes y que en todos los casos de la presente observación se encuentran estipulados por la entidad en los estudios previos, razón por la cual, si dentro de ese periodo de tiempo no se ha suscrito ni publicado la misma, se está desconociendo expresamente la obligación de que trata el art 11 de la Ley 1150 que versa: "***ARTÍCULO 11. DEL PLAZO PARA LA LIQUIDACIÓN DE LOS CONTRATOS.*** *La liquidación de los contratos se hará de mutuo acuerdo dentro del término fijado en los pliegos de condiciones o sus equivalentes, o dentro del que acuerden las partes para el efecto."* más allá que la ley consagre un término adicional para proceder con la suscripción del referido documento.

Por otro lado, la terminación anticipada no deja de ser un evento mediante el cual se materializa la finalización de un contrato. Así pues, una vez verificada esta condición empieza a correr para la entidad el término para suscribir el acta de liquidación. Así las cosas, no se están modificando las condiciones iniciales, pues, dicho sea de paso, la adición contractual es una excepción y no una regla general y, por tanto, la entidad conocía la fecha de finalización del contrato desde el momento mismo de la suscripción del negocio jurídico.

En ese sentido, se debe aclarar que la observación está orientada al desconocimiento de la obligación contractual y no al término fijado en la norma legal que regula el acto administrativo de liquidación.

Ahora bien, los plazos establecidos en el artículo 11 de la Ley 1150 de 2007 tienen una particularidad. Para el término de 2 meses, posteriores a las 4 iniciales, requieren que la entidad haya convocado o notificado al contratista para que se presentara a la liquidación del contrato o que, habiendo cumplido estos dos requisitos, el contratista no se hubiere presentado a suscribir, situaciones que no fueron evidenciadas en auditoria ni en la réplica excepto en el caso del contrato 356 de 2018.

Por lo expresado, la observación se modifica, retirando de la misma el literal b) del numeral 2, sobre el contrato 356 de 2018 y en los demás aspectos se mantiene.

Riesgo Asociado: Detrimento patrimonial por deficiencias en la etapa pos contractual: Suscribir el Acta de liquidación sin que la misma refleje el estado final del contrato y/o no se lleve a cabo la liquidación del contrato en los casos en que amerite

LEY 80 DE 1993; Artículo 60 – De Su Ocurrencia y Contenido. Modificado por el art. 217, Decreto Nacional 019 de 2012. *Los contratos de tracto sucesivo, aquéllos cuya ejecución o cumplimiento se prolongue en el tiempo y los demás que lo requieran, serán objeto de liquidación de común acuerdo por las partes contratantes, procedimiento que se efectuará dentro del término fijado en el pliego de condiciones o términos de referencia o, en su defecto a más tardar antes del vencimiento de los cuatro (4) meses siguientes a la*

finalización del contrato o a la expedición del acto administrativo que ordene la terminación, o a la fecha del acuerdo que la disponga.

Ley 1150 de 2011; Artículo 11. Del plazo para la liquidación de los contratos. *La liquidación de los contratos se hará e mutuo acuerdo dentro del término fijado en los pliegos de condiciones o sus equivalentes, o dentro del que acuerden las partes para el efecto. De no existir tal término, la liquidación se realizará dentro de los cuatro (4) meses siguientes a la expiración del término previsto para la ejecución del contrato o a la expedición del acto administrativo que ordene la terminación, o a la fecha del acuerdo que la disponga.*
Decreto 1082 de 2015; Artículo 2.2.1.1.2.4.3. Obligaciones posteriores a la liquidación. *Vencidos los términos de las garantías de calidad, estabilidad y mantenimiento, o las condiciones de disposición final o recuperación ambiental de las obras o bienes, la Entidad Estatal debe dejar constancia del cierre del expediente del Proceso de Contratación.*

PR- 154 EJECUCION Y CIERRE DEL EXPEDIENTE CONTRACTUAL ACTIVIDAD DE CONTROL No.6.1.32 REVISAR COMPONENTE JURIDICO DE LA LIQUIDACION: *El /la Profesional de la SJC efectuará la Revisión del componente jurídico del acta de liquidación. Una vez se encuentre debidamente ajustada el/la profesional designado/a por la SJC dará su visto bueno en el formato y procederá a remitir el acta a él/la supervisor/a para la revisión y suscripción del contratista, el/la subdirector/a Administrativo/a y Financiero/a del contrato. Surtido lo anterior el/la Supervisor/a del contrato allegará a la SJC el acta de liquidación para la suscripción por parte de él/la subdirector/a Jurídico/a y de contratación; posteriormente el Profesional de la SJC incorporará la fecha del acta.*

R- 154 EJECUCION Y CIERRE DEL EXPEDIENTE CONTRACTUAL ACTIVIDAD DE CONTROL 6.1 TABLA EXPLICATIVA DEL PROCEDIMIENTO 33: *El/la Profesional de la SCJ diligenciará en la plataforma del SECOP II la justificación del cierre del expediente contractual en la sección "MODIFICCION DEL CONTRATO" publicando los documentos que soportan la solicitud. VER condiciones generales. El/la profesional de la Subdirección Jurídica y de Contratación. Si no se aprueba la modificación, se devuelve para que el profesional jurídico justifique nuevamente el cierre del expediente*

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, 2018).
- Ejecutar lo establecido en el PR -154, CONTROL 6.1 TABLA EXPLICATIVA DEL PROCEDIMIENTO 33.
- Establecer un Control con el cumplimiento de los 6 elementos (Responsable, Periodicidad, Propósito, Procedimiento, Manejo de excepciones o desviaciones y Evidencia de la ejecución del control), que permita al área responsable detectar aquellos contratos que una vez cumplidos los requisitos, deba realizarse el debido cierre del expediente y ejecutar el control No. 6.1.33 del PR-154.

- Establecer el plazo para llevar a cabo la liquidación bilateral del contrato en términos que la entidad, acorde con la experiencia y los datos históricos, realmente puede llevarla a cabo.
- Llevar a cabo la liquidación bilateral del contrato, en los términos estipulados en el estudio previo, pliego de condiciones o en el cuerpo del contrato, según sea el caso, y de no ser posible la realización de la liquidación en dicho término, se debe dejar la evidencia de la gestión realizada con el contratista

Connotación: Administrativa.

No: 11

DEFICIENCIAS EN LOS DOCUMENTOS PREVIOS DEL PROCESO DE CONTRATACIÓN

Responsable de las acciones de mejora: SDAE

1. Deficiencias técnicas en los documentos previos

En 1 de 9 contratos de la muestra seleccionada, se evidenciaron deficiencias en la justificación técnica de los requerimientos solicitados en el contrato así:

1) En el contrato NO.3 DE 2019 con FAMOC DE PANEL S.A. cuyo objeto era "*ARRENDAMIENTO DEL INMUEBLE UBICADO EN LA CALLE 73 NO. 11-66 PARA LA SEDE DEL INSTITUTO PARA LA ECONOMÍA SOCIAL- IPES, CON EL PROPÓSITO DE DESARROLLAR SUS ACTIVIDADES ADMINISTRATIVAS, OPERATIVAS Y MISIONALES*." Se evidenció una modificación en los requerimientos técnicos del contrato respecto del contrato 297 de 2018 con el mismo contratista, sin que exista documento que técnicamente soporte dichos cambios, máxime cuando el valor del contrato no sufrió disminución alguna tales como:

- Disminución en la cantidad de cámaras IP requeridas de 32 a 7.
- Disminución en la cantidad de DVR pasando de 2 a 1.
- Disminución de la kVA de la UPS del DATA CENTER de 30 a 10 kVA.

Lo anterior debido a que en los estudios previos no se señaló con claridad y de manera técnica la justificación de los bienes y servicios a solicitar por parte del contratista en las calidades y cantidades allí señalas, lo que podría ocasionar una deficiencia en la prestación del servicio por parte del contratista.

2. *Deficiencias en el estudio de mercado*

En el proceso de Contratación Directa, que originó el Contrato de arrendamiento NO. 3 de 2019 con FAMOC DE PANEL S.A. cuyo objeto es "ARRENDAMIENTO DEL INMUEBLE UBICADO EN LA CALLE 73 NO. 11-66 PARA LA SEDE DEL INSTITUTO PARA LA

ECONOMÍA SOCIAL- IPES, CON EL PROPÓSITO DE DESARROLLAR SUS ACTIVIDADES ADMINISTRATIVAS, OPERATIVAS Y MISIONALES", por valor de $3.256.514.332; se observó que la Entidad

Con ocasión de este estudio, la entidad elaboró el documento titulado "Análisis y Comparación de los Bienes Inmuebles". En el referido documento informa que

> *"Sin perjuicio de lo anterior, el Instituto para la Economía Social - IPES, para la vigencia 2019, realizó una búsqueda de inmuebles de similares características al que actualmente ocupa, dentro de la zona geográfica de la Ciudad donde actualmente tiene su sede administrativa, a efectos de examinar de manera objetiva las condiciones actuales del mercado, estudio que arrojó los siguientes resultados."*

Continúa el documento afirmando: (…), se realizó el recorrido por el cuadrante, encontrando las ofertas que a continuación se relacionan; (…)".

Sin embargo, es importante indicar que las ofertas recibidas no son comparables entre sí, teniendo en cuenta las necesidades reales del IPES en cuanto al área requerida. En ese sentido, la entidad comparó las siguientes ofertas:

Oferta No.	Dirección	Área arrendada (m2)	Canon arrendamiento	Parqueaderos	Mobiliario	Observaciones
1	Calle 72 con Carrera 12	2400	$ 100.000.000	16	No	Cableado estructurado, el edificio es de 12 pisos y cada piso tiene un área de 200 m2, la oferta de alquiler no incluye mobiliario ni adecuación de infraestructura tecnológica.
2	Calle 76 No. 10-12	1060	$ 45.000.000	12	No	Casa de conservación, se podrían adecuar 70 puestos de trabajo, máximo.
3	Calle 76 No. 10 - 28	700	$ 37.000.000	20	No	Área construida de 500 m2

Ahora bien, la misma entidad advirtió que las ofertas no cumplían con los requerimientos ya que:

> *"1. Ninguno cuenta con el área mínima requerida por parte del Instituto, es decir por lo menos 3600 M2.*
> *2. Ninguno ofrece la opción de alquilar el mobiliario que incluya puestos de trabajo diseñados, distribuidos y adecuados en virtud del cumplimiento de la normatividad actual relacionada con salud ocupacional, (…).*
> *3. No cuentan con la adecuación en cuanto a infraestructura tecnológica. (…).*
> *4. No cuentan con áreas como enfermería, sala de capacitación, centro de monitoreo, entre otros. (…)*
> *5. Ninguno tiene la capacidad de alojar la totalidad de funcionarios y contratistas de la entidad."*

Así las cosas, si la entidad reconoció expresamente que las características de las cotizaciones recibidas no se adecuaban a la necesidad real, estas no debieron ser tenidas en cuenta dentro del estudio de mercado y, menos aún, para que se concluyera que *"Realizado el estudio inmobiliario a partir del análisis de los inmuebles ofrecidos, para la entidad la mejor opción es permanecer en las instalaciones en las cuales actualmente*

funciona", pues los inmuebles que fueron objeto de análisis no eran ponderables ni comparables entre sí.

Los anterior debido a que la entidad realizó el estudio de mercado sin tener en cuenta la uniformidad que debían tener las cotizaciones en cuanto el valor de las mismas, lo que puede ocasionar que el valor estimado del contrato no se ajuste a la realidad del mercado y que no se pueda concluir de manera objetiva que el valor pagado es el más económico para la entidad.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR – 144 Etapa De Planeación Contractual Estudios Previos, presentó el siguiente Diseño de Control:

Control 1: CONTROL 6.1.13: REVISAR ESTUDIOS Y DOCUMENTOS PREVIOS: Revisar los documentos contenidos en la carpeta contractual. Si los estudios están correctos se pasa a la actividad 15 o 16 de la elaboración del proyecto de pliegos, si no, volver a la actividad No.1. Responsable: Profesional de Jurídica y Contratación. (ESTUDIOS PREVIOS):

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 cuanto que no se encuentra documentado en el propósito del control, qué se revisa de los documentos, ni el procedimiento de cómo se hace la revisión de los mismos, así como tampoco la evidencia del control. Cabe señalar que el control indicado no es específico por cada uno de los documentos previos, tales como las cotizaciones, el estudio de sector o el estudio previo, sino que se encuentra descrito en el procedimiento de manera muy general para todos los documentos contenidos en la carpeta contractual, lo que dificulta la especificidad del control y por lo tanto la eficacia en la ejecución del mismo.

Valoración comentarios del Auditado

Por parte de la SJC, el auditado argumenta que:

> *"Se reitera que, si bien es cierto que los procesos y procedimientos que rigen la contratación estatal de la Entidad se encuentran en cabeza de la Subdirección Jurídica y de Contratación, la responsabilidad de la estructuración de los documentos que la soportan son responsabilidad de las dependencias solicitante de la contratación, ya que son éstas las conocedoras de la necesidad que se busca suplir.*
> *De igual manera, conforme a lo establecido en el procedimiento PR-154 EJECUCIÓN Y CIERRE DEL EXPEDIENTE CONTRACTUAL los supervisores de contratos deberán suscribir las actas de inicio y publicarlas en el SECOP II; realizar seguimiento a la entrega de los productos o servicios contratados dentro de los términos establecidos en el contrato y con las condiciones de calidad requeridas, además de informar de manera oportuna los posibles incumplimientos por parte del contratista, cuantificar los perjuicios e ingresar al aplicativo GOOBI oportunamente las terminaciones y las liquidaciones de los contratos cuando a ello haya lugar; justificar las modificaciones contractuales; revisar y aprobar o rechazar los informes*

de ejecución de contratos y/o convenios en la plataforma SECOP II y expedir y publicar en el SECOP II las certificaciones de cumplimiento cuando a ello haya lugar.
En consecuencia, de lo anterior, se solicita se desvincule a la Subdirección Jurídica y de Contratación del presente hallazgo en el informe definitivo."

Por parte de la SDAE, el auditado argumenta que:

"No se puede aseverar "DEFICIENCIAS TÉCNICAS EN LOS ESTUDIOS PREVIOS" cuando los mismos se materializan en un contrato y se cumple a cabalidad con las obligaciones Contractuales de ambas partes, entendiendo un contrato como el acuerdo de voluntades entre dos partes.
En este caso al requerir en los estudios previos ciertas cantidades y capacidades, se efectúa la contratación en ese mismo sentido para suplir una o varias necesidades de la entidad. Por lo que no se da lugar a la observación en la redacción actual."

Por parte de la SAF, el auditado argumenta que:

"Es importante señalar que en documento "Análisis y Comparación de los Bienes Inmuebles", elaborado en la etapa precontractual del contrato 03 de 2019, se involucraron y analizaron todas las variables necesarias para determinar que lo más beneficioso para la entidad era continuar en la ubicación actual.

Lo anterior conllevó:
i. *Se hizo la solicitud de cotizaciones a las siguientes firmas inmobiliarias sobre predios que cumplieran con las condiciones exigidas por el IPES:*

1) MODERLINE – Oficio Radicado No. 00110-816-026340 del 26/10/2017.
2) FAMOC DE PANEL – Oficio Radicado No. 00110-816-026342 del 26/10/2017
3) SERVEX COLOMBIA S.A.S – Oficio Radicado No. 00110-816-026337 del 26/10/2017.

Como resultado de ello, se obtuvieron los siguientes predios:

EDIFICIO	DIRECCIÓN	ÁREA M2	VALOR OFERTADO M2 CON IVA	VALOR MENSUAL CON IVA DEL ARRENDAMIENTO
EDIFICIO TORRE 73	CALLE 73 # 11-66	3600	$ 73,059	$ 263,012,400
EDIFICIO SAN CAYETANO	Carrera 85 D No 46 A-65	3549	$ 101,262	$ 359,380,000
EDIFICIO ELEMENTO	Calle 26 No, 69-76	3566	$ 119,999	$ 427,916,434

ii. *Se realizó una búsqueda de los predios disponibles en el sector, con el propósito de evidenciar si alguno cumplía con las condiciones técnicas exigidas por el IPES, lo cual, dio como resultado que ninguno de los predios cumplía con las condiciones, tal y como se evidencia en el documento:*

1. Ninguno cuenta con el área mínima requerida por parte del Instituto, es decir por lo menos 3600 M2.
2. Ninguno ofrece la opción de alquilar el mobiliario que incluya puestos de trabajo diseñados, distribuidos y adecuados en virtud del cumplimiento de la normatividad actual relacionada con salud ocupacional, y el Manual de Estandarización de Espacios de trabajo para Entidades del Estado, de la Agencia Nacional Inmobiliaria "Virgilio Barco Vargas", documento disponible en:

https://mail.google.com/mail/u/0/#inbox/1611fa403313c0a7?projector=1&messagePartId=0.1

3. No cuentan con la adecuación en cuanto a infraestructura tecnológica. Este punto también es vital, habida cuenta que la conectividad del Instituto pende que la infraestructura propia sea compatible con la que exista en el inmueble, de lo contrario resultaría imperativo realizar adecuaciones a efectos de lograr dicha compatibilidad, esas adecuaciones son onerosas y demandan de tiempo, dinero y voluntad del propietario o arrendador para realizarlas bajo su cuenta y riesgo.
4. No cuentan con áreas como enfermería, sala de capacitación, centro de monitoreo, entre otros. Dichos espacios que actualmente tiene la entidad, son espacios de los cuales no se puede prescindir puesto que irían en detrimento del bienestar de los funcionarios y contratistas que hacen uso de estos espacios.
5. Ninguno tiene la capacidad de alojar la totalidad de funcionarios y contratistas de la entidad.

Todo lo anteriormente expuesto, nos permite afirmar que:
iii. *En el sector no había disponibilidad de inmuebles que cumplieran con las condiciones técnicas exigidas por el IPES.*
iv. *Las ofertas recibidas de otros sectores de la ciudad, reflejaban un costo mayor para el IPES.*
En tal sentido, se manifiesta que la conclusión de continuar arrendando el edificio donde actualmente funciona la sede administrativa del IPES, no se tomó basada en que los inmuebles del sector no cumplían con las condiciones técnicas, sino que, por el contrario, fue el resultado de un estudio completo sobre todas las opciones disponibles.
Por lo anterior, solicitamos respetuosamente al equipo auditor que reconsidere y elimine esta observación del informe de auditoría."

La Auditoría efectúa el siguiente análisis:

Respecto de la solicitud realizada por la SJC de "se desvincule a la Subdirección Jurídica y de Contratación del presente hallazgo en el informe definitivo", es menester aclarar que no es posible acceder a dicha solicitud, por cuanto tal como lo señalo la SJC, los procesos y procedimientos que rigen la contratación estatal de la Entidad se encuentran en cabeza de la Subdirección Jurídica y de Contratación, por tanto si bien es cierto que la observación se centra en las deficiencias técnicas encontradas en el estudio previo al no existir soporte de los cambios técnicos realizados entre uno y otro contrato, el cual es responsabilidad del área que los elaboró, no es menos cierto que los controles que deben existir en los procesos y procedimientos se encuentran en cabeza de la SJC, por lo tanto y en vista que la SDAE no aportó argumentación o evidencia que desvirtúe lo manifestado en el informe preliminar, respecto del presente numeral, se mantiene la observación en cabeza de ambas áreas en lo que a cada quien corresponda.

Respecto de la réplica de la SDAE: Contrario a lo manifestado por el Auditado en su réplica, no es cierto que por el hecho de existir y ejecutar un contrato se pueda deducir entonces que del mismo no puedan existir deficiencias técnicas, pues, tal como se manifestó en la observación, la auditoria no evidenció en los documentos del contrato, y cabe mencionar que tampoco fue aportado en la réplica, los documentos que soporten técnicamente las características requeridas para la ejecución del contrato en mención, máxime por cuanto

de los elementos técnicos mencionados en ella hubo cambios entre el contrato de 2018 y el contrato de 2019 con el mismo contratista.

Respecto de la réplica de la SAF: En primer lugar, la solicitud de cotizaciones a las firmas inmobiliarias que hace referencia el estudio de mercado se llevó a cabo en el año 2017 y no se pudo evidenciar en los documentos del expediente contractual, la realización del mismo estudio para el año 2018 o 2019 que es el año del contrato objeto de la presente observación.

En segundo lugar, la auditoria no considera que se llevó a cabo un estudio de mercado de manera objetiva por cuanto señala el acápite "*Zona de Estudio*" del documento titulado *"Análisis y comparación de los bienes inmuebles": "Se definió un cuadrante para realizar la búsqueda de inmuebles ofertados en arrendamiento para oficinas, ubicado entre las Calles 63 a 76 y las Carreras 5 a 14 (Avenida Caracas), tal como se muestra en el gráfico siguiente".* Limitación geográfica que en primer lugar contraría especialmente lo estipulado en el numeral 1 del art. 2.2.1.2.1.4.11 del Decreto 1082 de 2015 que versa: *"1. Verificar las condiciones del mercado inmobiliario <u>en la ciudad</u> en la que la Entidad Estatal requiere el inmueble." (subrayado fuera de texto)*

Por lo tanto, dentro del expediente contractual no se evidenció soporte alguno del porqué la entidad escogió esa zona como la única en donde se realizaría el análisis de los precios, más allá de que la actual sede de la entidad se encuentre ubicada dentro de este sector. Al respecto, si la intención de la entidad era conocer los precios del mercado solamente en el sector, debió en primer lugar argumentar técnicamente porque esa limitación geográfica e igualmente, al no encontrar cotizaciones con características semejantes, debió ampliar la zona o cuadrante en donde pretendía realizaba el estudio, a efectos de conocer la realidad del canon de arrendamiento de los inmuebles con base en la verdadera necesidad de la entidad.

Igualmente, continua el documento de estudio de mercado afirmando: *"De la anterior información se puede concluir que en la actualidad no hay disponibilidad de inmuebles en la zona predeterminada en oferta de arrendamiento para oficinas que satisfaga las necesidades del instituto para la Economía Social por las siguientes razones: (…)".* Sobre lo precedente, y una vez evidenciado por parte de la entidad la escasez de bienes que cumplieran sus necesidades dentro del cuadrante en el cual quiso limitar la búsqueda, esta debió ampliar la zona de búsqueda, como quiera que no había obtenido la información imprescindible, o a lo sumo suficiente, para poder comparar las cotizaciones de forma objetiva.

Así las cosas, el análisis de mercado no contó con la información principal y básica, como quiera que no se tuvo una pluralidad de cotizaciones con la cual se pudiera realizar un verdadero ejercicio comparativo de cara a la obtención de un precio aproximado para el canon del inmueble objeto de arriendo, puesto que al final únicamente se tomó en cuenta el valor del inmueble que ya era objeto de ocupación por parte de la entidad.

En mérito de lo expuesto, el hallazgo se mantiene.

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:

1. *Deficiencias técnicas del estudio previo:*

Decreto 1082 de 2015 Artículo 2.2.1.1.2.1.1. Estudios y documentos previos. *Los estudios y documentos previos son el soporte para elaborar el proyecto de pliegos, los pliegos de condiciones, y el contrato. Deben permanecer a disposición del público durante el desarrollo del Proceso de Contratación y contener los siguientes elementos, además de los indicados para cada modalidad de selección:*
1. La descripción de la necesidad que la Entidad Estatal pretende satisfacer con el Proceso de Contratación.
2. El objeto a contratar, con sus especificaciones, las autorizaciones, permisos y licencias requeridos para su ejecución, y cuando el contrato incluye diseño y construcción, los documentos técnicos para el desarrollo del proyecto.
3. La modalidad de selección del contratista y su justificación, incluyendo los fundamentos jurídicos.
(…)

PR-144 ETAPA DE PLANEACION CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO: CONTROL 6.1.13: REVISAR ESTUDIOS Y DOCUMENTOS PREVIOS: *Revisar los documentos contenidos en la carpeta contractual. Si los estudios están correctos se pasa a la actividad 15 o 16 de la elaboración del proyecto de pliegos, si no, volver a la actividad No.1.*
Responsable: Profesional de Jurídica y Contratación. (ESTUDIOS PREVIOS).

2. *Deficiencias en el estudio de mercado:*

LEY 1437 DE 2011; Artículo 3. Principios*. (...) Las actuaciones administrativas se desarrollarán, especialmente, con arreglo a los principios del debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad.*

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.*

DECRETO 1082 DE 2015; Artículo 2.2.1.2.1.4.11. Arrendamiento de bienes inmuebles. *Las Entidades Estatales pueden alquilar o arrendar inmuebles mediante contratación directa para lo cual deben seguir las siguientes reglas:*
1. Verificar las condiciones del mercado inmobiliario en la ciudad en la que la Entidad Estatal requiere el inmueble.
2. Analizar y comparar las condiciones de los bienes inmuebles que satisfacen las necesidades identificadas y las opciones de arrendamiento, análisis que deberá tener en cuenta los principios y objetivos del sistema de compra y contratación pública.

Manual de Contratación MS-012 V3 - Actividad de control 5.1.2 Estudio de Mercado: *La dependencia que adelanta el proceso contractual, debe elaborar el estudio de mercado de acuerdo a los datos históricos o cotizaciones o análisis de precios unitarios o precios referencia, según corresponda.*

PR-144 ETAPA DE PLANEACION CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO: CONTROL 5.2*: El Subdirector o Jefe de Oficina o Asesora y profesionales designados deben elaborar el estudio de mercado de acuerdo a los datos históricos de adquisiciones de la Entidad o de otras entidades públicas en Bogotá D.C. o solicitudes de cotizaciones a proveedores autorizados en el mercado o análisis de precios unitarios o precios de referencia o consultas en el SECOP II e incorporar la información en los formatos dispuestos por la Entidad para tal efecto.*

El/la profesional designado/a por el/la Subdirector/a o Jefe de Oficina o Asesor/a debe ingresar a la sección denominada "SOLICITUD DE INFORMACION A PROVEEDORES

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, 2018).
- Modificar el PR-144, e incluir en el acápite 6.1 **"TABLA EXPLICATIVA DEL PROCEDIMIENTO**", los 6 elementos del diseño de control con sus respectivas explicaciones (Responsable, Periodicidad, Propósito, Cómo se hace, Excepciones o Desviaciones, Evidencia) por cada uno de los documentos que hacen parte de la etapa de planeación, es decir, el estudio de mercado, el estudio de sector y el estudio previo.
- Elaborar y adjuntar en los documentos previos del contrato, los documentos que técnicamente justifiquen las características técnicas solicitadas en aquel, de tal modo que de ellos se pueda concluir las razones por las cuales existen cambios técnicos entre contratos con el mismo objeto y contratista, pero de diferente vigencia.
- Para el caso de los arrendamientos, llevar a cabo el estudio de mercado en toda la ciudad, tal y como se realizó en el año 2017 y acorde a lo estipulado en el DECRETO 1082 DE 2015; Artículo 2.2.1.2.1.4.11.
- En caso de requerir limitar la zona en la cual se debe llevar a cabo el estudio de mercado, se debe llevar a cabo la justificación técnica de dicha limitación y la misma, debe reposar en los documentos previos del contrato.

- La comparación de las cotizaciones debe ser con aquellas que cumplan con las características técnicas establecidas en el estudio previo de necesidad.

Connotación: Administrativa con Posible connotación disciplinaria.

No: 12

DEFICIENCIAS EN LA EJECUCION DEL CONTRATO

Responsable de las acciones de mejora: SDAE

En 3 de 9 contratos de la muestra seleccionada, se evidenciaron deficiencias en el cumplimiento de las obligaciones por parte del contratista así:

1) En los contratos 297 de 2018, 3 de 2019 y 13 de 2020 con FAMOC DE PANEL S.A. cuyo objeto es "ARRENDAMIENTO DEL INMUEBLE UBICADO EN LA CALLE 73 NO. 11-66 PARA LA SEDE DEL INSTITUTO PARA LA ECONOMÍA SOCIAL- IPES, CON EL PROPÓSITO DE DESARROLLAR SUS ACTIVIDADES ADMINISTRATIVAS, OPERATIVAS Y MISIONALES.

Al realizar un seguimiento tanto de los informes de supervisión, las actas de liquidación y visita de auditoria, se evidencio el incumplimiento por parte del contratista en el suministro de un "Arco detector de metales".

2) En el contrato 341 de 2020 con ETB, cuyo objeto es: "ADQUISICIÓN, CONFIGURACIÓN Y PUESTA EN OPERACIÓN DE UNA SOLUCIÓN INTEGRAL DE BACKUP PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL INSTITUTO PARA LA ECONOMÍA SOCIAL – IPES," al realizar visita al punto comercial de Kennedy y la plaza de mercado la Perseverancia el día 28 de septiembre del presenta año se evidenciaron las siguientes deficiencias (Ver imágenes 4 y 5):

- El punto comercial de Kennedy: existencia de cableado sin canaleta y en mal estado, generando riesgos tanto de seguridad para los transeúntes como posibles riesgos eléctricos.
- En la Plaza de mercado de la Perseverancia: dentro de la oficina administrativa, el punto de Datos presentaba existencia de cableado sin peinar, lo que puede generar un riesgo operativo para dificultar la atención del soporte en el momento en que se requiera.

Situaciones que contrarían el objeto del contrato y las obligaciones específicas "Mantenimientos Técnicos". ETB opera y mantiene los equipos y sistemas entregados en las soluciones de los clientes 7 días, 24 horas al día, 365 días al año y ofrece los servicios de Mantenimiento Correctivo para toda la infraestructura de red y todos los elementos suministrados. Estos mantenimientos podrán realizarse de manera remota o en sitio, según lo determine ETB para cada caso.

1. Mantenimiento Preventivo: se realizará cuando ETB determine la necesidad de efectuarlo, en fechas que se programarán de común acuerdo con el cliente y cuyo objetivo consiste en llevar a cabo diagnósticos de los enlaces y equipos, para prevenir eventuales fallas de los mismos.

2. Mantenimiento Correctivo: consiste en atender las llamadas recibidas del cliente reportando daños en la solución, procediendo a su reparación dentro de los tiempos de respuesta establecidos.

Lo anterior debido a que las actividades de supervisión y/o interventoría de la ejecución contractual no se realizaron de acuerdo a los parámetros establecidos en el Procedimiento de supervisión del IPES en MIPG ni los parámetros establecidos en la ISO 27001: 2013 en su control A.15.2.1 Seguimiento y Revisión de los servicios de los proveedores, lo que podría ocasionar un incumplimiento del contrato y un posible detrimento patrimonial.

Análisis del Diseño de Controles

El diseño de las actividades de control señaladas en el Procedimiento PR- 154 ejecución y cierre del expediente contractual, presentó el siguiente Diseño de Control:

Control 2: 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

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 cuanto que no se encuentra documentado el tratamiento a las desviaciones ni la evidencia del mismo, así como tampoco se encuentra especificado en el control como se realiza el seguimiento referido.

Valoración comentarios del Auditado

Por parte de la SDAE, el auditado argumenta que:

> *"Respecto del numeral 1:*
> *Se solicita al equipo auditor, realizar una revisión sobre el alcance y extralimitación en el amplio número de los términos empleados (de acuerdo a la naturaleza de la definición de cada uno) en relación a los hechos sobre los cuales basa la observación, lo cual denota en un incumplimiento general sobre toda la naturaleza del objeto y obligaciones de los contratos que aluce.*
> *Lo anterior, entendiéndose que se emplean los términos:*
> *● Ejecución inadecuada y/o parcial del objeto contractual*
> *● por falencias en el seguimiento y control de los aspectos técnicos,*
> *● administrativos,*
> *● financieros,*
> *● contables y*
> *● jurídicos del mismo*

● y/o incumplimiento a la normatividad vigente aplicable para el desarrollo de la labor de supervisión.

Respecto del numeral 2:
Se realizan las siguientes aclaraciones de acuerdo a la redacción del auditor:
● No existe relación entre el número del anexo citado en la observación y el adjunto: "ANEXO 14 - Relación de contratos recurrentes suscritos IT-GOP de 2016 a 2020"
● No existe relación entre el número de contrato citado: "341 de 2020" con ETB, y el objeto que relaciona la observación: "ADQUISICIÓN, CONFIGURACIÓN Y PUESTA EN OPERACIÓN DE UNA SOLUCIÓN INTEGRAL DE BACKUP PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL INSTITUTO PARA LA ECONOMÍA SOCIAL – IPES,"
Se precisa que el contrato suscrito con la Empresa de Telecomunicaciones de Bogotá no tiene objeto de BackUp, adicionalmente las obligaciones contractuales se enfocan en el aprovisionamiento de canales de comunicación, no es responsabilidad del contratista la organización (Peinado) del cableado, ni la organización de la oficina, en el mencionado contrato no existen obligaciones de cableado estructurado, por lo que las observaciones no tienen fundamento.
Para su conocimiento los ISP (Prestadores de servicios de Internet) entregan sus servicios en punta, no es responsabilidad de los mismos la adecuación interna. al igual que en la casa la instalación se realiza hasta un dispositivo final como una toma o un módem y de allí en adelante las extensiones, conexiones y demás las realiza el usuario final, adicionalmente a que la observación se encuentra fuera del alcance de la auditoría atendiendo a temas de seguridad laboral, no riesgos de seguridad informática y no se puede afirmar" DEFICIENCIAS EN LA EJECUCIÓN DEL CONTRATO", con algo que no se ha contratado".

La Auditoría efectúa el siguiente análisis:

Respecto de la réplica al numeral 1 de la presente observación, la ACI se permite aclarar al auditado que los términos por él señalados, son los que componen, no la observación como tal, sino el riesgo al cual la presente observación se encuentra relacionada, recordando al auditado, que tal y como se explicó en la reunión de apertura de auditoria, el presente ejercicio de auditoria se encuentra basada en riesgos y su administración, y por lo tanto de la evaluación que de los controles establecidos por la entidad para mitigar dichos riesgos se obtenga evidencia en una determinada muestra; es por esta razón que la ACI, no llevará a cabo modificación de los términos allí utilizados, pues los mismos corresponden semántica y gramaticalmente al riesgo a evaluar, es decir, establecen el evento con más posibilidad de que suceda y que tendría un impacto sobre el cumplimiento de los objetivos de la entidad, tal como lo determina la Guía de Administración del riesgo del DAFP.

Por lo anterior, y en razón a que no se aportó evidencia que desvirtuara la observación, de tal suerte que contractualmente se exigía un "Arco detector de metales" y del mismo no se evidenció por parte de esta auditoria la entregada por parte del contratista, la observación se mantiene.

Respecto de la réplica en el numeral 2 de la presente observación, se aceptan los argumentos del área respecto de que no es el contratista ETB en ejecución del contrato 341 de 2020 quien debe subsanar las situaciones evidenciadas por el auditor y descritas en la observación, sin embargo, las situaciones allí señaladas tienen como doliente final el área "SEGURIDAD DE LA INFORMACION Y RECURSOS TECNOLÓGICOS",

perteneciente a la SDAE, bien sea directamente o a través de un tercero contratista, por lo tanto, las situaciones descritas en la observación, harán parte de la observación numero 3

En mérito de lo expuesto, el hallazgo se modifica en el sentido de eliminar de la misma el numeral 2 respecto del contrato 341 de 2020 y trasladar las situaciones allí señaladas ala hallazgo No.3 numeral 4 del presente informe. En lo demás, se mantiene el hallazgo.

Riesgo Asociado: Deficiencias en la labor de supervisión e interventoría ejercida: Ejecución inadecuada y/o parcial del objeto contractual por falencias en el seguimiento y control de los aspectos técnicos, administrativos, financieros, contables y jurídicos del mismo y/o incumplimiento a la normatividad vigente aplicable para el desarrollo de la labor de supervisión.

Normatividad o Criterio:

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.

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.

Decreto 1082 de 2013, Artículo 2.2.1.1.1.2.1. *Partícipes de la Contratación Pública. Los partícipes del sistema de compras y contratación pública para efectos del Decreto ley 4170 de 2011, son:*
1. *Los supervisores.*

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, 2018).
- Ejecutar el PR- 154 EJECUCION Y CIERRE DEL EXPEDIENTE CONTRACTUAL, especialmente en el control 3, respecto de la ejecución de los contratos por parte del contratista.

- Se recomienda la ejecución de un control documental que permita al supervisor llevar a cabo un seguimiento del cumplimento de todas y cada una las obligaciones del contrato, de tal suerte que le permita hacer las alertas pertinentes del incumplimiento del mismo.

Connotación: Administrativo con posible connotación Disciplinaria.

No:13

DEFICIENCIAS EN EL DISEÑO DEL CONTROL DEL PROCESO DE GESTION CONTRACTUAL

Responsable de las acciones de mejora: SJC

Se evidenciaron deficiencias en el diseño de los controles establecidos en los diferentes procedimientos del Proceso de Gestión Contractual 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 (2018), así:

RIESGO 1: Ineficacia del proceso de contratación por la adquisición de un bien, obra o servicio que no se encuentre incluido en el Plan Anual de Adquisiciones – PAA.

1) **Actividad de Control Analizada:** PR- 143 ETAPA DE PLANEACIÓN CONTRACTUAL - PAA V4: ACTIVIDAD CONTROL 6.1.1 ELABORAR EL PLAN ANUAL DE ADQUISICIONES.

   Diseño del Control: No se encuentra señalado en el control el propósito, ni cómo se lleva a cabo la actividad que permita mitigar las deficiencias en la Planificación y publicación del PAA es decir el control que se hace a la actividad de inclusión en el PAA de los diferentes objetos o necesidades por parte de las áreas. Se requiere señalar el procedimiento del manejo de excepciones y la evidencia de la ejecución del control a realizar.

2) **Actividad de Control Analizada:** PR- 143 ETAPA DE PLANEACIÓN CONTRACTUAL - PAA V4: ACTIVIDAD CONTROL 3: REVISAR Y APROBAR EL PLAN ANUAL DE ADQUISICIONES.

   Diseño del Control: Falta señalar el manejo de excepciones.

3) **Actividad de Control Analizada:** PR-143 ETAPA DE PLANEACIÓN CONTRACTUAL - PAA V4: ACTIVIDAD CONTROL 9: REALIZAR SEGUIMIENTO AL PLAN ANUAL DE ADQUISICIONES.

Diseño del Control: En el diseño del control no se especifica el procedimiento que lleva a cabo el comité de contratación, el manejo que hacen de las excepciones ni la evidencia que debe existir por parte del Comité de contratación.

RIESGO 2: Descripción inexacta de los bienes, obras y servicios que no satisfaga las necesidades de la Entidad.

4) **Matriz de Riesgos y Controles:** Cada vez que se va a realizar un proceso de contratación, los profesionales de contratación de la SJC y sus referentes en cada Subdirección verifican el cumplimiento de los requisitos jurídicos establecidos en los procedimientos PR-143 ETAPA DE PLANEACIÓN CONTRACTUAL PAA y PR-144 ETAPA DE PLANEACIÓN CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO para la Elaboración de los estudios de mercado, análisis del sector, estudios previos y Pliegos de condiciones. Como evidencia, los documentos generados en cada proceso de contratación a través de la plataforma SECOP II o en los expedientes contractuales, según corresponda. En caso de encontrar información faltante, se requiere a la dependencia que solicita la contratación a través de correo electrónico aportar la información para continuar con el respectivo proceso y se brinda asesoría al recurso humano de las distintas dependencias.

   Diseño del Control: El riesgo no se encuentra documentado en el SIG y se requiere establecer una fuente confiable de ejecución del control.

RIESGO 3: ineficacia del proceso de contratación por deficiencias en los documentos previos del proceso contractual.

5) **Actividad de Control Analizada:** PR-144 ETAPA DE PLANEACION CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO: CONTROL 5.2.

   Diseño del Control: En el diseño no se encuentran los elementos para determinar la actividad como un control, pues no está identificado el propósito, no se especifica quien debe revisar o cotejar el estudio de mercado y el modo como debe dejar evidencia de ello, por lo tanto, no es un control.

6) **Actividad de Control Analizada:** PR-144 ETAPA DE PLANEACION CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO: CONTROL 6.1.13: REVISAR ESTUDIOS Y DOCUMENTOS PREVIOS.

   Diseño del Control: No se encuentra documentado en el propósito del control, que se revisa de los documentos, ni el procedimiento de cómo se hace la revisión de los mismos, así como tampoco la evidencia del control. Cabe señalar que el control señalado no es especifico por cada uno de los documentos previos, tales como las cotizaciones, el estudio de sector o el estudio previo, sino que se encuentra descrito en el procedimiento de manera muy general para todos los documentos contenidos en la carpeta contractual, lo que dificulta la especificidad del control y por lo tanto la eficacia en la ejecución del mismo.

7) **Actividad de Control Analizada:** PR-144 ETAPA DE PLANEACION CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO: CONTROL 6.1.8.

   Diseño del Control: Falta especificar la evidencia de la ejecución del control.

RIESGO 4: Insuficiencia en la asignación de recursos al proceso contractual.

8) **Actividad de Control Analizada:** PR-144 ETAPA DE PLANEACION CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO: CONTROL 6.1.8: SOLICITAR APROPIACION PRESUPUESTAL: Subdirectora / Jefe de Oficina: Solicitar al ordenador del gasto, la respectiva apropiación presupuestal, previa constancia de la SDAE que indique que en la solicitud de contratación que respalda el proceso de contratación cumple con los objetivos y las metas de los proyectos de inversión de la Entidad:

   Diseño del Control: Falta detallar que ocurre en caso de presentarse desviaciones y detallar la evidencia del control.

RIESGO 5: ineficacia del Proceso de Selección por deficiencias en su desarrollo

9) **Actividad de Control Analizada:** PR-144 ETAPA DE PLANEACION CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO: CONTROL 6.1.16 REVISAR Y APROBAR O RECHAZAR DOCUMENTOS DE LA CONVOCATORIA.

   Diseño del Control: Falta especificar qué aspectos son los que se revisan en el control y la evidencia de la ejecución del mismo.

10) **Actividad de Control Analizada:** PR-144 ETAPA DE PLANEACION CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO: CONTROL 6.1.23 TABLA EXPLICATIVA: RESPONDER OBSERVACIONES.

    Diseño del Control: No se encuentra claramente establecido quien realiza el control, ni cuál es la actividad de control que se realiza a las observaciones previas su publicación, ni el propósito del control.

11) **Actividad de Control Analizada:** PR-144 ETAPA DE PLANEACION CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO: CONTROL 6.1.23 TABLA EXPLICATIVA: RESPONDER OBSERVACIONES.

    Diseño del Control: No se encuentra claramente establecido quien realiza el control, ni cuál es la actividad que se realiza a las observaciones previas su publicación, ni el propósito del control.

12) **Actividad de Control Analizada:** PR-145 ETAPA DE SELECCIÓN Y ADJUDICACION: CONTROL 6.1.26: EVALUAR PROPUESTAS Y RENDIR INFORME.

Diseño del Control: Falta documentar las actividades de control que se realizan al momento de verificar la evaluación de los proponentes, no existe documentado que control llevan para establecer entre otros, que se hayan evaluado a todas las propuestas y que se haya revisado que la evaluación estuvo acorde a las condiciones del pliego o de la Ley.

RIESGO 6: Nulidad del contrato por falencias en la elaboración y/o legalización del mismo.

13) **Actividad de Control Analizada:** PR-150 PERFECCIONAMIENTO Y REQUISITOS DE EJECUCION DEL CONTRATO: ACTIVIDAD DE CONTROL 6.1.16 EXPEDIR REGISTRO PRESUPUESTAL.

Diseño del Control: No se encuentra documentado en el SIG, control respecto de la revisión de la información que se encuentra en el RP y su correspondencia con las condiciones del contrato.

14) **Actividad de Control Analizada:** PR-150 PERFECCIONAMIENTO Y REQUISITOS DE EJECUCION DEL CONTRATO: ACTIVIDAD DE CONTROL 19 APROBAR O RECHAZAR GARANTIA: El subdirector jurídico y de contratación revisa y aprueba o rechaza la garantía del contrato a través del SECOP II, si se aprueban se informa de dicha aprobación, si no se aprueban se devuelven al contratista para su aprobación.

Diseño del Control: Falta establecer en el control cuales son los aspectos que se revisan para la aprobación o rechazo de la garantía.

RIESGO 7: Retraso en la adquisición de los bienes y servicios requeridos por la entidad.

15) **Matriz de Riesgos y Controles:** Cada vez que se va a realizar un proceso de contratación, los profesionales de contratación de la SJC, verifican el cumplimiento de los requisitos jurídicos establecidos en los procedimientos PR-143 ETAPA DE PLANEACIÓN CONTRACTUAL PAA y PR-144 ETAPA DE PLANEACIÓN CONTRACTUAL ESTUDIOS PREVIOS Y PROYECTO DE PLIEGO. Como evidencia, los documentos generados en cada proceso de contratación a través de la plataforma SECOP II o en los expedientes contractuales, según corresponda. En caso de encontrar información faltante, se requiere a la dependencia que solicita la contratación a través de correo electrónico aportar la información para continuar con el respectivo proceso.

Diseño del Control: En la prueba de recorrido se evidenció que, en algunos casos, no se solicita mediante correo electrónico, sino que se llevan a cabo reuniones informales con el fin de llevar a cabo las modificaciones de manera más rápida. Igualmente, el control no se encuentra establecido en el SIG y al llevarse a cabo remisión a otros procedimientos se requiere ser más específico a que controles de esos procedimientos se refiere.

16) **Matriz de Riesgos y Controles:** Los profesionales de contratación de la SJC realizan 12 capacitaciones anuales en el marco del PIC incorporada como buena práctica en la gestión contractual con respecto a los estudios previos, supervisión, liquidación de contratos con la finalidad de afianzar los conocimientos del recurso humano encargado de la contratación de las distintas dependencias. Como evidencia, las actas de asistencia a las capacitaciones. En caso de solicitar apoyo adicional, se brinda asesoría al personal de las distintas dependencias en materia contractual la cual se asigna dependiendo la modalidad de la selección del contratista, y se verifica a través de correo electrónico o lista de asistencia.

    Diseño del Control: No se encuentra documentado el SIG el control que permita verificar la realización de la actividad descrita en la matriz de riesgos de contratación

17) **Matriz de Riesgos y Controles:** Cada vez que se presente un cambio sustancial en la regulación contractual se lleva a cabo la modificación del Manual de Contratación, Supervisión e Interventoría del IPES y sus procedimientos asociados por parte de los profesionales de la gestión contractual con el visto bueno de la Dirección General. Como evidencia, las respectivas modificaciones al Manual y a los procedimientos asociados. En caso de presentarse incertidumbre en la normatividad aplicable, se brinda asesoría al recurso humano de las distintas dependencias.

    Diseño del Control: El diseño de control no establece un responsable ya sea como grupo o como designado, de la revisión periódica de la normativa legal y la contenida en el manual de contratación y demás procedimientos. Igualmente, el control no se encuentra establecido en el SIG.

RIESGO 8: Ineficacia de las modificaciones contractuales por falencias en la elaboración o expedición de las mismas.

18) **Actividad de Control Analizada:** PR-150 PERFECCIONAMIENTO Y REQUISITOS DE EJECUCION DEL CONTRATO: ACTIVIDAD DE CONTROL 18: REVISAR GARANTIAS DEL CONTRATO: El profesional de SJC revisará las garantías del contrato a través de la plataforma SECOP II y las remitirá para aprobación o rechazo del subdirector jurídico

    Diseño del Control: Falta establecer en el control cuales son los aspectos que se revisan para la aprobación o rechazo de la garantía.

RIESGO 9: Afectación en la transparencia del proceso de contratación por la inobservancia de los principios que orientan la contratación Estatal.

19) **Actividad de Control Analizada:** PR-145 ETAPA DE SELECCIÓN Y ADJUDICACION: CONTROL ACTIVIDAD DE CONTROL 2 REVISAR Y APROBAR O RECHAZAR RESOLUCION DE APERTURA Y PLIEGO DE CONDICIONES DEFINITIVO.

Diseño del Control: El control no describe sobre qué aspectos y como realiza la revisión del cumplimiento de los principios de contratación en los documentos del proceso de selección ni la evidencia del control respectivo.

RIESGO 10: Ineficacia de las modificaciones contractuales por falencias en la elaboración o expedición de las mismas.

20) Actividad de Control Analizada: PR- 154 EJECUCION Y CIERRE DEL EXPEDIENTE CONTRACTUAL ACTIVIDAD DE CONTROL No.6.1.32 REVISAR COMPONENTE JURIDICO DE LA LIQUIDACION: El /la Profesional de la SJC efectuará la Revisión del componente jurídico del acta de liquidación. Una vez se encuentre debidamente ajustada el/la profesional designado/a por la SJC dará su visto bueno en el formato y procederá a remitir el acta a él/la supervisor/a para la revisión y suscripción del contratista, el/la subdirector/a Administrativo/a y Financiero/a del contrato. Surtido lo anterior el/la Supervisor/a del contrato allegará a la SJC el acta de liquidación para la suscripción por parte de él/la Subdirector/a Jurídico/a y de contratación; posteriormente el Profesional de la SJC incorporará la fecha del acta.

Diseño del Control: No se encuentra documentado en el SIG, el procedimiento paso a paso de la liquidación del contrato, que permita mitigar una interpretación diferente de la normatividad aplicable.

RIESGO 11: Deficiencias en la labor de supervisión e interventoría ejercida.

21) Actividad de Control Analizada: NO DOCUMENTADO EN EL SIG

Diseño del Control: No existe un control a la labor del supervisor más allá de las actas que éste debe suscribir con el contratista.

22) Actividad de Control Analizada: 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

Diseño del Control: No se encuentra señalado el tratamiento a las desviaciones ni la evidencia del mismo, especificar en el control como se realiza el seguimiento referido.

RIESGO 12: Beneficios propios y/o a terceros.

23) Actividad de Control Analizada: Los profesionales de contratación cada vez que se va a realizar un contrato, verifican que la información suministrada por las áreas solicitantes corresponda con los requisitos establecidos de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisión con la información suministrada. En caso de encontrar información faltante, se requiere a las áreas solicitantes a través de correo para el suministro de la información y poder

continuar con el proceso de contratación. Como evidencia la respectiva lista de chequeo diligenciada y correos solicitando la información faltante en los casos que aplique.

Diseño del Control: El control no se encuentra documentado en el SIG.

24) **Actividad de Control Analizada:** La Entidad lleva a cabo el Comité de Contratación presidido por la Directora General mediante el cual se realiza el seguimiento a los procesos de contratación de conformidad con lo dispuesto en la Resolución 570 de 2012. En caso de encontrar inconsistencias en alguna de las etapas del proceso de contratación se realizarán las recomendaciones pertinentes. Como evidencia las respectivas actas de comité de contratación.

Diseño del Control: El control no se encuentra documentado en el SIG.

RIESGO 14: Ineficacia del Contrato por la Inadecuada aplicación de las normas externas que rigen la elaboración de contratos interadministrativos.

25) **Actividad de Control Analizada:** Los PR-153 ETAPA DE PLANEACION, SELECCION Y ADJUDICACION - CONVENIOS Y CONTRATOS INTERADMINSITRATIVOS.ACTIVIDAD DE CONTROL 11 REVISAR Y APROBAR O RECHAZAR EL PROCESO: El subdirector jurídico y de contratación revisa los estudios y documentos previos, anexos formatos y demás documentos y aprueba o rechaza a través del SECOP II

Diseño del Control: Hace falta establecer la periodicidad y como se hace el control, especificar qué es lo que se revisa en los estudios y documentos previos y la evidencia del control.

26) **Actividad de Control Analizada:** La Entidad lleva a cabo el Comité de Contratación presidido por la Directora General mediante el cual se realiza el seguimiento a los procesos de contratación de conformidad con lo dispuesto en la Resolución 570 de 2012. En caso de encontrar inconsistencias en alguna de las etapas del proceso de contratación se realizarán las recomendaciones pertinentes. Como evidencia las respectivas actas de comité de contratación.

Diseño del Control: El control no se encuentra documentado en el SIG. Ineficacia del Contrato por la Inadecuada aplicación de las normas externas que rigen la elaboración de contratos interadministrativos.

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, 2018).

Connotación: Administrativa.

9. PLAN DE MEJORAMIENTO

Las Subdirecciones de Diseño y Análisis Estratégico SDAE y Jurídica y de Contratación SJC, junto con los responsables de los procesos, suscribirán un Plan de Mejoramiento con las acciones a seguir en cada una de las observaciones presentadas, y lo enviarán a esta Asesoría dentro de los ocho (8) días hábiles siguientes al recibo del **Informe Final** de Auditoría.

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.

10. ANEXOS

ANEXO 1 *Solicitud de recursos a Dirección General para auditoría TI – vigencia 2019*
ANEXO 2 *Expectativas de SDAE respecto a la auditoría regular al proceso GSIRT*
ANEXO 3 *Estado de la seguridad de la información de la ISO 27001:2013*
ANEXO 4 *Conformación del equipo de sistemas de la SDAE*
ANEXO 5 *Mapas de riesgos*
ANEXO 6 *Muestras de auditoría por proceso auditado*
ANEXO 7 Tiempos de respuesta de los usuarios para cerrar un caso
ANEXO 8 *Ejecución planes de mantenimiento, vigencias 2018, 2019 Y 2020*
ANEXO 9 *Cumplimiento funciones Comité de Sistemas y Seguridad de la Información (Resolución IPES 615/2013)*
ANEXO 10 *Matriz de Aplicabilidad vs marco ISO 27001:2013*
ANEXO 11 *Relación de usuarios directorio activo a agosto/2020*