ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural	**INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL**
	PROCESO DE SEGUIMIENTO Y EVALUACIÓN
	INFORME DE AUDITORÍA

FECHA DE EMISIÓN DEL INFORME	Día:	**30**	Mes:	**11**	Año:	**2020**

Tipo de Auditoría:	Auditoría Interna de Gestión
Proceso:	Proceso Nivel de Apoyo - Gestión de Sistemas de Información y Tecnología
Líder de Proceso:	Juan Fernando Acosta Mirkow
Responsable Operativo:	Equipo del Área de Sistemas
Objetivo de la Auditoría:	Verificar el cumplimiento de los requisitos legales y reglamentarios aplicables a las actividades del proceso de Gestión de Sistemas de Información y Tecnología, así como el cumplimiento de los protocolos, manuales, políticas, modelos, procedimientos y demás lineamientos internos asociados al proceso.
Alcance de la Auditoría:	Se examinarán las actividades realizadas en el Instituto durante el 1 de julio de 2019 al 30 de junio de 2020, de acuerdo con las muestras seleccionadas.
Criterios de la Auditoría:	▪ Constitución Política de Colombia de 1991. ▪ Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. ▪ Ley 527 de 1999. “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones" ▪ Ley 1221 de 2008. “Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones" ▪ Ley 1266 de 2008. "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones" ▪ Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones” ▪ Ley 1341 de 2009. "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones" ▪ Ley 1474 de 2011 “Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública” ▪ Decreto Ley 019 de 2012. Por el cual se dictan normas para suprimir o

	reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. ▪ Ley 1581 de 2012. "Por el cual se dictan disposiciones generales para la protección de datos personales" ▪ 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. ▪ Ley 1928 de 2018. "Por medio de la cual se aprueba el «Convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest" ▪ Ley 1951 de 2019. "Por la cual crea el Ministerio de Ciencia, Tecnología e Innovación, se fortalece el Sistema Nacional de Ciencia, Tecnología e Innovación y se dictan otras disposiciones" ▪ Decreto 619 de 2007 Alcaldía Mayor de Bogotá, D.C. "Por el cual se establece la Estrategia de Gobierno Electrónico de los organismos y de las entidades de Bogotá, Distrito Capital y se dictan otras disposiciones" ▪ Decreto 316 de 2008 Alcaldía Mayor de Bogotá, D.C. "Por medio del cual se modifica parcialmente el artículo 3° del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico" ▪ Decreto 2573 de 2014. "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones" ▪ Decreto 103 de 2015. "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones" ▪ Decreto Único Reglamentario 1078 de 2015. "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" ▪ Decreto Único Reglamentario 1081 de 2015. "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República" ▪ Decreto 208 de 2016 Alcaldía Mayor de Bogotá, D.C. "Por medio del cual se adopta el Manual de Imagen Institucional de la Administración Distrital y el eslogan o lema institucional de la Alcaldía Mayor de Bogotá, D. C., para el período 2016 – 2019" ▪ Decreto 1413 de 2017 "Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales" ▪ Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" ▪ Acuerdo 57 de 2002 Concejo de Bogotá D.C. "Por el cual se dictan disposiciones generales para la implementación del Sistema Distrital de Información -SDI-, se organiza la Comisión Distrital de Sistemas, y se dictan otras disposiciones" ▪ Acuerdo 130 de 2004 Concejo de Bogotá D.C. "Por medio del cual se

	establece la infraestructura integrada de datos espaciales para el Distrito Capital y se dictan otras disposiciones" ▪ Acuerdo 279 de 2007 Concejo de Bogotá D.C. "Por el cual se dictan los lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital" ▪ Directiva Presidencial 02 de 2002 "Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software)" ▪ Directiva 2 de 2002 Alcaldía Mayor de Bogotá, D.C. "Formulación de Proyectos Informáticos y de Comunicaciones" ▪ Directiva 05 de 2005 Alcaldía Mayor de Bogotá, D.C. "Políticas Generales de Tecnologías de Información y Comunicaciones aplicables a las entidades del Distrito Capital" ▪ Directiva 22 de 2011 Alcaldía Mayor de Bogotá, D.C. "Estandarización de la información de identificación, caracterización, ubicación y contacto de los ciudadanos y ciudadanas que capturan las entidades del Distrito Capital" ▪ Directiva 11 de 2012 Alcaldía Mayor de Bogotá, D.C. "Promoción y uso de software libre en el Distrito Capital" ▪ Directiva 04 de 2016 Alcaldía Mayor de Bogotá, D.C. "Modificar y ampliar el alcance de la Directiva 011 de 2012 "Promoción y uso de Software Libre en el Distrito Capital"" ▪ Resolución 305 de 2008 Comisión Distrital de Sistemas (CDS) de la Secretaría General Alcaldía Mayor de Bogotá D.C. "Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre" ▪ Resolución 3564 de 2015. MinTIC "Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública" ▪ Resolución 002 de 2017 Comisión Distrital de Sistemas (CDS) de la Secretaría General Alcaldía Mayor de Bogotá D.C. "Por la cual se adoptan las políticas específicas para el desarrollo de la Infraestructura Integrada de Datos Espaciales para el Distrito Capital – IDECA" ▪ Resolución 003 de 2017 Comisión Distrital de Sistemas (CDS) de la Secretaría General Alcaldía Mayor de Bogotá D.C. "Por la cual se adopta la Guía de sitios Web para las entidades del Distrito Capital y se dictan otras disposiciones" ▪ Resolución 004 de 2017 Comisión Distrital de Sistemas (CDS) de la Secretaría General Alcaldía Mayor de Bogotá D.C. "Por la cual se modifica la Resolución 305 de 2008 de la CDS" ▪ Resolución 003 de 2018 Comisión Distrital de Sistemas (CDS) de la Secretaría General Alcaldía Mayor de Bogotá D.C. "Por la cual se aclara la Resolución 004 de 2017 de la CDS" ▪ Documento CONPES 3582 de 2009 "Política Nacional de Ciencia, Tecnología e Innovación" ▪ Documento CONPES 3701 de 2011 "Lineamientos de política para la Ciberseguridad y Ciberdefensa"

	▪ Documento CONPES 3854 de 2016 “Política Nacional de Seguridad Digital” ▪ Documento CONPES 3920 de 2018 “Política Nacional de Explotación de Datos (Big Data)” ▪ Norma Técnica ISO 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos ▪ Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información - PETI ▪ Manual de Gobierno Digital ▪ Lineamientos, Circulares y documentos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, Alta Consejería Distrital de TIC y entes reguladores en esta materia. ▪ Documentos del Proceso de Apoyo Gestión de Sistemas de Información y Tecnología (Planes, Políticas, caracterización, manuales, procedimientos, Instructivos, Formatos, entre otros)
Pruebas de Auditoría utilizadas:	Verificación documental Comprobación
Métodos de Muestreo:	Se realizó revisión de toda la información solicitada y entrevista en algunos casos específicos.

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día	04	**Mes**	09	**Año**	2020	**Desde**	03/09/2020 D / M / A	**Hasta**	30/11/2020 D / M / A	Día	17	Mes	11	Año	2020

Asesor de Control Interno	Auditor Líder	Equipo Auditor
Eleana Marcela Páez Urrego	Eleana Marcela Páez Urrego	Eleana Marcela Páez Urrego Lilliana María Calle Carvajal

1. RESUMEN EJECUTIVO

En cumplimiento del rol de Evaluación y Seguimiento de la Asesoría de Control Interno y con base en el Plan Anual de Auditoría 2020 del IDPC, se adelantó auditoría al Proceso de Gestión de Sistemas de Información y Tecnología, el cual fue comunicado a la líder del proceso, a través del radicado Orfeo 20201200044493 del 1 de septiembre de 2020.

Para el desarrollo de la presente auditoría se presentaron algunas limitaciones, en especial, no contar dentro del equipo auditor con un perfil enfocado al área de Sistemas, limitante que impidió hacer pruebas en equipos, software y/o servidores de la entidad. Así mismo, en algunos casos, la escasa explicación por parte del proceso al remitir información, esto debido a que solo aporta pantallazos o información no relevante, lo que dificultó un análisis más amplio.

Teniendo en cuenta lo anterior, la auditoría se adelantó con base en la normatividad que lo regula, procedimientos, manuales e instructivos, en la que se observó la efectividad en la aplicación y cumplimiento de los mismos.

Se evidenciará en el informe varias inexactitudes y/o inobservancias que podrán ser controvertidos por el proceso. Es importante además mencionar que, se auditó al proceso y no a personas.

Atendiendo lo anterior, se relaciona entonces lo evidenciado, a saber:

1.1 REVISIÓN DOCUMENTACIÓN PROCESO

Se realizó revisión de la documentación vigente en el proceso Gestión de Sistemas de Información y Tecnología observando lo siguiente:

1.1.1 Caracterización

Se cuenta con caracterización del proceso en su versión 3 del 17 de julio de 2019, la cual tiene como objetivo:

"*Formular, ejecutar y evaluar las políticas, planes, proyectos, infraestructura y servicios de tecnología, relacionados con los sistemas de información, que permitan operar, mantener y renovar la plataforma tecnológica acorde con los requerimientos institucionales, así como asegurar los flujos de información adecuados para el desarrollo de los procesos y el cumplimiento de los fines misionales del IDPC*".

La caracterización se encuentra definida en el marco del ciclo PHVA, sin embargo, se evidencia que la misma es demasiado extensa, conteniendo actividades que pueden estar inmersas en otras, como es el caso de:

"1. Planear las actividades definidas para salvaguardar la información. 2. Planear campañas de sensibilización con temas de seguridad",

La cual se encuentra dentro del Planear, no obstante, esta acción hace parte integral de la Política de Seguridad.

De igual manera, como actividades que hacen parte del Hacer se encuentran:

ACTIVIDAD	OBSERVACIÓN
Realizar las acciones pertinentes para atender los servicios y/o requerimientos de soporte técnico en materia de hardware o software.	De esta actividad se encuentra como soporte "*Solución y cierre de la solicitud debidamente documentada en la Mesa de Ayuda*", sin embargo, una vez revisada la información aportada por el proceso, como se evidenciará más adelante, este registro no se encuentra de esta manera, por lo cual no es posible hacer un seguimiento al cumplimiento de los tiempos establecidos.
1. Ejecutar y controlar los proyectos relacionados con tecnología de la información y las comunicaciones. 2. Brindar apoyo técnico a los procesos previos a la adquisición de bienes o contratación de	De acuerdo con las salidas incluidas en la caracterización "*Reportes / Informes / Justificación / apoyo en el estudio de mercado*", no obstante, es importante mencionar que los proyectos de tecnología de la información no se

ACTIVIDAD	OBSERVACIÓN
servicios que incluyan un componente tecnológico, a cargo de las dependencias del IDPC.	ciñen únicamente a la contratación, sino a las diferentes actividades que se realizan para dar cumplimiento al PETI, no obstante, al no contar con unos proyectos definidos como se observará más adelante, no se puede realizar una adecuada ejecución y control de los mismos. De igual manera, se evidencian debilidades en cuanto al apoyo técnico.
1. Administrar y garantizar el correcto funcionamiento de la Intranet 2. Publicación y actualización de información en la Intranet, de acuerdo a las solicitudes que realicen.	Estas actividades pueden ser unificadas como atención de requerimientos, así como se encuentra en el procedimiento definido.
1. Gestionar la apertura, inactivación, eliminación, backup y archivo de las cuentas de correo institucional. 2. Elaborar y divulgar instrucciones de uso del correo institucional.	
1. Coordinar los servicios de mantenimiento y desarrollo de TI. 2. Administrar la infraestructura tecnológica sobre la cual se soportan los sistemas de información del IDPC (Servidores, Redes y Bases de Datos). 3. Diseñar y ejecutar un Plan anual de Mantenimiento Preventivo y Correctivo.	Dentro de los procedimientos no se encuentra el plan de mantenimiento definido, ni hace parte de los documentos de planeación de este proceso.
Ejecutar acciones que garanticen el respaldo de la información	Actividad bien definida
Brindar apoyo en el cargue y depuración de datos en aplicativos externos, para la generación de los siguientes informes institucionales: 1. Informes de Contabilidad 2. Informes de Presupuesto 3. Informes de Contratación 4. Informes de Balance Social 5,Control fiscal interno 6.control fiscal interno especiales 7. Gestión y resultados 8. Personal y costos 9. CGR presupuestal 10. Plan de Mejoramiento	Si bien es una acción que se encuentra a cargo del área de Sistemas, puede hacer parte de una actividad macro. De igual manera, se evidencian debilidades en su cumplimiento.
1. Gestión y apoyo técnico al sistema de gestión documental Orfeo 1. Actualización y administración de bases de datos 2. Pruebas funcionales 4. Seguimiento para mejora continua	Esta actividad no hace parte de los procedimientos definidos, de igual manera, se pueden unificar estas acciones.
Generar la articulación adecuada de los sistemas de información del IDPC	

ACTIVIDAD	OBSERVACIÓN
Ejecutar los planes institucionales propios del proceso para contribuir con la gestión y el desempeño institucional	El seguimiento a la ejecución de los planes se realiza mediante el POA, no obstante, es importante mencionar que en la revisión realizada durante la vigencia 2019 por la Asesoría de Control Interno a este instrumento se evidenció que se cuenta con un documento en Excel que contempla los procesos de contratación, por lo cual es importante mencionar que los planes y proyectos de tecnología de la información no se ciñen únicamente a la contratación, sino a las diferentes actividades que se realizan para dar cumplimiento a los mismos, sin embargo, al no contar con unos proyectos definidos como se observará más adelante, no se puede realizar una adecuada ejecución y control de los mismos.
Ejecutar los controles definidos en la matriz de riesgos, así como el plan de tratamiento para los riesgos	Actividad bien definida
Ejecutar las actividades programadas en el plan de mejoramiento	Actividad bien definida
Atender las PQRS y las comunicaciones internas que se le asignen la proceso con oportunidad	Actividad bien definida

Para finalizar, dentro de las actividades definidas en el Actuar no deben ir las actualizaciones de manuales, procedimientos, riesgos e indicadores, ya que en esta etapa se deben tomar las acciones necesarias en caso de identificar alguna debilidad en la ejecución del proceso.

1.1.2 Manual de Seguridad de la Información

Este manual se encuentra en su versión 1 del 27 de septiembre de 2019, el cual tiene como objetivo:

"*Proteger, asegurar y garantizar la confidencialidad, autenticidad, integridad, disponibilidad y confiabilidad de los activos de información del Instituto Distrital de Patrimonio Cultural, alineadas a los objetivos estratégicos de la entidad, a través de la formulación e implementación de políticas, medidas de seguridad y mecanismos de control*".

La evaluación de este instrumento se ve reflejada en el numeral 1.4

1.1.3 Plan de Seguridad de la Información

Este plan se encuentra en su versión 2 del 28 de enero de 2020, el cual tiene como objetivo:

"*Presentar el plan de seguridad y privacidad de la información del IDPC y los elementos que lo conforman, como marco de referencia para el establecimiento y regulación de lineamientos y*

medidas que permitan el aseguramiento de la protección y uso adecuado de la información y activos de información que la soportan al interior de la Entidad".

La evaluación de este instrumento se ve reflejada en el numeral 1.4

1.1.4 Plan Tratamiento de Riesgos de Seguridad de la Información

Este plan se encuentra en su versión 2 del 28 de enero de 2020, el cual tiene como objetivo:

"*Brindar al Instituto una herramienta con enfoque sistemático que proporcione las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información, a través de métodos que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y expedición de políticas así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo*".

La evaluación de este instrumento se ve reflejada en el numeral 1.4

1.1.5 Plan Estratégico de Tecnologías de la Información PETI 2016-2020

Este plan se encuentra en su versión 4 del 28 de enero de 2020, el cual tiene como objetivo:

"*Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital*".

La evaluación de este instrumento se ve reflejada en el numeral 1.3

1.1.6 Procedimiento Atención de requerimientos de recursos Tecnológicos

Este procedimiento se encuentra en su versión 2 del 17 de julio de 2019, el cual tiene como objetivo:

"*Gestionar oportunamente las incidencias y peticiones asociadas a la operación de los recursos tecnológicos disponibles en el IDPC, radicadas y gestionadas a través de la Mesa de ayuda*".

Dentro de este se evidencian como debilidades:

- No cuenta con normatividad asociada.
- Dentro de las políticas se encuentra la atención de peticiones e incidencias dentro de las 24 horas, no obstante, el cumplimiento de esta no pudo ser verificada, teniendo en cuenta que la información entregada por el proceso no permitía realizar esta revisión, como se evidenciará más adelante. Ver numeral 1.5

1.1.7 Procedimiento Backup y restauración de la Información

Este procedimiento se encuentra en su versión 2 del 27 de septiembre de 2019, el cual tiene como objetivo:

"*Proteger la información, bases de datos y documentación crítica para la entidad, con el fin de conservar los respaldados que permitan la recuperación de archivos ante los eventos que se puedan presentar*".

De manera general, se encuentra bien definido el procedimiento de Backup y cuenta con puntos de control, no obstante, no se pudo realizar una verificación del cumplimiento del mismo, ya que para la presente vigencia se contó con la excepción del aislamiento preventivo, por lo cual, no se siguió estrictamente el procedimiento.

1.2 SEGUIMIENTO RIESGOS DE GESTIÓN, SEGURIDAD DE LA INFORMACIÓN Y DE PROVEEDORES

Para realizar la revisión de los riesgos se tomó como base la información remitida por el proceso en materia de riesgos de proveedores y de seguridad de la información, en relación con los de gestión, teniendo en cuenta que se realizó su verificación en el informe de seguimiento a riesgos presentado por esta Asesoría de Control Interno, en este informe se incluyen recomendaciones para actualizar las matrices de riesgo existentes.

1.2.1 Riesgos de Gestión

Se tienen definidos 2 riesgos para el proceso, cuyos controles y planes de manejo se han venido desarrollando con algunas debilidades. Es importante mencionar que estos se encuentran enfocados al daño o pérdida de infraestructura tecnológica o información, sin embargo, teniendo en cuenta el objetivo del proceso tan amplio, así como las actividades definidas dentro de la caracterización se pueden adicionar algunos riesgos encaminados a la ejecución de los planes y proyectos, fallas en sistemas de información, demoras en la atención de requerimientos, debilidades en apoyo técnico prestados, entre otros.

1.2.2 Riesgos de Seguridad de la Información

Si bien se cuenta con un Plan de Tratamiento de Riesgos de Seguridad de la Información, no se cuenta con la identificación de los mismos, por lo cual desde la Asesoría de Control Interno sugiere tener en cuenta algunos temas generales como: ataques cibernéticos, control de acceso, control de software licenciado, entre otros.

1.2.3 Riesgos de Proveedores

En cuanto al monitoreo de los riesgos relacionados con los contratistas o proveedores en relación a los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación, se manifiesta por el auditado que:

"*Los riesgos identificados corresponden a la etapa de planeación, ejecución, selección y evaluación y, se clasifican como de tipo operacional, jurídico y tecnológico.*

Los controles establecidos para dichos riesgos son monitoreados por el apoyo y la supervisión del contrato de acuerdo con la periodicidad establecida. En este caso en particular los controles no tienen una periodicidad específica, porque solo se ejecutan durante el proceso precontractual, de

ejecución y/o pos contractual, es decir cuando se presenta el proceso de contratación y durante el término de su duración. A la fecha ningún riesgo se ha materializado.

Las valoraciones de los riesgos son bajo (en la mayoría de los casos), medio y alto (en una proporción menor) y la responsabilidad del riesgo es en algunos casos responsabilidad (sic) del contratista y en otra responsabilidad de la entidad. El tratamiento de los riesgos se enmarca en la categoría "reducir el riesgo", es decir que las medidas que han sido establecidas por el proceso tienen por objetivo reducir la probabilidad y el impacto del riesgo y para ellos e (sic) han establecido controles.

En cuanto al seguimiento de los controles, estos se realizan a través del Sistema Electrónico de Compras Públicas –SECOP-, plataforma en la que se inscribe, aprueba y hace seguimiento a todo el proceso de gestión contractual, desde la etapa de planeación, la ejecución y la finalización del contrato. Como evidencia queda registrado en SECOP el desarrollo de todo el proceso de gestión contractual. Las observaciones y desviaciones de los riesgos se atienden de manera oportuna una vez se evidencian durante la ejecución del control y pueden subsanarse a través de correos electrónicos u oficios al contratista solicitando completar información del proceso contractual o responder a situaciones inmediatas que pueden derivar en la materialización de un riesgo."

De lo anterior se infiere que se cuenta con las matrices de riesgo establecidas y se han venido ejecutando los controles y acciones propuestas por cada uno de los responsables, de igual manera que no se ha presentado materialización de riesgos, no obstante, es importante resaltar que para realizar una adecuada administración y gestión de riesgos es necesario realizar monitoreo periódico a las matrices de riesgos y dejarlo documentado con el fin de contar con la trazabilidad de lo ocurrido en el proceso contractual para así tomar las acciones que se requieran a futuro. Así mismo, se resalta que esta actividad se encuentra definida en el numeral 6.14 del Manual de Seguridad vigente de la Entidad, para la cual no se tiene soporte de su cumplimiento.

1.3 PETI –PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN 2016-2020

Si bien se trata de un PETI con una vigencia de 4 años, en la actualización que surtió en el año 2020, el organigrama y las funciones descritas en el PETI no fueron actualizados en concordancia con el Acuerdo 01 del 21 de enero de 2019. Aún se menciona a la Secretaría General en el Organigrama y no se tiene en cuenta la Oficina Asesora de Planeación.

No se evidencia la misión y visión de la entidad.

1.3.1 Construcción del PETI

La guía para la construcción del PETI, cuenta con una serie de pasos y requisitos que hacen parte de la planeación del área para la construcción del mismo, es por ello, que esta Auditoría se enfocó en el numera 7.9.1 de la guía, la cual desarrolla la construcción del PETI, es decir, cuál debe ser su contenido, utilizando las herramientas señaladas en los capítulos anteriores.

Dado lo anterior, se identificará, si se cumplió o no con el numeral 7.9.1. "*Desarrollo de la sesión*"

1. "*Construir la introducción, el objetivo y alcance del PETI en el primer capítulo del documento. La introducción deberá describir el trabajo que se ha realizado durante los últimos años en el*

habilitador de arquitectura, los PETI anteriores y el trabajo futuro por ejecutar. El alcance deberá describir los elementos que contiene el documento. El objetivo deberá incluir la definición de los pasos a seguir para lograr los objetivos de los componentes y propósitos de la Política de Gobierno Digital utilizando los habilitadores de Arquitectura, Seguridad y Privacidad y Servicios Ciudadanos Digitales."

No se evidencia introducción, se describe el objetivo, pero no hay ninguna relación del trabajo llevado a cabo en los últimos años, como tampoco lo que se encuentra pendiente por ejecutar. No se definen los pasos para lograr los objetivos allí propuestos.

2. "*Construir un Marco normativo utilizando como plantilla la tabla de normatividad construida en la Sesión 7: Analizar el entorno y la normatividad vigente, estableciendo el segundo capítulo del documento."*

Se definió el marco normativo, sin embargo, se evidenció que, las siguientes normas relacionadas en el PETI, ya están derogadas o su tipología no corresponde, así:

- Decreto 053 de 2002, Derogado por el artículo 26 del Decreto 510 del 27 de agosto de 2019.
- Decreto 397 de 2002, Derogado por el artículo 2 del Decreto Distrital 319 de 2011 y este a su vez Derogado por el artículo 7 del Decreto Distrital 077 de 2012.
- Resolución 001 de 2003, Derogada por el art. 30, Resolución de la C.D.S. 256 de 2008
- Directiva 305 de 20 de octubre de 2008, sin embargo, al consultar no es una Directiva sino una Resolución expedida por la Comisión Distrital de Sistemas (CDS) de Bogotá D.C, la cual tiene algunas derogatorias mediante la Resolución 02 de 2011. Igualmente, la Resolución 004 de 2017 le introduce algunas modificaciones.
- Resolución 378 de 2008, fue derogada por el Artículo 6 (sic) de la resolución 003 de 2017 -C.D.S-.
- Decreto 1151 de 2008, Derogado por el Decreto 2693 del 21 de Diciembre de 2012 y este a su vez fue derogado por el art. 14 del Decreto Nacional 2573 de 2014.
- Decreto 1747 de 2000, Derogado por el art. 22, Decreto Nacional 333 de 2014

3. *"Presentar el entendimiento estratégico mediante la estrategia de la entidad identificada en la Sesión 2: Entender la estrategia y mostrar la alineación de la estrategia de TI describiendo cada uno de los objetivos y metas de TI definidos en la Sesión 11: Construir la estrategia de TI y presentar la última medición de las metas de TI."*

Si bien se definieron las estrategias, estas no contaron con metas medibles, es decir, qué se deseaba y cómo se lograría, si esta se podría o no alcanzar con los recursos asignados y si la meta era o no importante para el área.

En conclusión, las estrategias no cuentan con metas medibles.

4. *"Presentar la hoja de ruta construida en la Sesión 17: Construir la hoja de ruta y describir cada una de las iniciativas gastos de operación utilizando las fichas de iniciativas y de gastos propuestas en esta sesión."*

No se observó la identificación de los gastos con componentes de TI asociados a la operación utilizando como insumo los recursos y roles identificados en el Modelo operativo y la planeación presupuestal de las vigencias anteriores.

No se evidencian fichas de iniciativa de inversión y de gastos de operación, es decir, para cada vigencia cuánto se tenía, cuánto se gastó y cuánto se requería para terminar cada proyecto.

5. *Describir la situación actual mediante la información generada en las sesiones de la segunda fase, utilizando las fichas de servicio construidas en la Sesión 5: Evaluar y comprender los servicios y el Modelo operativo construido en la Sesión 4: Identificar y caracterizar la operación. Como introducción a este capítulo se puede utilizar la tabla de caracterización de servicios."*

No se evidenció la medición de cuáles servicios debería ser mejorados con el uso de las TIC, esto es, aquellos de mayor impacto como tampoco las capacidades para llevarlas a cabo.

6. *"Describir la situación objetivo utilizando el catálogo de brechas construido en la Sesión 13: Identificar las brechas y la demás información que se generó a través de las sesiones de la tercera fase."*

No se observa la definición de brechas que permitan identificar las mejoras en los servicios y en la operación.

7. *"Incluir el estado actual del tablero de indicadores de TI de la Sesión 20: Definir el seguimiento y control del PETI."*

No se evidenciaron indicadores para evaluar el control y seguimiento sobre las inversiones.

8. *"Presentar el Plan de comunicaciones del PETI que se va a utilizar para comunicar el PETI utilizando el listado de comunicaciones y la matriz de interesados definidos en la Sesión 18: Definir las Comunicaciones del PETI."*

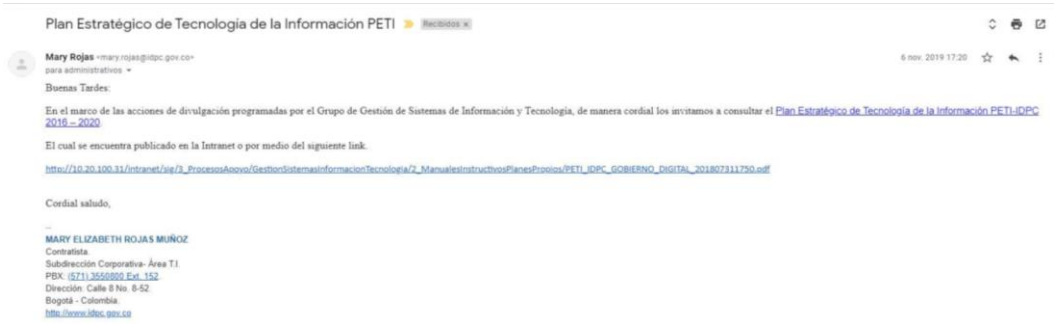
En Reunión virtual llevada a cabo el 4 de noviembre de 2020, se le indagó a la responsable de Sistemas, Ingeniera Mary Rojas sobre el Plan de comunicaciones del PETI y actividades desarrolladas durante el período evaluado, respondiendo lo siguiente:

"*se enviaron correos informativos al grupo denominado "administrativos" y una publicación en la intranet."*

Se le preguntó si tenía prueba de ello, indicando que "*la publicación se realizó en la intranet del 26 de septiembre de 2019 y los correos procederá a buscarlos y a aportarlos."*

La Asesora de Control Interno, le pregunta si se programó está comunicación, para lo cual informa que "*no hay programación de publicación o comunicación a través de un cronograma."*

Atendiendo lo anterior, mediante correo electrónico del 6 de noviembre aporta los siguientes pantallazos:


Plan Estratégico de Tecnología de la Información PETI

Mary Rojas <mary.rojas@idpc.gov.co>
para administrativos

6 nov. 2019 17:20

Buenas Tardes:

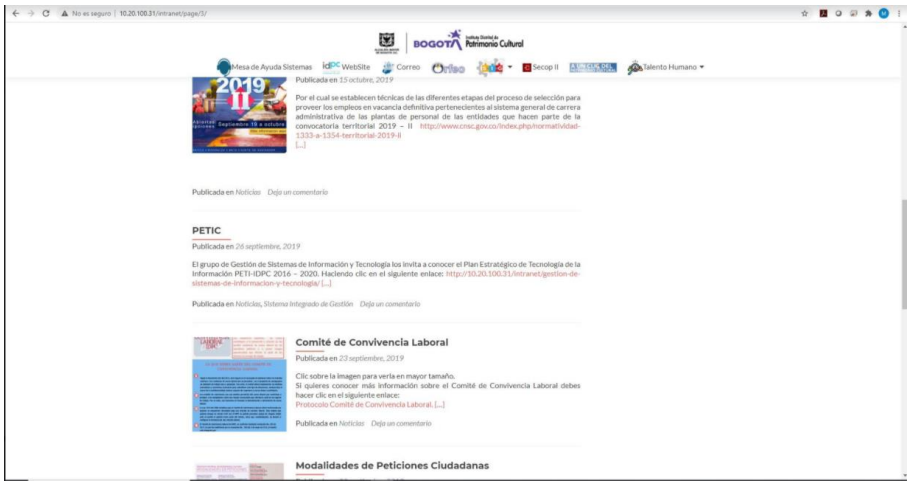
En el marco de las acciones de divulgación programadas por el Grupo de Gestión de Sistemas de Información y Tecnología, de manera cordial los invitamos a consultar el Plan Estratégico de Tecnología de la Información PETI-IDPC 2016 – 2020

El cual se encuentra publicado en la Intranet o por medio del siguiente link.

http://10.20.100.31/intranet/sig/3_ProcesosApoyo/GestionSistemasInformacionTecnologia/2_ManualesInstructivosPlanesPropios/PETI_IDPC_GOBIERNO_DIGITAL_20180731750.pdf

Cordial saludo,

MARY ELIZABETH ROJAS MUÑOZ
Contratista
Subdirección Corporativa- Área T.I.
PBX: (571) 3550800 Ext. 152
Dirección: Calle 8 No. 8-52
Bogotá - Colombia
http://www.idpc.gov.co



Se evidencia entonces que en efecto el 26 de septiembre de 2019, se realizó la correspondiente publicación en la intranet, así como correo del 6 de noviembre de 2019, se remitió correo a los funcionarios de la entidad, donde se les invita a consultar el PETI 2016-2020.

No obstante, no se observa divulgación de la modificación efectuada en la vigencia 2020, como tampoco existe dentro del PETI el Plan de Comunicaciones definida en esta sesión.

9. *"Las entidades que han desarrollado un PETI con anterioridad deben validar los entregables con la nueva versión de la guía. La sesión específica que explica esta equivalencia es Sesión 23: Validar equivalencias y relación de evidencias."*

N/A

Si bien la entidad presentó su PETI, en el cual de manera muy general se evidencian los proyectos a realizar en la vigencia 2017-2020, no se observa que se haya tenido en cuenta la guía para llevarlo a cabo, lo que dificulta tener un panorama más claro de cómo, cuándo y con qué se van a desarrollar dichos proyectos.

Es preciso indicar que, los proyectos definidos en el documento denominado "PETI" y que se relacionan, no pudieron ser objeto de análisis por cuanto estos no fueron desarrollados en el PETI, como tampoco en documentos adicionales.

PROYECTO_1. Actualización de la plataforma tecnológica de la entidad.
PROYECTO_2. Fortalecimiento y sostenibilidad del Sistema Integrado de Gestión – Implementación Orfeo
PROYECTO_3. Fortalecimiento de las plataformas web y correo electrónico de la entidad
PROYECTO_4. Sistema de respaldo de datos (Backup)
PROYECTO_5. Actualización de versión Sistema de Mesa de ayuda (Helpdesk)
PROYECTO_6. Modelo de Seguridad y Privacidad de la Información
PROYECTO_7. Actualización y proyección de Documentación-Proceso de Apoyo de Gestión de Sistemas de Información.
PROYECTO_8. Implementación de Gobierno Digital
PROYECTO_9. Sistema Integrado de Conservación de documentos Digitales

Así las cosas, no se encontró prueba que permita establecer si estos proyectos fueron terminados, qué recursos se invirtieron, en cuánto tiempo se desarrollaron, si aún hay alguno en proceso, lo que conlleva al incumplimiento no solo de la guía de Gobierno Digital, sino además con el principio de planeación, esto teniendo en cuenta que los proyectos deben ir armonizados con los proceso y objetivos propuestos por la entidad y deben garantizar no solo su ejecución e implementación en el lapso de tiempo propuesto, sino que además con los recursos asignados, a los cuales se les debe hacer seguimiento periódicamente.

Y así lo ratificó la actual responsable de sistemas, Ingeniera Mary Rojas, en reunión virtual adelantada el 4 de noviembre de 2020 cuando se le indagó dónde estaban definidos los proyectos con su meta, desarrollo, cumplimiento y terminación, a lo que respondió que, "*en el PETI objeto de esta auditoría no se discriminaron los proyectos, presupuesto y cronograma, en conclusión, en el PETI no se encuentran metas, desarrollo cumplimiento y terminación de estos*."

Adicionalmente, es necesario indicar que los numerales 1, 4 y 13 del artículo 2.2.35.3 del Decreto 1083 de 2015, indican, entre otros aspectos, lo siguiente:

1 (…) "*que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado*."

(…)
3 "*Liderar la gestión, seguimiento y control de la ejecución de recursos financieros asociados al portafolio de proyectos y servicios definidos en el plan estratégico de Tecnologías y Sistemas de información."*

1.3.2 Reportes y/o informes de ejecución de proyectos relacionados con tecnología de la información y las comunicaciones.

El auditado reporta los siguientes contratos:

Objeto del Contrato	Número de Contrato	Valor del Contrato	Fecha del Contrato	Estado
Contratar la adquisición de licencias de software para los equipos de cómputo del Instituto	IDPC-CV-427-2019	$ 65,310,488	11 de Julio de 2019	Ejecutado

Objeto del Contrato	Número de Contrato	Valor del Contrato	Fecha del Contrato	Estado
Distrital de Patrimonio Cultural.				
Adquisición e instalación de los accesorios de red para las conexiones de datos de casa Genoveva del Instituto Distrital de Patrimonio Cultural.	IDPC-CV-463-2019	$ 9,000,140	19 de septiembre de 2019	Ejecutado
Adquisición de UPS para la regulación de energía de la sede Casa Genoveva	IDPC-CV-472-2019	$ 26,037,200	4 de Octubre de 2019	Ejecutado
Adquisición de servicios de mantenimiento, actualización y soporte de la mesa de ayuda Proactivanet del Instituto Distrital de Patrimonio Cultural.	IDPC-PS-502-2019	$ 21,500,000	10 de Diciembre de 2019	Ejecutado, sin embargo hay una obligación que se dará cuando se requiera relacionada con el soporte.
Contratar la renovación de las licencias, soporte y capacitación del equipo de seguridad perimetral fortigate 100D de propiedad del instituto distrital de patrimonio cultural.	IDPC-PS-231-2020	$ 11,081,228	6 de Marzo de 2020	Ejecutado, sin embargo hay una obligación que se dará cuando se requiera relacionada con el soporte.
Contratar el alquiler e instalación de computadores de escritorio con su respectiva configuración y puesta en funcionamiento en las instalaciones del instituto distrital de patrimonio cultural	IDPC-PS-244-2020	$ 104,500,000	01 de Abril de 2020	Se realizó la entrega de 65 equipos de cómputo por parte de la empresa TECHNOLOGY WORLD
Contratar la renovación y actualización de licencias de software antivirus para los equipos de cómputo del instituto distrital de patrimonio cultural, en el marco del fortalecimiento institucional	IDPC-PS-277-2020	$ 30,933,308	22 de Abril de 2020	En ejecución, el plazo de este contrato es de 3 años, se indica que la empresa entregó 300 licencias software antivirus.
Contratar la renovación y ampliación del almacenamiento de la solución de respaldo de información para el instituto distrital de patrimonio cultural	IDPC-PS-284-2020	$ 99,300,000	24 de Abril de 2020	En ejecución

Se evidencia la suscripción de varios contratos para el área de tecnología, y según las tablas en Excel reportadas, se les viene haciendo seguimiento a las obligaciones a cada uno de ellos, no obstante, es necesario indicar que estos contratos no fueron establecidos dentro del Plan Estratégico de Tecnología de la Información, reiterando que los mismos deben obedecer al resultado de un adecuado ejercicio de planeación, realizándose previamente la definición de portafolios de proyectos y un proceso de transformación que involucre tecnologías digitales.

La guía de Gobierno Digital para la elaboración del PETI, es clara en determinar que los proyectos deberán estar orientados por algunos principios, las estructuraciones de ellos tendrán que contar con unos tiempos y costos definidos, y serán tenidos en cuenta para la actualización del PETI. Situaciones que ya fueron evidenciadas dentro del análisis del PETI, pero que además, ratifica la debilidad en dicha estructuración.

En conclusión, se debe alinear el PETI al Plan estratégico de la entidad siguiendo los lineamientos de la Guía del MinTic y otras normas vigentes.

1.3.3 Apoyo técnico a los procesos previos a la adquisición de bienes o contratación de servicios que incluyan un componente tecnológico.

Para este punto, el auditado adjunta los contratos suscritos entre julio de 2019 y junio de 2020, y documentos del contrato obviando la pregunta de fondo, la cual va encaminada a que se demuestre cuál fue la planeación y en qué se soportó técnicamente **previo** a la adquisición de bienes.

Es importante mencionar que la evidencia es el pilar de cualquier auditoría, por lo que cuando esta no sea suficiente, adecuada y eficaz, no se podrán emitir conclusiones razonables en la auditoría.

No puede entonces, el auditado enviar información indistinta, trasladándole al auditor la responsabilidad de buscar lo que requiera. Así las cosas, esta respuesta se tendrá como no aportada.

De igual manera, en cuanto al apoyo técnico para la adquisición de bienes o contratación de servicios que incluyan un componente tecnológico, dentro del informe de seguimiento a la Austeridad en el Gasto realizado por esta Asesoría de Control Interno, se evidenció que no se dejaba documentado análisis de ventajas y desventajas en la compra o arrendamiento de estos bienes, a través de la implementación de mejores prácticas, valoración de todos los costos tanto fijos como variables, entre estos: los seguros, actualizaciones, mantenimiento, licenciamiento, etc., análisis que deberá reflejarse en el respectivo estudio del sector.

1.4 SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La revisión de este punto se basa en el Modelo de Seguridad y Privacidad de la Información planteado por Ministerio de Tecnologías de la Información y las Comunicaciones, este tiene 3 componentes que corresponden a: 1. Seguridad de la Información, 2. Privacidad de la Información y 3. Adopción del Protocolo IPv6.

1.4.1 Seguridad de la Información

Este componente contempla un ciclo de funcionamiento a través de 5 fases a saber: Diagnóstico, Planificación, Implementación, Evaluación del Desempeño y Mejora Continua.

1.4.1.1 Fase de Diagnóstico – Etapas previas a la Implementación

De acuerdo con lo establecido en el Modelo, en esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, identificando el nivel de madurez y las vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación. No obstante, no se evidencia que esta fase haya sido desarrollada por el IDPC previo a la etapa de planificación, ya que en el Plan de Seguridad definido se manifiesta que se debe desarrollar, más no el resultado obtenido.

1.4.1.2 Fase de Planificación

El modelo establece que:

(…)
"*esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo*".

Dentro de esta fase se contemplan como resultados:

- Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.
- Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.
- Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.
- Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.
- Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección.
  Matriz con la identificación, valoración y clasificación de activos de información.
  Documento con la caracterización de activos de información, que contengan datos personales
  Inventario de activos de Ipv6
- Integración del MSPI, con el sistema de gestión documental de la entidad.
- Documento con la metodología de gestión de riesgos.
  Documento con el análisis y evaluación de riesgos.
  Documento con el plan de tratamiento de riesgos.
  Documento con la declaración de aplicabilidad.
  Documentos revisados y aprobados por la alta Dirección.
- Documento con el plan de comunicación, sensibilización y capacitación para la entidad.

- Documento con el Plan de diagnóstico para la transición de Ipv4 a Ipv6.

1.4.1.2.1 Política de seguridad y privacidad de la información.

La Política de Seguridad del IDPC, se encuentra definida dentro del Manual de Seguridad de la Información, esta contiene declaración regulación y responsables; teniendo en cuenta las recomendaciones fijadas en el Modelo de Seguridad y Privacidad de la Información, así como en la Guía No. 2 Elaboración de la política general de seguridad y privacidad de la información de MinTIC, no se evidencian lo objetivos, alcance y nivel de cumplimiento. Adicionalmente, es importante mencionar que esta política no contempla la Privacidad de la Información, de igual manera, el Manual no fue aprobado por la Alta Dirección.

Para verificar su divulgación se le solicitó al auditado los soportes, evidenciando que el Manual de Seguridad fue publicado en la intranet el 29 de enero de 2020 para el acceso de todos los funcionarios, sin embargo, teniendo en cuenta la importancia de este documento en la Entidad, se recomienda generar otros medios con el fin de garantizar su aplicación.

1.4.1.2.2 Manual de Políticas de Seguridad y Privacidad de la Información.

De acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información:

"*Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información*

En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente.

La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación"

Para lo cual, la Entidad cuenta con el Manual de Seguridad, no obstante, este se centra únicamente en la seguridad, excluyendo la privacidad de la información, que si bien se menciona en la Política de Protección de Datos, no se desarrolla completamente, como se evidencia en el numeral 1.4.2

En la Guía No. 2 Elaboración de la política general de seguridad y privacidad de la información de MinTIC, se presentan algunas recomendaciones de políticas de seguridad de la información para el Modelo de Seguridad y privacidad de la Información para las Entidades del Estado, las cuales se relacionan a continuación contrastando con las del IDPC:

POLÍTICAS SUGERIDAS MINTIC	POLÍTICAS IDPC
Organización de la Seguridad de la Información Gestión de Activos Control de Acceso No Repudio Privacidad y Confidencialidad Integridad	Software y licenciamiento Uso de Recursos Tecnológicos Carpetas de Red, Discos de Red, Carpetas Virtuales Respaldo y restauración de la información Control de Acceso Manejo de Contraseñas para

POLÍTICAS SUGERIDAS MINTIC	POLÍTICAS IDPC
Disponibilidad del Servicio e Información Registro y Auditoría Gestión de Incidentes de Seguridad de la Información Capacitación y Sensibilización en Seguridad de la Información	Administradores de Tecnología Transferencia de Información Seguridad para la relaciones con Proveedores Uso de Internet Uso de Correo Electrónico Tercerización o Outsourcing

Si bien las políticas propuestas por MinTIC no son obligatorias, si es importante revisar cuáles de ellas son aplicables en el IDPC, de igual manera, darle más relevancia a las políticas de Privacidad y Confidencialidad.

Ahora bien, en relación con el cumplimiento de las políticas establecidas por el IDPC se evidencia lo siguiente:

1.4.1.2.2.1 Software y Licenciamiento

Para verificar el cumplimiento de esta política se solicitó lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas, recibiendo la siguiente información

SOFTWARE LIBRE	
NOMBRE	**CARACTERÍSTICA**
Adobe Reader	Visualizador de archivos PDF
Java	Complemento para aplicaciones
Google Chrome	Navegador de Internet
Mozilla Firefox	Navegador de Internet
Safari	Navegador de Internet equipos MAC
E-Pass	Software para instalación de Firma Electrónica
Putty	Software para conexión de equipos de red
Visor de Autocad	Visor gratuito para planos de Autocad
7 ZIP	Software para comprimir y descomprimir archivos
Chrome Remote Desktop	Software de conexión remota
Google Earth pro	Software que permite visualizar múltiple cartografía
Explorador KSI	Firma de documentos enviados a entes de control
Chip	Software de Contaduría General
Sivicof	Software Transmisión de información a la contraloría
Segplan	Software de seguimiento al plan de desarrollo de Bogotá
Presenter Light	Software de proyección de video beam
Epson Power Light	Software de proyección de video beam
Google Drive File Stream	Sincronización de documentos en línea
Open Office	Suite de ofimática libre
Complemento de Access Runtime	Permite probar aplicaciones de Microsoft Access
SAP	Cliente de conexión Bogdata

SOFTWARE LICENCIADO	
NOMBRE	**CARACTERÍSTICA**
Windows Server 2008	Sistema Operativo de Servidores
Windows Server 2016	Sistema Operativo de Servidores
Windows 7	Sistema Operativo PC
Windows 8	Sistema Operativo PC
Windows 10	Sistema Operativo PC
Microsoft Office 2010	Paquete de Ofimática
Microsoft Office 2013	Paquete de Ofimática
Microsoft Office 2016	Paquete de Ofimática
Antivirus Kaspersky	Antivirus
ADOBE PHOTOSHOP CC	Licencia de Diseño Grafico
PROJECT STD 2019OLP NLGOV	Licencia de seguimiento de proyectos
PDF PRO	Licencia para convertir archivos pdf
SKETCHUP PRO	Licencia de Diseño Grafico
ADOBE CLOUD	Licencia de Diseño Grafico
ADOBE ILUSTRATOR CC – CREATIVE	Licencia de Diseño Grafico
AUTOCAD 2019 3D	Diseño de Planos
LICENCIAS ARCGIS FOR DESKTOP	Licencias de Georeferenciación
LICENCIA FILE MAKER PRO ADVANC	Licencias de Colecciones Colombianas
Explorer	Navegador
Google Chrome	Navegador
Mozilla Fire Fox	Navegador
SIIGO	Sistema de Contabilidad e Inventarios

Con las tablas entregadas no es preciso evidenciar en qué equipos se tiene instalado, o quiénes son los responsables, sumado a ello y por el limitante mencionado al inicio de este informe, esta auditoría no realizó pruebas in situ, lo que impidió establecer si se tiene o no instalado un software diferente a los mencionados en el listado que antecede.

Es importante mencionar que, en reunión virtual con la encargada de Sistemas, al respecto, nos indicó "*se evidenció que algunos equipos contaban con el autocad estudiantil, esto debido a que las licencias que se tenían no eran suficientes para la cantidad de arquitectos y estas son gratuitas, sin embargo, teniendo en cuenta que estaban instaladas en equipos de la entidad, se desinstaló y a esas personas se les asignó un equipo de alquiler ya que en estos sí se podía instalar por no ser equipos propios, ya para este año se adquirieron las licencias de un aforo más grande para los arquitectos.*"[1]

Consultado contrato IDPC-CV-427-2019, se evidenció que, para el año 2019 se adquirieron, cinco (5) licencias AUTOCAD 2019 3D Full Versión y para la vigencia 2020 se renovaron estas licencias y se adquirieron 19 más, a través del contrato IDPC-CV-298-2020, sin que se pueda demostrar si son suficientes o se continúa teniendo este software sin licencia en equipos de arrendamiento.

[1] Acta del 4 de noviembre de 2020

Revisando el contrato de arrendamiento de equipos de cómputo se evidencia que en la cláusula 29. Derechos de Autor se estipuló "*EL CONTRATISTA y EL INSTITUTO, declaran que la información recolectada y los productos generados en el marco del presente contrato, independientemente de su grado de desarrollo, pertenecen exclusivamente a EL INSTITUTO, entidad a la que corresponden los derechos de propiedad intelectual, desde su inicio hasta su materialización física en los términos establecidos en la Ley 23 de 1982, o sus modificaciones. Si es el caso, todos los productos serán entregados al Supervisor del contrato en medios impresos y magnéticos. La utilización y difusión de los productos resultantes se realizarán bajo la autorización expresa de EL INSTITUTO*."

Igualmente, en el Manual de Seguridad de la Información se establece:

"*El IDPC instalará los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización del IDPC (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para el Instituto, por lo que ésta práctica no está autorizada.*

Todo el software usado en la plataforma tecnológica del IDPC debe tener su respectiva licencia y acorde con los derechos de autor*.*

Los programas instalados en los equipos, son de propiedad del IDPC, la copia no autorizada de programas o de su documentación, implica una violación a la política general del IDPC. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por el IDPC o las sanciones que especifique la ley". (Subraya y negrita fuera de texto original)

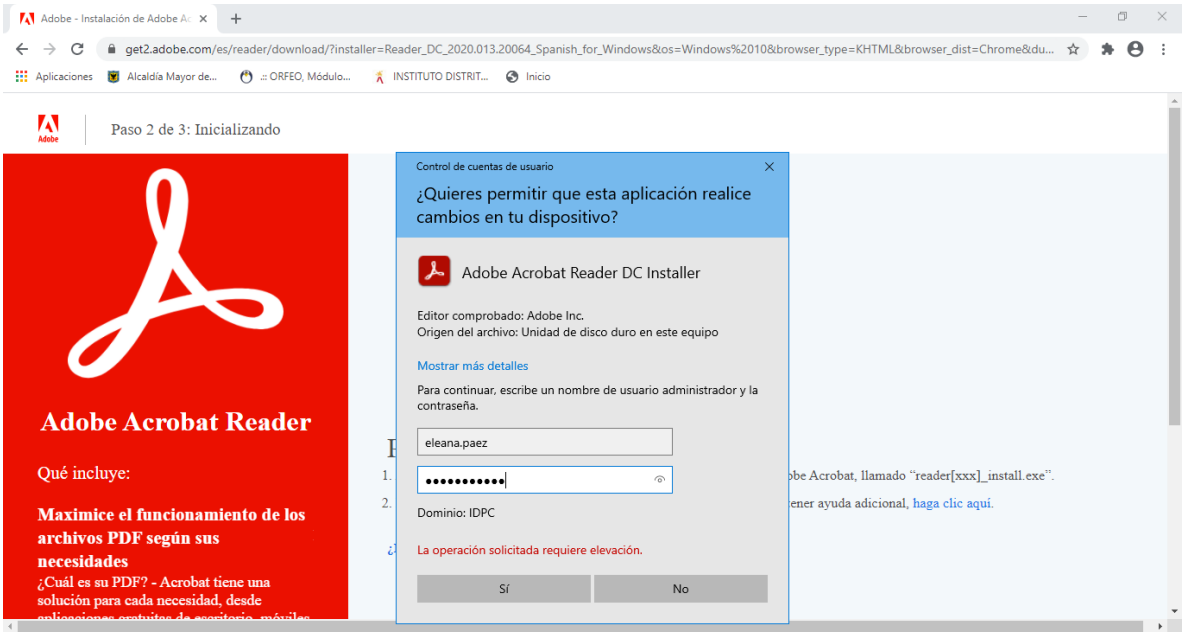
En el mismo sentido, el Plan de Seguridad y Privacidad de la Información IDPC, contempló en el Uso y protección de equipo de cómputo, lo siguiente "*En los equipos de cómputo del Instituto de Patrimonio Cultural, **tanto de arriendo como propios**, se restringe la instalación de software o programas, sistemas de información, herramientas de software que no sean licenciados y autorizados. Por esta razón se solicita clave de administrador para realizar estas acciones, dicha clave es únicamente conocida por el equipo de Sistemas*." (Subraya y negrita fuera de texto original)

De la anterior clausula y política, se desprende, que estos equipos, así sean en alquiler deben respetar las normas que sobre derecho de autor le corresponden, por tanto, al autorizar la instalación de copias de software que por Ley requieren licencia, así sea en equipos de alquiler, viola la Decisión Andina 351 de 1993, la cual determina que "*todo acto de explotación de la obra, diferente a la copia en la memoria del computador, a la copia de seguridad (acebo) o a la adaptación para exclusiva utilización, se entenderá como violación a las normas de Derecho de Autor si no cuenta con la previa y expresa autorización del autor o titular legítimo de tales derechos*."[2]

Se recomienda entonces, dar igual tratamiento a los equipos de alquiler que a los propios, en especial para evitar transgredir las normas que sobre derechos de autor corresponde acatar.

[2] Circular 05 del 9 de octubre de 2001-Dirección Nacional de Derechos de Autor.

En relación con la restricción de instalación de software, se realizó prueba con el portátil fuera del dominio, evidenciando que efectivamente se requiere clave de administrador para la instalación de software.



1.4.1.2.2.2 Uso de Recursos Tecnológicos

Teniendo en cuenta que esta política establece "*El proceso de gestión de sistemas de información definirá la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas*", se evidencia el listado de software mencionado en el punto anterior, de igual manera, en reunión virtual con la encargada de Sistemas, se indagó cómo se garantiza que todo el software usado en la plataforma tecnológica del IDPC debe tener su respectiva licencia y acorde con los derechos de autor, a lo cual se respondió "*Se hacen contratos anualmente comprando licencias y se entregan a la entidad, desde el año pasado reposan carpetas con licencias, de años anteriores se validó con el encargado del almacén y se hace una entrada al almacén y son instaladas en los equipos, indica que hay algunas que son gratuitas y cuando se piden se valida que el software realmente sea gratuito. Ya cuando se requiere otras licencias se adquieren y se hace un proceso de contratación que toca pagarlas*"

De igual manera, se preguntó por los esquemas de seguridad para realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del IDPC, respondiendo "*Para la conexión de servidores se utiliza un VPN, pero solo hay como 4 o 5 instaladas y son administradas por el firewall de la entidad, además se hizo un manual de instalación para configurar la conexión remota de escritorios a equipos google remote, el cual permite conectar a las máquinas siempre y cuando se sincronice con el correo electrónico y los computadores tienen que estar prendidos, algunas veces los computadores se apagan por bajas en la luz, y en horas no laborales, por tanto se solicitó de manera muy comedida a quienes prestan la vigilancia que en caso de que se apaguen los computadores, ellos los prendan para que*

funcione el remoto, se indica además que ese remoto también tiene usuario y contraseña para su acceso.

Se pregunta que estos VPN desde cuándo se manejan, la Ingeniera indica que este año, pero que tiene entendido que en años anteriores también tenían VPN para poderse conectar, sin embargo y dada la virtualidad, este año se ha utilizado con mayor frecuencia"

Teniendo en cuenta lo anterior, se evidencia que se da cumplimiento parcial a la política, por cuanto, como se mencionó en el numeral anterior, el software utilizado no se encuentra completamente licenciado.

1.4.1.2.2.3 Carpetas de Red, Discos de Red, Carpetas Virtuales

Para esta revisión se consultó en reunión virtual con la encargada de Sistemas, por la gestión de estas carpetas de red, a lo cual se respondió "*Carpetas de red como tal hay muy poquitas, que ella recuerde, están las del escáner, planeación tiene una carpeta en un servidor, a las que se les hace acebo diaria, por tanto, está respaldada la información, no hay muchas unidades de red. Se ha pensado en implementar un file server para que todo quede en un solo servidor y para uso de cada subdirección, actualmente no está así*". Lo anterior evidencia que se ha venido cumpliendo lo establecido y generando mejora continua.

1.4.1.2.2.4 Respaldo y restauración de la información

En cuanto al respaldo de información, se cuenta con Inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas del IDPC la auditada adjunta:

- Archivo en Excel denominado "Inventario Backup", en el cual muestra la relación de acebo 2019, describiendo el nombre del contratista, número de contrato y la ubicación de la información objeto de respaldo, para 181 contratista, se pega pantallazo para evidenciar que contiene cada archivo, así:

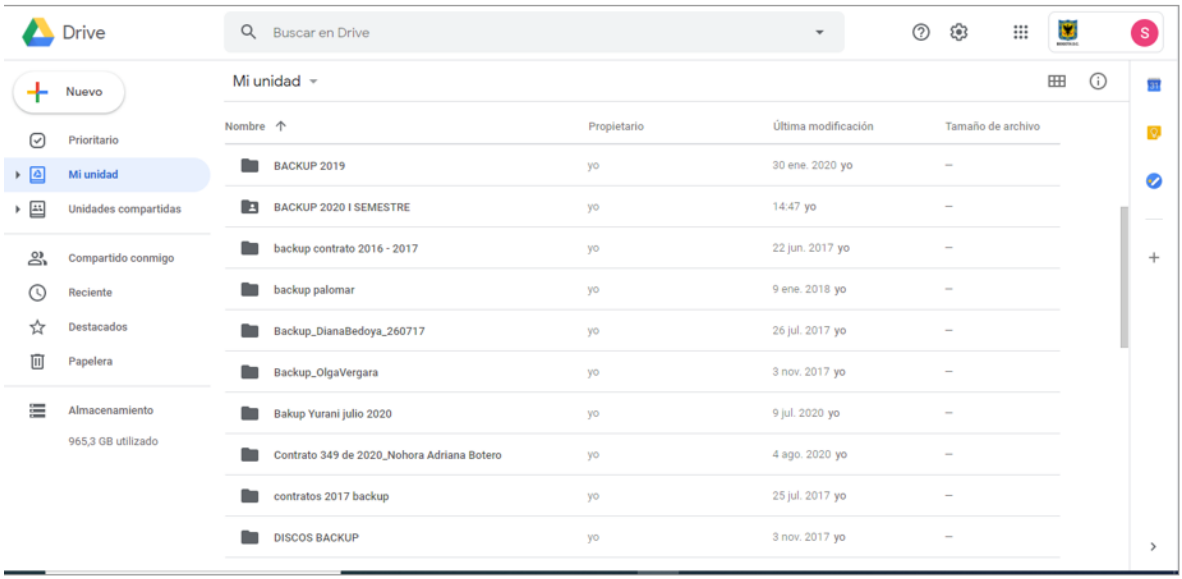
En el mismo archivo, pero en otra hoja de cálculo denominada "Phenix" se evidencia, ubicación nombres y años, con 44 registros:

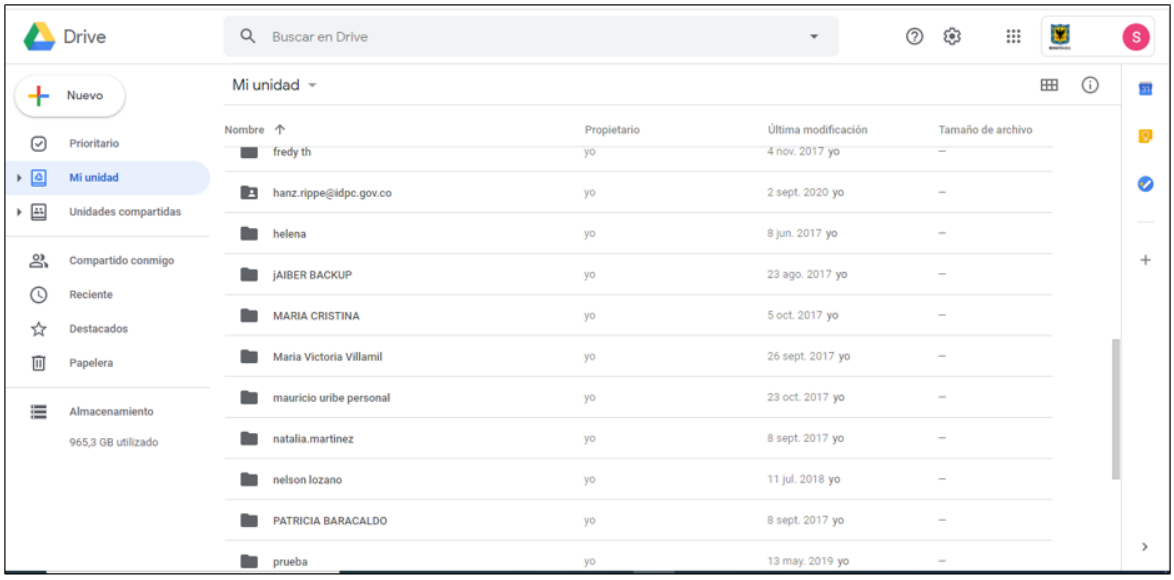
SERVIDOR PHENIX		
UBICACIÓN	NOMBRE	AÑOS
Disco Local D	Diana Bedoya	2017
Disco Local D	Olga Vergara	2017
Disco Local D	Maria Cristina Fonseca	2017
Disco Local D	Patricia Baracaldo	2017
Disco Local E	Monica Clavijo Roa	2017
Disco Local E	Ruth Corredor	2017
Disco Local E	Erika Quintana	2017
Disco Local E	Hernan Herrera	2017
Disco Local E	Juan Ortiz	2017
Disco Local E	Luz Mery Ponguta	2017
Disco Local E	Juan Fernando Acosta	2017
Disco Local E	Otto Alejandro Burbano	2017
Disco Local E	Gustavo Caicedo	2017
Disco Local E	Magda Puentes	2017
Disco Local E	Adriana Gonzalez	2017
Disco Local E	Ana Maria Carvajal	2017

- Archivo en Excel denominado “Inventario Aplicativos”, en el cual están relacionados los nombres de los sistemas de información, responsable, descripción del sistema, tipo, proveedor, estado, licenciamiento y fecha de vencimiento de la licencia, el cual contiene 15 registros:

INFORMACIÓN GENERAL							
NOMBRE DEL SISTEMA DE INFORMACIÓN	**RESPONSABLE**	**DESCRIPCIÓN DEL SISTEMA**	**TIPO**	**PROVEEDOR**	**ESTADO**	**LICENCIAMIENTO**	**FECHA VENCIMIENTO DE LA LICENCIA**
INTRANET	Grupo de gestion de sistemas	Plataforma informativa con accesos directos a paginas institucionales	Cliente – Servidor	Grupo de gestion de sistemas.	**desarrollo**	Licenciamiento ilimitado,.	indefinida.
PAGINA WEB	Web Master Subdireccion de Divulgacion	Breve descripción del objetivo del sistema y los servicios que presta el mismo. **Ejemplo:** Sistema de Gestión Documental que garantiza la trazabilidad y calidad de la documentación de la Entidad, el cual permite realizar radicación masiva, radicación vía mail, busquedas de documentos, etc.	Tipo de arquitectura que tiene el sistema de información:	Nombre del empleado, contratista o empresa contratista que da soporte al sistema.	Estado del sistema de información: **desarrollo, pruebas o producción.**	Licenciamiento ilimitado, licenciamiento para un procesador, cantidad de licencias por usuaro nombrado, cantidad de licencias por usuarios concurrentes, etc.	Fecha hasta la cual se tiene el contrato de mantenimiento o soporte del sistema con el proveedor.
ORFEO	Idelber Sanchez	Sistema de Gfestion Documental	Web Server con base de datos central	Idelber Sanchez	Producción	Licenciamiento Libre GPL. Ilimitado.	Ilimitada
PROACTIVANET	Grupo de gestion de sistemas	Software de Mesa de ayuda	Web	TCM Tecnologias	Producción	Licenciamiento limitado	Noviembre de 2020

- Archivo en Word denominado “Backup en drive de sistemas”, el cual contiene dos (2) pantallazos:





En reunión virtual sostenida con la Ingeniera Mary Rojas, sobre el particular, aclaró:

"(…) También se cuenta con discos externos para hacer acebo a equipos de servidores que se van y cuando la información así lo requiere, este año ya no se utilizaron, sino que se abrió una carpeta en el drive y ahí cada usuario deja su acebo. Para los que tienen mucha información en ese momento se presta un disco externo.

Se le pregunta que cómo se verifica que los usuarios si agreguen en el drive toda la información, a lo que contesta que un tema de confianza con las personas porque no puede estar detrás de todo el mundo y la información que se produce es de la entidad y para la entidad.

En lo que respecta a la confidencialidad de la información por temas sensibles, la ingeniera indica que a esa información solamente pude ingresar el grupo de sistemas, ya que esta fue creada con la cuenta de esta área, esto con el fin de garantizar su continuidad. Cuando se crea la carpeta se va sacando de los permisos y ya no queda nadie más a diferencia de sistemas."[3]

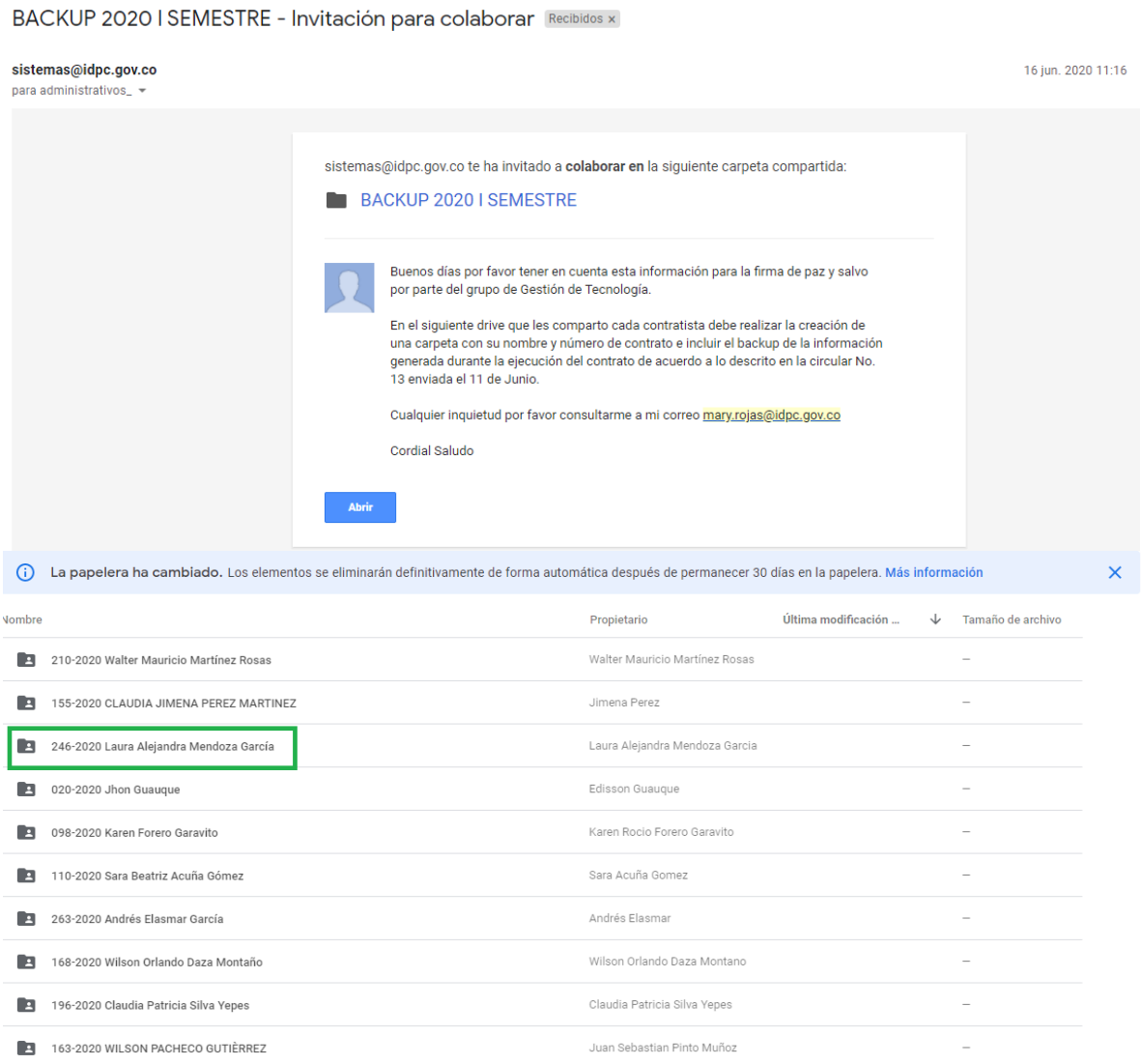
Sobre el particular, es necesario aclarar que en lo que respecta a las copias de seguridad que reposan en el drive, pese manifestar que por temas de confidencialidad de la información solo tiene acceso el grupo de sistemas, esta auditoría realizó una prueba, encontrando que se puede acceder desde cualquier perfil a estas copias de seguridad, lo que sin duda genera inseguridad en la información, además hay que tener en cuenta que algunos contratistas manejan temas sensibles, es el caso de la Oficina Asesora Jurídica, en cabeza de la Contratista que lleva los procesos y demandas en contra de la entidad, a cuya carpeta se pudo ingresar sin ningún tipo de restricción, evidenciándose entonces la falta de controles de seguridad y la ruptura de confidencialidad argumentada.

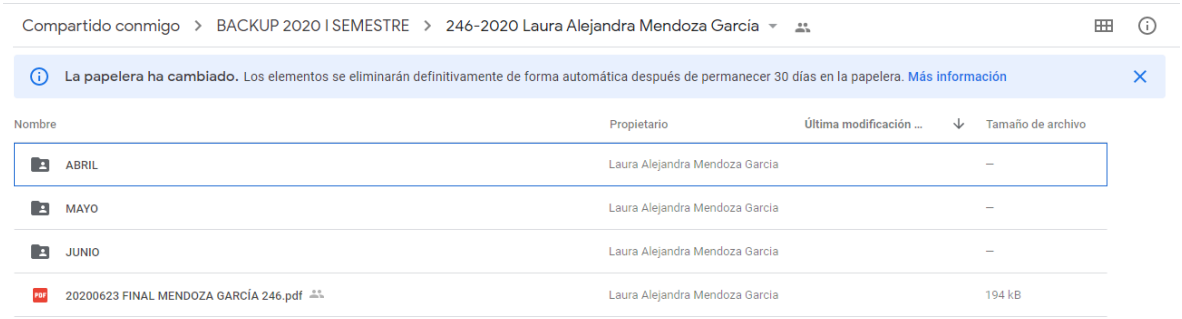
Igualmente, el Plan de Seguridad y Privacidad de la Información IDPC, contempla que, *"Los Activos de información de los procesos del IDPC deberán ser identificados y administrados dentro*

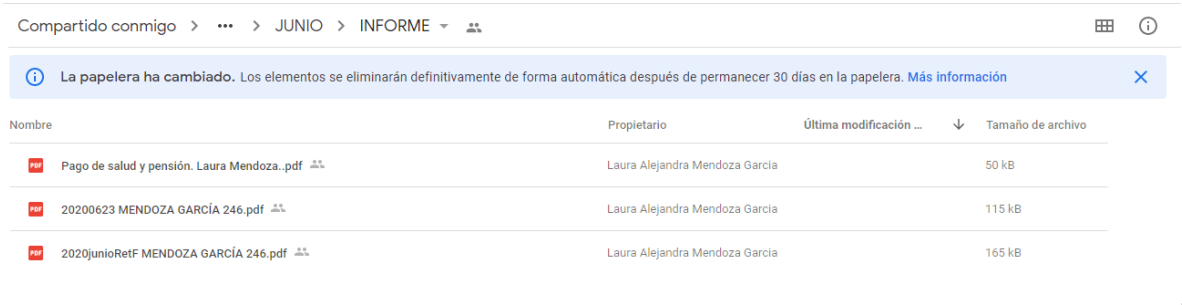
[3] Acta del 4 de noviembre de 2020

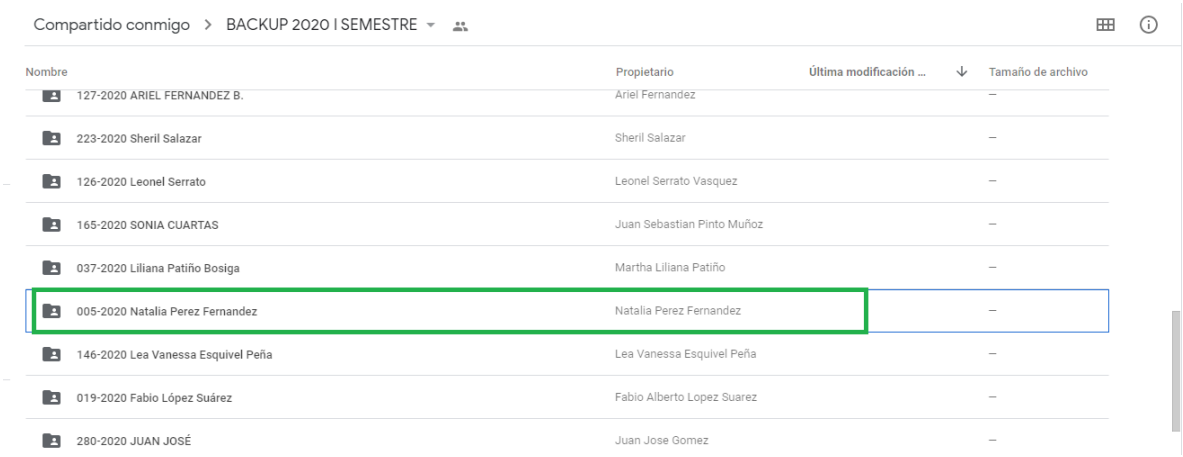
de un inventario, al igual que valorados con respecto a su sensibilidad o criticidad frente a impactos de afectación sobre la confidencialidad, integridad y disponibilidad de estos."

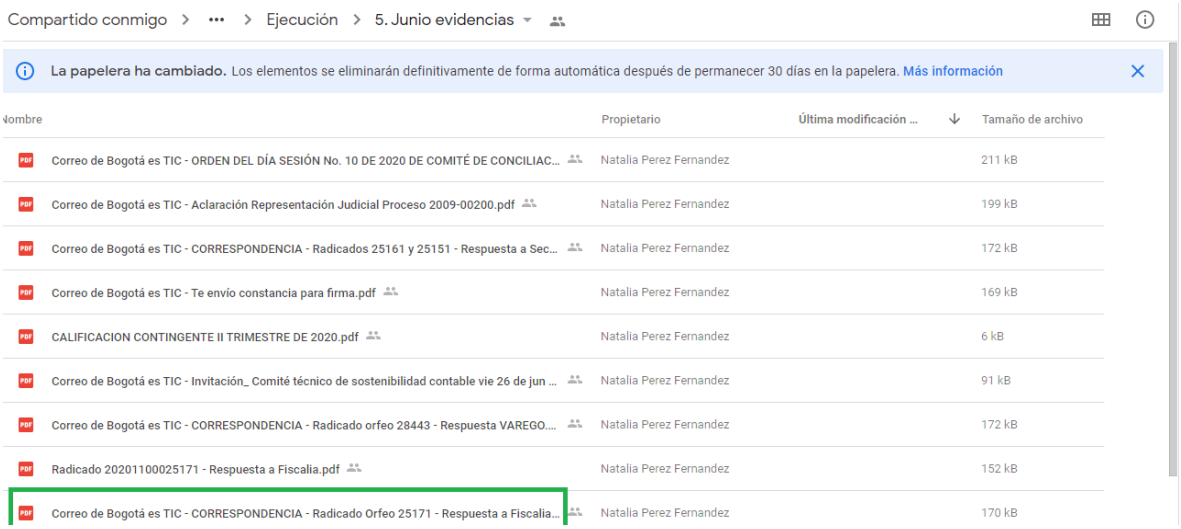
Se aportan pantallazos del 6 de noviembre en los que se puede evidenciar el acceso que se tuvo a la información generada por los contratistas en el desarrollo de sus contratos e incluida en la carpeta denominada "Backup".



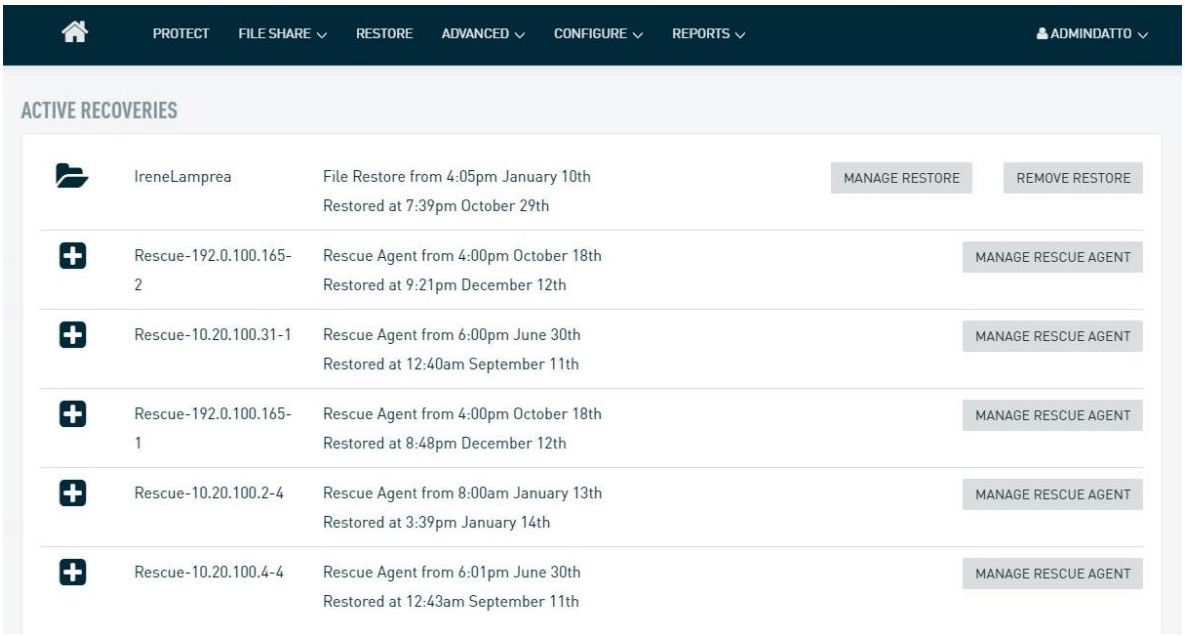

Compartido conmigo > BACKUP 2020 I SEMESTRE > 246-2020 Laura Alejandra Mendoza García
La papelera ha cambiado. Los elementos se eliminarán definitivamente de forma automática después de permanecer 30 días en la papelera. Más información
Nombre
Propietario
Última modificación ...
Tamaño de archivo
ABRIL
Laura Alejandra Mendoza Garcia
–
MAYO
Laura Alejandra Mendoza Garcia
–
JUNIO
Laura Alejandra Mendoza Garcia
–
20200623 FINAL MENDOZA GARCÍA 246.pdf
Laura Alejandra Mendoza Garcia
194 kB


Compartido conmigo > ••• > JUNIO > INFORME
La papelera ha cambiado. Los elementos se eliminarán definitivamente de forma automática después de permanecer 30 días en la papelera. Más información
Nombre
Propietario
Última modificación ...
Tamaño de archivo
Pago de salud y pensión. Laura Mendoza..pdf
Laura Alejandra Mendoza Garcia
50 kB
20200623 MENDOZA GARCÍA 246.pdf
Laura Alejandra Mendoza Garcia
115 kB
2020junioRetF MENDOZA GARCÍA 246.pdf
Laura Alejandra Mendoza Garcia
165 kB


Compartido conmigo > BACKUP 2020 I SEMESTRE
Nombre
Propietario
Última modificación ...
Tamaño de archivo
127-2020 ARIEL FERNANDEZ B.
Ariel Fernandez
223-2020 Sheril Salazar
Sheril Salazar
126-2020 Leonel Serrato
Leonel Serrato Vasquez
165-2020 SONIA CUARTAS
Juan Sebastian Pinto Muñoz
037-2020 Liliana Patiño Bosiga
Martha Liliana Patiño
005-2020 Natalia Perez Fernandez
Natalia Perez Fernandez
146-2020 Lea Vanessa Esquivel Peña
Lea Vanessa Esquivel Peña
019-2020 Fabio López Suárez
Fabio Alberto Lopez Suarez
280-2020 JUAN JOSÉ
Juan Jose Gomez



En cuanto a las pruebas realizadas a los Backup, el auditado adjunta pantallazo, en el cual se observa la restauración de archivos y el rescate de información de enero a octubre (no se evidencia año) como tampoco es explícito a qué información se refiere, ni si se puede realizar a toda la información de la entidad, y lo más importante si esta recuperación fue efectiva, es decir, si no se perdieron archivos.



En la reunión virtual ya mencionada, se le indagó sobre la frecuencia de respaldo de la información e indicar qué medios que se utilizan, a lo que respondió "*Se tiene solución de almacenamiento llamado "DATO" cuya frecuencia está en los pantallazos que nos adjuntó; de los servidores se hizo*

una prueba, para el día 4 de noviembre, encontrando que este se hace cada hora, inicia a las 8 am hasta las 6 pm y vuelve e inicia a las 8am, después de las 6 de la tarde no queda acebo, cada copia genera información full en caso de que suceda algo y el peso de la información es grande por eso la parametrización de horario.

En cada servidor hay lo siguiente:

- *Directorio activo de la entidad*
- *Intranet*
- *Trámites virtuales*
- *Backup de años anteriores*
- *Construplan (intervención)*
- *SIIGO (ya está en la nube)*
- *ORFEO gestión documental*
- *Consola del antivirus"*

Sin embargo, con el pantallazo que adjunta, no es posible inferir lo argumentado por la Ingeniera.

1.4.1.2.2.5 Control de Acceso

Para la conexión remota se utiliza VPN como se mencionó anteriormente dando cumplimiento a lo establecido en esta política.

1.4.1.2.2.6 Manejo de Contraseñas para Administradores de Tecnología

Frente a este punto, se indagó por las contraseñas de administrador y cómo es su manejo, para lo cual se respondió: "*Esta clave solo es manejada por el grupo de sistemas, y no ha sido compartida con nadie más. El oficial de seguridad obtuvo algunas, pero precisamente para hacer pruebas en temas de seguridad*", dando cumplimiento a lo establecido.

1.4.1.2.2.7 Transferencia de Información

Se evidencia que los contratos cuentan con cláusula, en la cual se establecen los Acuerdos de Confidencialidad y/o de Intercambio de Información entre el instituto y proveedores, de acuerdo a lo informado, esta cláusula se encuentra en revisión por parte del oficial de seguridad para verificar que esté adecuada.

1.4.1.2.2.8 Seguridad para las Relaciones con Proveedores

De acuerdo con lo explicado en el punto anterior se cumple con el requisito y se está verificando su adecuación.

1.4.1.2.2.9 Uso de Internet

Frente a este punto se preguntó por los controles existentes, respondiendo:

"*Se administra o limita con el firewall, se le da permiso a los usuarios de internet con restricciones, nada de redes sociales como youtube o acebook, es decir, aquello que genera interferencia en los canales. Hay algunos grupos control de acceso total, que necesitan más acceso a todos esos canales de comunicación, como el área de comunicaciones y algunos subdirectores o jefes de oficinas.*

Esto se realiza enviando un correo, ejemplo, el Señor Miguel Villamizar solicitó permiso para 3 personas, por cuanto las obligaciones del contrato, requerían acceder a algunas páginas restringidas, con ese correo, se verifica la IP de la máquina y se agrega y pueden navegar en esas páginas.

Las páginas pornográficas, se encuentran bloqueadas desde el principio y nadie tiene acceso.

¿Qué otras páginas tienen restricción total?, vimeo y pinterest, son páginas que se utilizan para comunicación y diseño gráfico y en algún momento se desbloquean a ciertas personas que lo requieren para trabajar, se desbloquean para la IP exclusivamente que lo solicite.

¿Se ha detectado que hay personas que quieran ingresar a páginas restringidas?, algunos usuarios tratan ingresar al acebook o a netflix, pero dado que el consumo a esas páginas es muy alto, y genera interferencias e intermitencias, esas páginas están bloqueadas, aunque no se puede detectar quién".

De lo anterior se puede deducir que existen controles que garantizan que la navegación en Internet se realice de forma razonable y con propósitos laborales.

1.4.1.2.2.10 Uso de Correo Electrónico

En cuanto a la gestión de cuentas de correo electrónico se informó que "*se estableció su manejo a través de la mesa de ayuda, pero teniendo en cuenta que las personas desde casa no pueden acceder, actualmente las novedades se manejan a través del correo electrónico.*

Se manejan cuentas básicas que tienen un límite y las bussines que son ilimitadas, pero no se les dan a todos los usuarios ya que son muy costosas".

De manera general y como usuario de correo electrónico, la Asesoría de Control Interno pudo verificar el cumplimiento de esta política.

1.4.1.2.2.11 Tercerización u Outsourcing

Para evaluar este punto, se solicitó el monitoreo de los riesgos relacionados con los contratistas o proveedores en relación a los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación, el cual fue evaluado en el numeral 1.2.3.

1.4.1.2.3 Procedimientos de Seguridad de la Información

La Guía No. 3 de MinTIC, establece como recomendaciones de procedimientos para el Modelo de Seguridad y privacidad de la Información en las Entidades del Estado:

PROCEDIMIENTOS SUGERIDOS	ESTADO IDPC
Procedimiento de Capacitación y Sensibilización del Personal	En el proceso Gestión del Talento Humano, se cuenta con PIC y procedimiento de monitoreo al mismo, se recomienda incluir en este Plan las actividades de Capacitación y Sensibilización del proceso Gestión de Sistemas.
Procedimiento de Ingreso y Desvinculación del Personal	En el proceso Gestión del Talento Humano, se cuenta con procedimientos para la Vinculación y Desvinculación.
Procedimiento de Identificación y Clasificación de Activos	Se cuenta con los procedimientos asociados al proceso Gestión Documental, no obstante, en estos no se especifica la manera en que los activos de información son identificados e inventariados por la entidad, así como también se debe especificar como son clasificados de acuerdo a su nivel de confidencialidad o criticidad, como se asignan y se devuelven los activos una vez se termina la relación laboral con la entidad.
Procedimiento para Ingreso Seguro a los Sistemas de Información	No se cuenta con un procedimiento, sin embargo en el Manual de Seguridad se encuentran algunas políticas en este sentido, por lo tanto, es importante revisar qué puntos adicionales pueden ser incluidos en estas.
Procedimiento de Gestión de Usuarios y Contraseñas	No se cuenta con un procedimiento, sin embargo en el Manual de Seguridad se encuentran algunas políticas en este sentido, por lo tanto, es importante revisar qué puntos adicionales pueden ser incluidos en estas.
Procedimiento de Controles Criptográficos	No se cuenta con este procedimiento
Procedimiento de Gestión de Llaves Criptográficas	No se cuenta con este procedimiento
Procedimiento de Control de Acceso Físico	No se cuenta con un procedimiento, sin embargo en el Manual de Seguridad se encuentran algunas políticas en este sentido, por lo tanto, es importante revisar qué puntos adicionales pueden ser incluidos en estas.
Procedimiento de Protección de Activos	Se cuenta con los procedimientos asociados al proceso Administración de Bienes e Infraestructura, sin embargo, en estos no se indica cómo se determina la ubicación de los equipos que procesan información confidencial, cómo se aseguran dichas instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños, por polvo, agua, interferencias, descargas eléctricas etc.
Procedimiento de Retiro de Activos	Se cuenta con los procedimientos asociados al proceso Administración de Bienes e Infraestructura, sin embargo, en estos no se indica el flujo de las solicitudes, autorizaciones y el control que tendrá el activo fuera de la entidad, así como también los controles de seguridad que deberá incluir el equipo cuando esté por fuera (controles criptográficos, cifrado de discos etc.)
Procedimiento de Mantenimiento de Equipos	Se cuenta con los procedimientos asociados al proceso Administración de Bienes e Infraestructura, sin embargo, en estos no se especifica cómo se ejecutan mantenimientos preventivos o correctivos dentro de la entidad, indicando los

PROCEDIMIENTOS SUGERIDOS	ESTADO IDPC
	intervalos en que estos deberán realizarse, con base a las sugerencias de los proveedores o si existen seguros atados a los equipos y los mantenimientos sean requisitos. Ni el modo en que los mantenimientos se llevarán a cabo y el personal que deberá ejecutarlo, llevando el registro apropiado.
Procedimiento de Gestión de Cambios	No se cuenta con este procedimiento
Procedimiento de Gestión de Capacidad	No se cuenta con este procedimiento
Procedimiento de Separación de Ambientes	No se cuenta con este procedimiento
Procedimiento de Protección contra Códigos Maliciosos	No se cuenta con estos procedimientos, sin embargo en el Manual de Seguridad se encuentran algunas políticas en este sentido, por lo tanto, es importante revisar qué puntos adicionales pueden ser incluidos en estas.
Procedimiento de Aseguramiento de Servicios en la Red	
Procedimiento de Transferencia de Información	
Procedimiento para el Tratamiento de la Seguridad en los Acuerdos con los Proveedores	
Procedimiento Adquisición, Desarrollo y Mantenimiento de Software	
Procedimiento de Control Software	
Procedimiento de Gestión de Incidentes de Seguridad de la Información	
Procedimiento de Gestión de la Continuidad de Negocio	No se cuenta con este procedimiento

1.4.1.2.4 Roles y Responsabilidades de Seguridad y Privacidad de la Información

Dentro de la Resolución 237 de 2020, correspondiente al funcionamiento del Comité Institucional de Gestión y Desempeño, se encuentran definidos los responsables de cada política del MIPG, incluyendo la de Seguridad Digital. De igual manera, en el Manual de Seguridad de la Información, se encuentran identificados los responsables. No obstante lo anterior, no se cumple con todo lo establecido en la Guía No. 4 Roles y responsabilidades de seguridad y privacidad de la información, dado que no se establecen funciones específicas.

1.4.1.2.5 Inventario de activos de información

La Entidad cuenta con Activos de Información definidos para cada dependencia, los cuales de manera general cumplen con lo establecido en la Guía No. 5 Gestión De Activos.

1.4.1.2.6 Integración del MSPI con el Sistema de Gestión documental

Si bien la Entidad cuenta con un proceso de Gestión Documental con sus respectivos procedimientos, lineamientos e instructivos, los mismos no se encuentran alineados con el Modelo de Seguridad y Privacidad de la Información.

1.4.1.2.7 Identificación, Valoración y Tratamiento de Riesgos

EL IDPC cuenta con el Manual de Administración de Riesgos, en el cual se encuentran definidos los lineamientos para la identificación, valoración y tratamiento de riesgos de gestión, corrupción y seguridad informática, de igual manera, se cuenta con Plan de Tratamiento de Riesgos de Seguridad de la Información, no obstante, se recomienda unificar los documentos.

1.4.1.2.8 Plan de Comunicaciones

Si bien se han venido desarrollando socializaciones del Manual de Seguridad, así como envíos de tips de seguridad, no se cuenta con un plan de comunicaciones que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad.

1.4.1.2.9 Plan de transición de Ipv4 a Ipv6

No se cuenta con un plan de transición estructurado que cumpla con los requisitos de la Guía No 20 Transición de Ipv4 a Ipv6 para Colombia.

1.4.1.3 Fase de Implementación

Dentro de esta fase se contemplan como resultados:

- Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
- Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.
- Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.
- Documento con las estrategias del plan de implementación de Ipv6 en la entidad, aprobado por la Oficina de TI.

No se cuenta con estos resultados, adicionalmente, las debilidades mencionadas anteriormente en las fases de diagnóstico y planificación del Modelo de Seguridad, impiden una adecuada implementación por lo cual no se revisará a fondo esta fase, únicamente se recomienda adecuar estas fases con el fin de generar un modelo ajustado a las necesidades del IDPC.

1.4.1.4 Fase de Evaluación de Desempeño

Dentro de esta fase se contemplan como resultados:

- Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.
- Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.

Pese a que se realizan monitoreos y seguimientos a los instrumentos aprobados en el IDPC, estos no se escalan a la Alta Dirección para la toma de decisiones frente al Modelo de Seguridad de la Información. De igual manera, no se cuenta con estos resultados, adicionalmente, las debilidades mencionadas anteriormente en las fases de diagnóstico y planificación del Modelo de Seguridad, impiden una adecuada implementación por lo cual no se revisará a fondo esta fase, únicamente se recomienda adecuar estas fases con el fin de generar un modelo ajustado a las necesidades del IDPC.

1.4.1.5 Fase de Mejora Continua

Teniendo en cuenta lo mencionado en las anteriores fases, es importante iniciar las acciones correctivas que se requieran.

1.4.2 Privacidad de la Información

Este componente del Modelo de Seguridad y Privacidad de la Información, cuenta con 3 temas que se deben tener en cuenta en las Entidades como son:

- Contar con una herramienta de análisis sobre impacto en la privacidad: En el IDPC no se pudo evidenciar la existencia de esta herramienta.
- Descripción de los flujos de información: La descripción de flujos de información se encuentra incluida en los procedimientos del IDPC, no obstante, es importante mencionar que esta no incluye qué información está siendo recolectada, con qué propósito, cómo, en qué cantidad y si la misma es objeto de divulgación.
- Identificar los riesgos de privacidad: Dentro de la matriz de riesgos, no se cuenta con riesgos relacionados con la privacidad de la información.

La implementación del componente de privacidad sigue el mismo ciclo de operación adoptado para seguridad de la información consistente en cinco fases o etapas así: diagnóstico, planeación, implementación, gestión y mejora continua.

1.4.2.1 Fase Diagnostico

Así como en el componente de Seguridad de la Información, en el de Privacidad, no se evidencia soporte de la ejecución de esta fase.

1.4.2.2 Fase Planificación

En esta fase el IDPC cuenta con Política de Tratamiento y Protección de Datos, no obstante, hace falta implementar otros documentos tales como:

- ✓ Documento con el plan de gestión de la privacidad sobre la información, aprobado por la alta dirección de la entidad.
- ✓ Definición de roles en relación con la Información.
- ✓ Procedimientos de privacidad.
- ✓ Plan de capacitación al interior de la entidad

1.4.2.3 Fase de Implementación

En cuanto a los resultados de esta fase se evidencia:

RESULTADOS	ESTADO IDPC
Documento con los riesgos contra la privacidad identificados y las medidas de solución adoptadas a partir de la implementación del plan de gestión de la privacidad de la información	Dentro de la matriz de riesgos, no se cuenta con riesgos relacionados con la privacidad de la información.
Documento que evidencie el registro de las Bases de datos	Se encuentran como bases de datos registradas en la SIC: • Bases de datos Talento Humano IDPC • Bases de datos Contratistas IDPC
Documento con el índice de información clasificada, reservada, revisada y sus procedimientos ajustados	La Entidad cuenta con Índice de Información Clasificada y Reservada, el cual está en proceso de actualización.

1.4.2.4 Fase de Evaluación del desempeño

Si bien se realizó seguimiento a la implementación de la política de Tratamiento y Protección de Datos Personales no se cuenta con ninguno de los documentos definidos como resultado de esta fase:

- Documento con los resultados del plan de seguimiento
- Documento con el Plan de auditoría interna y resultados revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces
- Comunicación de los indicadores al público a través de la rendición de cuentas, informe a la PGN y al Congreso de la República.

1.4.2.5 Fase de Mejora Continua

Teniendo en cuenta lo mencionado en las anteriores fases, es importante iniciar las acciones correctivas que se requieran.

1.4.3 Adopción del Protocolo Ipv6

Este componente tiene como fases para el proceso de transición del protocolo Ipv4 a Ipv6, Planeación, Implementación y Pruebas de funcionalidad.

1.4.3.1 Fase de Planeación

En esta fase, se debe definir el plan y la estrategia de transición de Ipv4 a Ipv6, en procura de los resultados que permitan dar cumplimiento con la adopción del nuevo protocolo.

- Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y software) de cada Entidad diagnosticada, Informe de la Infraestructura de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones , de cómputo y almacenamiento con el cumplimiento de Ipv6, plan de direccionamiento en Ipv6, plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con Ipv6, Informe de preparación (Readiness) de los sistemas de comunicaciones, bases de datos y aplicaciones.

  No se cuenta con plan de diagnóstico, sin embargo, se cuenta con Inventario de TI (Hardware y software) de cada Entidad diagnosticada, Informe de la Infraestructura de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento.

- Documento que define la estrategia de para la implementación y aseguramiento del protocolo Ipv6 en concordancia con la política de seguridad de las entidades.

  No se cuenta con este documento.

1.4.3.2 Fase de Implementación

Para esta fase no se cuenta con el Documento con el informe de la implementación del plan y la estrategia de transición de Ipv4 a Ipv6, revisado y aprobado por la alta Dirección.

1.4.3.3 Fase Pruebas de funcionalidad

Teniendo en cuenta que no se han desarrollado las dos fases anteriores, no se ha podido llevar a cabo la última fase.

1.5 ATENCIÓN REQUERIMIENTOS RECURSOS TECNOLÓGICOS

1.5.1 Solicitudes y su solución o cierre en la Mesa de Ayuda

Conforme al Procedimiento Atención de Requerimientos de Recursos Tecnológicos, se estableció la mesa de ayuda con el propósito de gestionar las incidencias y peticiones que ingresan por los canales y para los servicios que definiera el equipo de sistemas.

Así mismo, en sus políticas de operaciones se definió que todos los incidentes y peticiones de servicio debían ser registrados por los funcionarios y/o contratistas en el sistema de atención de mesa de ayuda, las cuales debían ser resueltas en un término no mayor a 24 horas conforme a los niveles de servicio definidos.

Teniendo en cuenta lo anterior, esta auditoría solicitó al grupo de sistemas, una relación de todas las solicitudes conforme al alcance de la auditoría y su solución o cierre a través de la mesa de ayuda.

Una vez revisados los documentos aportados por el auditado, se evidencia que aportan documento generado por "proactivanet" de julio de 2019 a marzo de 2020, que contiene incidencias y peticiones resueltas por la mesa de ayuda, indicando cuántas ingresaron según la categorización asignada, no obstante, con dicha información no es posible determinar quién realizó la solicitud, cómo y en qué término se solucionó, como tampoco es posible evidenciar si en efecto todas las peticiones y/o incidencias ingresadas fueron concluidas.

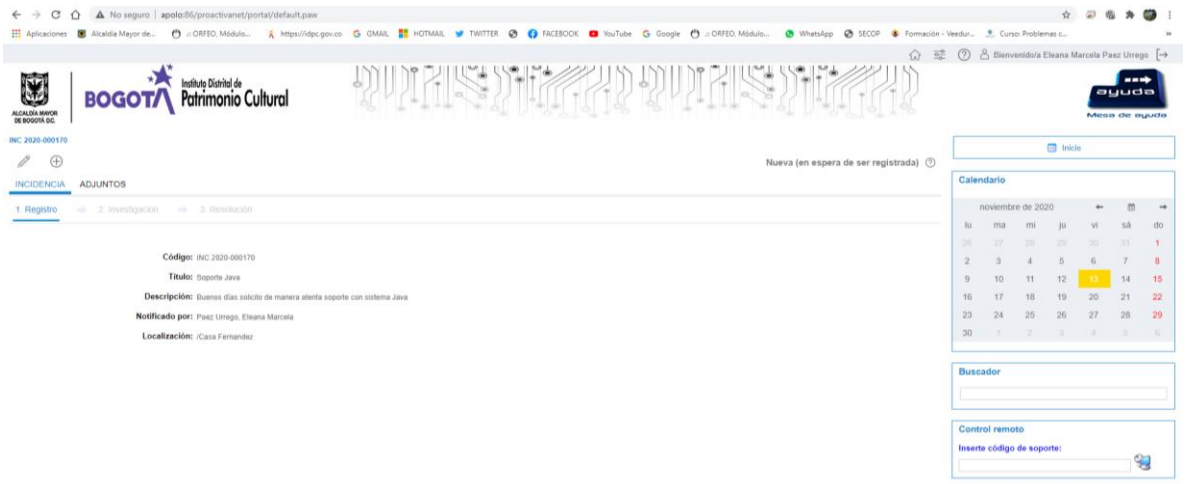
Para las incidencias y peticiones de abril a junio de 2020, adjuntan archivo en Excel, en el cual además se evidencia el nombre del solicitante, pero persiste la falta de información relacionada con la solución, el término y si fue cerrada satisfactoriamente o no.

A continuación, se relaciona lo evidenciado:

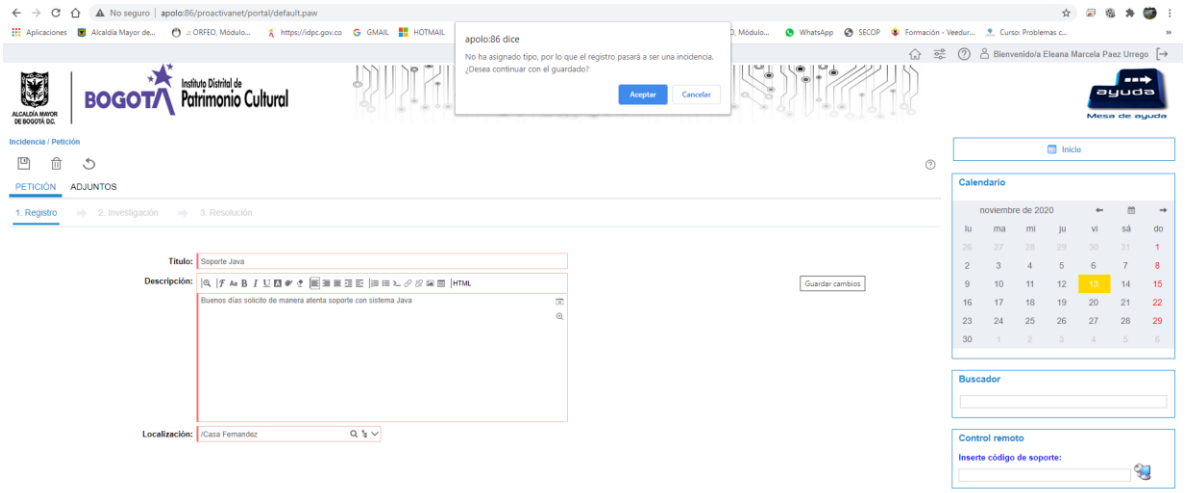
PERÍODO	***INCIDENCIAS Y PETICIONES RECIBIDAS***	***CATEGORIAS***
1/07/2019 a 31/12/2019	360	66
01/01/2020 a 31/03/2020	159	10
Abril 2020	116	SIN
Mayo 2020	86	SIN
Junio 2020	123	SIN

Dado lo anterior, no se cumplió con el requerimiento efectuado por la auditoría, motivo por el cual no fue posible establecer los criterios de solución, término y efectividad.

El procedimiento además establece que el sistema genera un número de caso, el cual será informado al solicitante por correo electrónico para su seguimiento, información que no está evidenciada en los reportes entregados, sin embargo, la Asesoría de Control Interno realizó pruebas para verificar, no obstante, si bien al finalizar la petición se hace entrega del número de caso, este no se informa por correo electrónico como lo manifiesta el procedimiento.



No fue posible observar que la clasificación de la incidencia y/o petición, coincidan con la solicitud, como tampoco su asignación conforme a los criterios de priorización. Se hace necesario además informar que no se observa un reporte en el cual se establezca un diagnóstico y/o análisis de reiteración de solicitudes por una misma causa y cuál es la solución de fondo brindada a dicha situación. Sin embargo, la Asesora de Control Interno realizó verificación evidenciando que a pesar de hacer una clasificación de petición, el Sistema lo toma automáticamente como una Incidencia.



En conclusión, con la información aportada por el auditado no fue posible evidenciar que se estén llevando a cabo todas las actividades planteadas en el procedimiento, sin embargo, al realizar las pruebas, se evidencia que estas no se están desarrollando plenamente.

1.5.2 Solicitudes de publicación y actualización de información en la Intranet, con los soportes de atención.

El auditado adjunta documento generado por “proactivanet” de julio de 2019 a marzo de 2020, que contiene incidencias y peticiones resueltas por la mesa de ayuda, en la que se observa cuántas ingresaron por concepto de publicaciones, no obstante, con dicha información no es posible determinar quién realizó la solicitud, cuál fue el o los documentos objeto de publicación y sí se atendió de manera oportuna.

Para el mes de abril 2020, adjunta archivo en Excel, en el cual además se evidencia el nombre del solicitante, pero persiste la falta de información relacionada con cuál fue la solicitud, el término y si fue publicada satisfactoriamente o no.

Según lo allí evidenciado, de julio a diciembre de 2019 se efectuaron 18 publicaciones, de enero a marzo de 2020 se llevaron a cabo 10 y en abril 2; no se evidencian para los meses de mayo a junio de 2020.

De acuerdo a la información aportada por el auditado no fue posible establecer los criterios de solución, término y efectividad.

1.5.3 Apertura, inactivación, eliminación, Backup y archivo de las cuentas de correo institucional

Para esta pregunta igualmente se adjunta el documento generado por "proactivanet" de julio de 2019 a marzo de 2020, el cual contiene las publicaciones efectuadas en ese periodo, esto es, setenta y siete (77) solicitudes relacionadas con soporte a correo electrónico y para los meses de abril a junio, según archivo en Excel, cincuenta y uno (51).

Igualmente, en reunión llevada a cabo con la Ingeniera Mary Rojas, encargada del área de Sistemas, nos indicó lo siguiente en lo que respecta a las cuentas de correo institucional, "s*e estableció su manejo a través de la mesa de ayuda, pero teniendo en cuenta que las personas desde casa no pueden acceder, actualmente las novedades se manejan a través del correo electrónico. Se manejan cuentas básicas que tienen un límite y las bussines que son ilimitadas, pero no se les dan a todos los usuarios ya que son muy costosas."*

Con la información suministrada no es posible determinar cuál fue la solicitud, qué solución requería, quién la realizó, a excepción de los meses de abril a junio que, si posee el nombre del solicitante, no fue posible entonces establecer los criterios de solución, término y efectividad.

1.5.4 Elaboración y divulgación de instrucciones de uso del correo institucional.

El Manual de Seguridad de la Información (versión 1 del 27/09/2019) en su numeral 6.13 contiene una serie de indicaciones relacionadas con la creación y uso del correo electrónico, cumpliendo con ello lo referente a la elaboración de instrucciones del uso del correo institucional.

No obstante lo anterior, no se evidencia o no se aporta documentación que dé cuenta de la divulgación a los usuarios sobre la existencia de estas instrucciones.

1.5.5 Apoyo en el cargue y depuración de datos en aplicativos externos, para la generación de los informes institucionales.

El auditado adjunta:

- Certificado de recepción de información de los documentos y formularios de la cuenta mensual de SIVICOF, para los meses de abril, mayo y junio de 2020
- Actas de "transmisión de información mensual SIVICOF" para los meses de junio a diciembre de 2019; marzo, abril, mayo y junio de 2020. Igualmente, la cuenta anual correspondiente al año 2019.

No se evidencian soportes relacionados con certificados para los meses de julio de 2019 a marzo de 2020, como tampoco actas para los meses de enero y febrero de 2020.

Es importante mencionar que esta actividad se encuentra dentro de las obligaciones contractuales número 5 y 6 de los Contratos de Prestación de Servicios y Apoyo a la Gestión números 131 de 2019 y 007 de 2020, respectivamente, cuyo contratista es Jaiber Alfonso Sarmiento Ruíz, del área de sistemas, al cual se le asignó, entre otras obligaciones, está la de "*Apoyar los procesos de trasmisión de datos e informes ante los entes de control que le sean asignados".*

Si bien no se aportó toda la información correspondiente a la cuenta SIVICOF, se hace necesario mencionar que, la Asesoría de Control Interno conforme a su programación anual, ha venido haciendo seguimiento al cargue mensual de la cuenta SIVICOF para la vigencia 2020, seguimientos en los cuales, entre otras cosas, evidenciaron lo siguiente:

- Para la cuenta correspondiente al mes de febrero de 2020, se evidenció el cargue extemporáneo de los documentos correspondientes a deuda pública, estos debían reportarse el 3 de marzo y se cargaron el 11 de marzo.

- El formulario CBN-1090 correspondiente a la cuenta anual, se subió a la plataforma SIVICOF el 16 de marzo de 2020, sin que se evidenciara en su momento autorización de la Contraloría para cargarlo nuevamente.

Situaciones que fueron puestas en conocimiento del Área Financiera, a través del respectivo informe, sin que se presentara pronunciamiento al respecto.

Conforme a la obligación descrita, el contratista de sistemas, apoya el proceso de transmisión, por tanto, debe conocer y tener un control de las fechas en la cuales se efectuará el cargue y cuáles son los requisitos para retransmitir un documento cuando ha sido objeto de modificación.

Adicionalmente en el acta del 7 de abril, aportada por el área, no se dijo nada con respecto a la extemporaneidad de la información de deuda pública, como tampoco sobre la retransmisión del formulario CBN-1090.

Así las cosas, se evidencia debilidad en el seguimiento y protocolos para el cargue de información en la Plataforma Sivicof, omitiendo dentro de las actas de seguimiento este tipo de novedades que afecta la transmisión de la cuenta.

1.5.6 Plan de Mantenimiento Preventivo y Correctivo

En cuanto al Plan de Mantenimiento preventivo y correctivo se hace entrega del cronograma de mantenimiento de equipos definido para la ejecución del contrato 348-2019, no obstante, no se hace entrega del plan que se estructura previamente y que es base para definir los estudios previos de contratación. De igual manera esta programación está firmada por el responsable de Almacén, sin contar con algún visto bueno desde el área de Sistemas, quienes son los expertos técnicos en la materia; adicionalmente, se contempla únicamente la vigencia 2019 y no se remite información concerniente al 2020.

En cuanto a la ejecución del cronograma de mantenimiento se evidencia:

ACTIVIDAD	SEGUIMIENTO
Inspección técnica	Se encuentra programado en el mes de mayo de 2019 y como soporte de ejecución se hace entrega de Informe diagnóstico realizado por la Empresa contratista con base en visita técnica.
Mantenimiento de Computadores	Se hace entrega de las hojas de vida de los equipos por cada una de las sedes así: Casa Cadel 3 equipos, Centro de Documentación 18 equipos, Casas Gemelas y Fernández 137 equipos, Casa 7 Balcones 20 equipos y Casa Sámano 4 equipos, para un total de 182 equipos con mantenimiento preventivo.

ACTIVIDAD	SEGUIMIENTO
Mantenimiento de Equipos de Impresión	Como soporte de la ejecución de esta actividad dentro del Plan de Mantenimiento se evidencia la hoja de vida de 11 impresoras.
Mantenimiento de Servidores	Para la ejecución de esta actividad, se evidencia hoja de vida de 6 servidores.
Mantenimiento de Equipos de Comunicación	No se evidenciaron soportes de la ejecución de esta actividad.
Mantenimiento de UPS	No se evidenciaron soportes de la ejecución de esta actividad.
Mantenimiento Correctivo	No se evidenciaron soportes de la ejecución de esta actividad.

De manera general, se concluye que no se cuenta con un Plan de Mantenimiento previo a la contratación, igualmente, en materia de la ejecución del cronograma entregado para la vigencia 2019, no se puede evidenciar el cumplimiento total de este.

2. DESCRIPCIÓN HALLAZGOS

2.1 FORTALEZAS – CONFORMIDADES - CUMPLIMIENTOS

No.	Descripción Fortaleza
1	Disposición del equipo de trabajo para la atención de la auditoría.
2	El proceso de Gestión de Sistemas de Información y Tecnología se ha venido fortaleciendo en cuanto a su documentación y talento humano, lo que ha permitido evidenciar una mejora continua.

2.2 OPORTUNIDADES DE MEJORA

No.	Descripción Oportunidad de Mejora
1	Teniendo en cuenta la transversalidad de los documentos que hacen parte del proceso Gestión de Sistemas de Información y Tecnología, es necesario, además de generar el documento y publicarlo en la intranet, se requiere su socialización a través de otros medios con el fin de garantizar su aplicación. **Respuesta y documentos aportados por el Auditado:** Se precisa que los documentos que hacen parte del proceso de Gestión de Sistemas de Información y Tecnología se publican en los medios de comunicación interna del Instituto como lo es la Intranet y el correo electrónico haciendo un envío masivo a la cuenta de correo administrativos@idpc.gov.co. Anexo evidencia de correos electrónicos enviados Por lo expuesto anteriormente, respetuosamente se solicita levantar la observación. ✓ Pantallazo Intranet “Tips de Seguridad Informática” ✓ Pantallazo Intranet “Tips de Seguridad para proteger tu correo electrónico corporativo” ✓ Pantallazo Intranet “Seguridad Informática” 4/12/2019 ✓ Pantallazo Intranet “Seguridad de los Dispositivos en el Trabajo” ✓ Pantallazo Intranet “Información de la telefonía IP” 4/12/2019 ✓ Pantallazo Intranet “Tips de Seguridad” ✓ Correo Electrónico del 24/08/2019 “Tips de Seguridad Informática” ✓ Pantallazo Intranet “Recomendaciones para realizar teletrabajo desde casa” ✓ Pantallazo Intranet “Tips de Seguridad Informática”

2.2 OPORTUNIDADES DE MEJORA	
No.	**Descripción Oportunidad de Mejora**
	✓ Correo Electrónico del 6/11/2019 "Plan Estratégico de la Información PETI" **Análisis de la respuesta y documentación:** Si bien se evidencian varias publicaciones, es necesario que se aborden todos los temas del Proceso y como se indica en la oportunidad de mejora, no solo a través de Intranet, máximo que en esta época con el trabajo en casa la mayoría no tiene acceso a la página. Nótese que solo se adjunta dos (2) correos electrónicos. Por tanto se recomienda continuar socializando a través de otros medios.
2	Se debe garantizar que la información corresponda a las solicitudes que se efectúen, además debe existir tabulación de datos que permita establecer que las solicitudes que ingresaron fueron atendidas satisfactoriamente y dentro del término. **Respuesta otorgada por el Auditado:** El tiempo definido dentro de la parametrización de la Mesa de Ayuda es de máximo 24 horas para su atención y/o solución, tiempo que se cumple sin novedad alguna, como se puede evidenciar, no se tiene ninguna queja o reclamo donde algún usuario informe el incumplimiento de algún incidente o petición registrado en la Mesa de ayuda. No obstante, lo anterior la entidad cambiará el software de mesa de ayuda con el fin de mejorar estos informes. Por lo expuesto anteriormente, respetuosamente se solicita levantar la observación. **Análisis de la Respuesta:** Teniendo en cuenta que esta oportunidad de mejora se dejó además como una No Conformidad, se retira.
3	Es necesario tener en cuenta las políticas propuestas por MinTIC, que si bien no son obligatorias, se tornan importantes para el desarrollo de los documentos del proceso en el IDPC. **Respuesta otorgada por el Auditado:** Es muy importante la observación, pero debido al cambio de administración, el instituto ya está trabajando en las nuevas políticas, las cuales ya están terminadas y nos encontramos en trámite de presentación ante el Comité de Gestión y Desempeño para aprobación final y publicación. Por lo expuesto anteriormente, respetuosamente se solicita levantar la observación. **Análisis de la Respuesta:** Es preciso señalar que esta Auditoría tuvo como alcance, del 1 de julio de 2019 a 30 de junio de 2020, y la nueva política a la que hace referencia es posterior a este periodo, por tanto, se mantiene la oportunidad de mejora.
4	Unificar los lineamientos del Manual de Administración de Riesgos y el Plan de Tratamiento de Riesgos de Seguridad de la Información. **Respuesta otorgada por el Auditado:** De acuerdo con los resultados del diagnóstico del modelo de seguridad y privacidad de la información - MSPI

2.2 OPORTUNIDADES DE MEJORA	
No.	**Descripción Oportunidad de Mejora**
	realizado en la entidad, el Instituto elaborará la metodología de riesgos de seguridad de la información el cual incluye su análisis, valoración y tratamiento de riesgos. De igual manera se elaborará el instrumento para registrar los riesgos por proceso. La identificación de los riesgos se realizará para la vigencia 2021 una vez identificados los activos de información críticos por proceso. **Análisis de la Respuesta:** Conforme a la respuesta otorgada, implícitamente se acepta la oportunidad de mejora, por tanto, esta se mantiene.
5	En relación con el acompañamiento realizado para el cargue y depuración de datos en aplicativos externos, se evidencian algunas debilidades, las cuales fueron incluidas dentro de los seguimientos realizados a la cuenta Mensual y Anual reportada en SIVICOF, por lo que es necesario tomar acciones que eviten la reincidencia de estas situaciones. **Respuesta otorgada por el Auditado:** Revisado el tema con el área financiera ya se encuentra un plan de mejoramiento sobre el cumplimiento de los reportes de SIVICOF, el cual fue elaborado conjuntamente entre las dos áreas. **Análisis de la Respuesta:** Conforme a la respuesta otorgada, implícitamente se acepta la oportunidad de mejora, por tanto, esta se mantiene.

2.3 OBSERVACIONES – CUMPLIMIENTOS PARCIALES	
No.	**Descripción Observación**
1	Los soportes entregados para la ejecución de la auditoría por parte del responsable del proceso Gestión de Sistemas de Información y Tecnología, en algunos casos no evidencian de manera completa el cumplimiento de las actividades, lineamientos o políticas, incluidas dentro de la documentación del proceso, como se pudo evidenciar en el contenido del informe. **Respuesta otorgada por el Auditado:** Actualmente se está adelantando la actualización de los documentos del proceso de Gestión de sistemas de Información y Tecnología., con el fin de dar cumplimiento a las actividades allí propuestas. **Análisis de la Respuesta:** Conforme a la respuesta otorgada, implícitamente se acepta la observación, por tanto, esta se mantiene.
2	La documentación del proceso Gestión de Sistemas de Información y Tecnología no se encuentra acorde con lo que se desarrolla. Ver numeral 1.1 **Respuesta otorgada por el Auditado:** Actualmente se está adelantando la actualización de los documentos del proceso de Gestión de sistemas de Información y Tecnología., con el fin de dar cumplimiento a las actividades que desarrolla.

2.3 OBSERVACIONES – CUMPLIMIENTOS PARCIALES	
No.	**Descripción Observación**
	Análisis de la Respuesta: Conforme a la respuesta otorgada, implícitamente se acepta la observación, por tanto, esta se mantiene.
3	En el PETI, se evidencian algunas debilidades, tales como: ▪ Algunas descripciones de las normas no corresponden, es el caso, de la Ley 1341 de 2009. ▪ Hay Leyes que han sido reglamentadas, sin embargo, no se hace mención a esa reglamentación o modificación o actualización. ▪ No se tuvo en cuenta el CONPES 3854 del 7 de marzo de 2017 y sus adendas. ▪ Los contratos aportados no están alineados con el Plan Estratégico de la entidad. **Respuesta otorgada por el Auditado:** El PETI revisado en esta auditoría corresponde al documento elaborado en 2016, el cual terminó su vigencia en junio de 2020. Por lo anterior el Instituto inició el proceso para desarrollar el nuevo plan que regirá para los años 2020 a 2024 teniendo en cuenta que la entidad durante el segundo semestre del 2020 ha trabajado en conjunto con el equipo designado para la construcción del plan y así mitigar las debilidades encontradas en el diagnóstico realizado en el Primer semestre del presente año. **Análisis de la Respuesta:** Conforme a la respuesta otorgada, implícitamente se acepta la observación, por tanto, esta se mantiene.
4	En cuanto al apoyo técnico para la adquisición de bienes o contratación de servicios que incluyan un componente tecnológico, se evidenció que no se dejaba documentado dicho acompañamiento, situación que fue incluida dentro del informe de seguimiento a la Austeridad en el Gasto Público y cuenta con plan de mejoramiento abierto, al cual se le seguirá realizando seguimiento. **Respuesta otorgada por el Auditado:** Se seguirán realizando las acciones pertinentes para dar cumplimiento al plan de mejoramiento vigente. **Análisis de la Respuesta:** Conforme a la respuesta otorgada, implícitamente se acepta la observación, por tanto, esta se mantiene.
5	En el Manual de Políticas de Seguridad no se incluye la Privacidad de la Información, como lo requiere el Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones. **Respuesta otorgada por el Auditado:** El instituto ya está trabajando en la actualización del manual de políticas de seguridad de la información con la que aplican al IDPC incluyendo la política de privacidad y protección de datos personales de acuerdo a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones. **Análisis de la Respuesta:** Conforme a la respuesta otorgada, implícitamente se acepta la observación, por tanto, esta se mantiene.

2.3 OBSERVACIONES – CUMPLIMIENTOS PARCIALES	
No.	**Descripción Observación**
6	Es importante complementar los procedimientos existentes con lo establecido en la Guía No. 3 de MinTIC Procedimientos de Seguridad de la Información y generar los que aún no se encuentran documentados. **Respuesta otorgada por el Auditado:** Para la vigencia 2021 se realizarán los procedimientos que aplican al IDPC de acuerdo al diagnóstico de seguridad y privacidad de la información. **Análisis de la Respuesta:** Teniendo en cuenta que esta oportunidad de mejora se dejó además como una No Conformidad, se retira.
7	Para la correcta implementación, evaluación y mejora del Modelo de Seguridad y Privacidad de la Información es necesario contar con un adecuado diagnóstico y planificación del mismo. **Respuesta y documentos aportados por el Auditado:** El Instituto al día de hoy ya terminó de elaborar el diagnóstico del Modelo de Seguridad y Privacidad de la Información, nos encontramos en fase de socialización. Anexo documento y presentación. Por lo expuesto anteriormente, respetuosamente se solicita levantar la observación. ✓ Instrumento de Identificación de la Línea Base de Seguridad – Hoja Portada del 31/10/2020 ✓ Presentación Power Point “MSPI- Modelo de Seguridad y Privacidad de la Información” nov/2020 **Análisis de la Documentación:** Teniendo en cuenta que esta oportunidad de mejora se dejó además como una No Conformidad, se retira.

2.4 NO CONFORMIDADES - INCUMPLIMIENTOS		
No.	**Requisito**	**Descripción No Conformidad**
1	Manual de Administración de Riesgos y Plan de Tratamiento de Riesgos de Seguridad de la Información	Es importante complementar los procedimientos existentes con lo establecido en la Guía No. 3 de MinTIC Procedimientos de Seguridad de la Información y generar los que aún no se encuentran documentados. **Respuesta otorgada por el Auditado:** Para la vigencia 2021 se realizarán los procedimientos que aplican al IDPC de acuerdo al diagnóstico de seguridad y privacidad de la información. **Análisis de la Respuesta:** Conforme a la respuesta otorgada, se acepta la No Conformidad, por tanto, esta se mantiene.

2.4 NO CONFORMIDADES - INCUMPLIMIENTOS		
No.	**Requisito**	**Descripción No Conformidad**
2	Manual de Administración de Riesgos y Manual de Seguridad y Privacidad de la Información numeral 6.1.4	No se evidencia documentación del monitoreo realizado a los riesgos relacionados con los contratistas o proveedores en relación a los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación. Ver numeral 1.2.3 **Respuesta otorgada por el Auditado:** Se acepta la observación, y se incluirá en el Modelo de Seguridad y privacidad de la Información los riesgos con los contratistas, proveedores y terceros que accedan a la información del IDPC. **Análisis de la Respuesta:** Conforme a la respuesta otorgada, se acepta la No Conformidad, por tanto, esta se mantiene.
3	Guía Construcción del PETI – Gobierno Digital V.2 Numerales 1 y 4 del artículo 2.2.35.3 del Decreto 1083 de 2015	El PETI no se construyó con base en la guía establecida por Gobierno Digital, tal y como se explica en el numeral 1.3.1 1 (…) "*que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado*." (…) 4. "*Liderar la gestión, seguimiento y control de la ejecución de recursos financieros asociados al portafolio de proyectos y servicios definidos en el plan estratégico de Tecnologías y Sistemas de información*." **Respuesta y documentos aportados por el Auditado:** El PETI revisado en esta auditoría corresponde al documento realizado en 2016, el cual terminó su vigencia en junio de 2020. Por lo anterior el Instituto inició el proceso para desarrollar el nuevo plan que regirá para los años 2020 a 2024 teniendo en cuenta que el Ingeniero Juan Carlos Cubillos Líder de Gobierno digital ha convocado durante el segundo semestre del presente año mesas de trabajo con el equipo designado por la entidad. El documento que se está terminando, basado en la "G.ES.06 Guía para la construcción del PETI" de Julio de 2019, con un objetivo claro, así como el alcance del documento, se encuentra en la fase final de construcción, teniendo en cuenta que el mismo quedará terminado en diciembre de 2020, para aprobación el comité Directivo. Anexo informe de Análisis y Evaluación de Madurez de Gobierno digital, Presentación Formulación PETI, Fase I, II Y III PETI, elaborado y presentado por el líder de gobierno digital, Ingeniero Juan Carlos Cubillos

2.4 NO CONFORMIDADES - INCUMPLIMIENTOS		
No.	**Requisito**	**Descripción No Conformidad**
		Por lo expuesto anteriormente, se solicita respetuosamente retirar la no conformidad, ya que la misma no podría dar lugar a acciones de mejora toda vez que el nuevo documento corrige las debilidades del anterior. ✓ Análisis y evaluación de madurez de gobierno digital para el IDPC del 18/06/2020 ✓ Archivo denominado "PETI Fase 1-Comprender" el cual contiene varias hojas de cálculo, en el cual está como responsable de la Política, el señor Juan Carlos Cubillos. Además, está la Ficha de la Entidad en cuyo documento aparece como representante legal es el Dr PATRICK MORALES. ✓ Formulación del PETI usando el habilitador de Arquitectura (sin fecha) ✓ Plan Estratégico de Tecnologías de la Información PETI 2020-2023, versión 1 del 29/10/2020 ✓ Política de Gobierno Digital del MINTIC **Análisis de la respuesta y documentación:** De la respuesta y evidencias aportadas, se confirma entonces que para el periodo auditado no se contaba con un PETI conforme a la guía. La creación del nuevo PETI, esto es, 2020-2023, sin duda refleja el esfuerzo para consolidar un Plan con todos los aspectos relevantes, no obstante, la evaluación que se realizó por parte de esta Auditoría estuvo enfocada al PETI versión 4 (2016-2020), del cual no se evidencia ningún documento adicional que permita establecer el cumplimiento de lo ya mencionado, por tanto, se mantiene la No Conformidad. En cuanto a lo indicado por el auditado "*se solicita respetuosamente retirar la no conformidad, ya que la misma no podría dar lugar a acciones de mejora toda vez que el nuevo documento corrige las debilidades del anterior*", es importante precisar que no se pueden realizar correcciones, no obstante, se pueden formular acciones correctivas que conlleven a la mejora del proceso.
4	Guía Construcción del PETI – Gobierno Digital V.2	El PETI definido no cuenta con el desarrollo de los proyectos allí descritos, estos no contienen metas, así como actividades a desarrollar, lo que dificulta establecer si los mismos fueron o no cumplidos. Ver numeral 1.3.1 y numeral 1.3.2 **Respuesta y documentos aportados por el Auditado:** El PETI revisado en esta auditoría corresponde al documento realizado en 2016, el cual terminó su vigencia en junio de 2020. Por lo anterior el Instituto inició el proceso para desarrollar el nuevo plan que regirá para los años 2020 a 2024 teniendo en cuenta que el Ingeniero Juan Carlos Cubillos Líder de Gobierno digital ha convocado durante el segundo semestre del presente año mesas de trabajo con el equipo designado por la entidad con el fin de incluir los proyectos con sus respectivas metas y fechas para su desarrollo.

2.4 NO CONFORMIDADES - INCUMPLIMIENTOS

No.	Requisito	Descripción No Conformidad
		Anexo informe de Análisis y Evaluación de Madurez de Gobierno digital, Presentación Formulación PETI, Fase I, II Y III PETI, elaborado y presentado por el líder de gobierno digital, Ingeniero Juan Carlos Cubillos. Por lo expuesto anteriormente, se solicita respetuosamente retirar la no conformidad, ya que la misma no podría dar lugar a acciones de mejora toda vez que el nuevo documento corrige las debilidades del anterior. ✓ Análisis y evaluación de madurez de gobierno digital para el IDPC del 18/06/2020 ✓ Archivo denominado "PETI Fase 1-Comprender" el cual contiene varias hojas de cálculo, en el cual está como responsable de la Política, el señor Juan Carlos Cubillos. Además, está la Ficha de la Entidad en cuyo documento aparece como representante legal es el Dr PATRICK MORALES. ✓ Formulación del PETI usando el habilitador de Arquitectura (sin fecha) ✓ Plan Estratégico de Tecnologías de la Información PETI 2020-2023, versión 1 del 29/10/2020 ✓ Política de Gobierno Digital del MINTIC **Análisis de la respuesta y documentación:** De la respuesta y evidencias aportadas, se confirma entonces que para el periodo auditado no se contaba con un PETI conforme a la guía. La creación del nuevo PETI, esto es, 2020-2023, sin duda refleja el esfuerzo para consolidar un Plan con todos los aspectos relevantes, no obstante, la evaluación que se realizó por parte de esta Auditoría estuvo enfocada al PETI versión 4 (2016-2020), del cual no se evidencia ningún documento adicional que permita establecer el cumplimiento de lo ya mencionado, por tanto, se mantiene la No Conformidad. En cuanto a lo indicado por el auditado "*se solicita respetuosamente retirar la no conformidad, ya que la misma no podría dar lugar a acciones de mejora toda vez que el nuevo documento corrige las debilidades del anterior*", es importante precisar que no se pueden realizar correcciones, no obstante, se pueden formular acciones correctivas que conlleven a la mejora del proceso.
5	Modelo de Seguridad y Privacidad de la Información MinTIC	No se evidencia que la fase de diagnóstico haya sido desarrollada por el IDPC previo a la etapa de planificación Ver numeral 1.4.1.1 **Respuesta y documentos aportados por el Auditado:** A la fecha el Instituto ya cuenta con el diagnóstico del Modelo de Seguridad y Privacidad de la Información MSPI. Anexo: Instrumento Evaluación MSPI - IDPC con corte a 31/10/2020, el cual arrojó como resultado: Cumplimiento PHVA 19 / 100, Evaluación de efectividad de los controles 28/100 con un

2.4 NO CONFORMIDADES - INCUMPLIMIENTOS		
No.	**Requisito**	**Descripción No Conformidad**
		nivel repetible Cumplimiento de ciberseguridad 26/100 Por lo expuesto anteriormente, se solicita respetuosamente retirar la no conformidad ✓ Instrumento de Identificación de la Línea Base de Seguridad – Hoja Portada del 31/10/2020 **Análisis de la respuesta y documentación:** Como se puede evidenciar, es un documento generado en el mes de octubre de 2020, es decir, no estaba dentro del alcance de la Auditoría, por tanto y en el entendido de que no se aporta documentación que corresponda al periodo evaluado, se mantiene la No Conformidad.
6	Decisión Andina 351 de 1993 y Plan Seguridad y Privacidad de la Información -IDPC V.2 del 28/01/2020	Instalación de software que por Ley requieren licencia, en equipos de alquiler conforme a lo explicado en el numeral 1.4.1.2.2.1 **Respuesta otorgada por el auditado:** Revisada la observación se procedió a realizar la verificación de los equipos de alquiler identificando que aquellos que tenían software (licencias de AUTOCAD con licencia de prueba de 30 días fueron reemplazados por equipos propios de la entidad y con licencias propias, teniendo en cuenta que el Instituto realizó el presente año una adquisición de licencias mayor a la de a años anteriores con el fin de mejorar el trabajo de funcionarios y contratistas de la entidad. **Análisis de la respuesta:** Conforme a lo anterior, se puede observar que en efecto se estaba transgrediendo la norma, para lo cual el auditado adelantó una corrección, por tanto, y con el propósito de que se tomen medidas para que esto no vuelva a ocurrir, se debe adelantar una acción correctiva, por lo que se mantiene la No Conformidad.
7	Plan Seguridad y Privacidad de la Información -IDPC V.2 del 28/01/2020	Ausencia de controles y limitaciones a información restringida y confidencial, de acuerdo a lo expuesto en el numeral 1.4.1.2.2.4 **Respuesta y documentos aportados por el Auditado:** Teniendo en cuenta la observación realizada de acuerdo a lo expuesto en el numeral 1.4.10.2.2.4 Se informa al grupo de Control Interno que se realizó el ajuste correspondiente en conjunto con el proveedor de correo electrónico para que la información que se encontraba expuesta quedará totalmente restringida. Anexo imagen de acceso restringido Por lo expuesto anteriormente, respetuosamente se solicita realizar la validación nuevamente y levantar la observación. ✓ Pantallazo, en el cual se evidencia que se restringió la página de acceso al drive de Backup.

2.4 NO CONFORMIDADES - INCUMPLIMIENTOS		
No.	**Requisito**	**Descripción No Conformidad**
		Análisis de la respuesta y documentación: En efecto, al verificar el acceso a los Backup creados por el Proceso, se pudo evidenciar que se restringió, es decir, se adelantó una corrección, no obstante y con el propósito de que esto no se repita, se debe adelantar una acción correctiva, por tanto, se mantiene la No Conformidad.
8	Modelo de Seguridad y Privacidad de la Información Guía No. 4 Roles y responsabilidades de seguridad y privacidad de la información	No se establecen funciones específicas para cada rol o responsable que interviene en la formulación, ejecución y seguimiento del Modelo de Seguridad y Privacidad de la Información. Ver numeral 1.4.1.2.4 **Respuesta otorgada por el Auditado:** El Instituto ya ha venido trabajando en la definición de roles y responsabilidades de seguridad de la información, el cual se entregará el día 10 de diciembre del presente año, mediante un acto administrativo. Por lo expuesto anteriormente, se solicita respetuosamente retirar la no conformidad. **Análisis de la Respuesta:** Conforme a la respuesta otorgada, implícitamente se acepta la No Conformidad, por tanto, esta se mantiene dado que las acciones se realizan posterior al alcance de la auditoría.
9	Modelo de Seguridad y Privacidad de la Información Guía No. 6 Gestión Documental	No se evidencia integración del Modelo de Seguridad y Privacidad de la Información con el proceso de Gestión Documental. Ver numeral 1.4.1.2.6 **Respuesta otorgada por el Auditado:** Se acepta la observación y se incluirá en los planes de seguridad y privacidad del 2021. El cual contempla las actividades del sistema de gestión documental electrónico de archivo – SGDEA. **Análisis de la Respuesta:** Conforme a la respuesta otorgada, se acepta la No Conformidad, por tanto, esta se mantiene.
10	Modelo de Seguridad y Privacidad de la Información – Plan de Comunicaciones Plan Estratégico de Tecnologías de la Información - Plan de Comunicaciones	No se cuenta con Plan de Comunicaciones definido para los diferentes instrumentos del proceso Gestión de Sistemas de Información y Tecnología, tales como Manual de Seguridad y PETI. Ver numeral 1.4.1.2.8 **Respuesta otorgada por el Auditado:** Se acepta la observación y se incluirá en los planes de seguridad y privacidad del 2021. **Análisis de la Respuesta:**

2.4 NO CONFORMIDADES - INCUMPLIMIENTOS		
No.	**Requisito**	**Descripción No Conformidad**
		Conforme a la respuesta otorgada, se acepta la No Conformidad, por tanto, esta se mantiene.
11	Modelo de Seguridad y Privacidad de la Información	No se cuenta con un plan de transición estructurado que cumpla con los requisitos de la Guía No 20 Transición de Ipv4 a Ipv6 para Colombia. Ver numeral 1.4.1.2.9 y numeral 1.4.3 **Respuesta y documentos aportados por el Auditado:** Se precisa que para la realización de la auditoría en ningún momento se solicitó información acerca de la transición de IPV4 a IPV6 en el Instituto por lo cual no fue entregada en su momento. Por lo tanto, se aclara que el Instituto realizó la contratación de un Ingeniero Experto para realizar la transición del protocolo IPV4 a IPV6 desde el mes Julio y que actualmente ya se cuenta con los documentos de Plan de Diagnóstico, Plan de Transición y Plan de direccionamiento IPV6, documentos que se han elaborado de acuerdo a la guía de transición IPV4 a IPV6 de Mintic. Los mismos se adjuntan como evidencia. Anexo Plan de Diagnóstico, Plan de Transición y Plan de direccionamiento IPV6. Por lo expuesto anteriormente, respetuosamente se solicita levantar la observación. ✓ Documento en borrador (sin fecha) denominado “Plan de Diagnostico IPv6” ✓ Hoja de Cálculo denominada “Plan de Direccionamiento IPV6-IDPC” ✓ Documento en borrador (sin fecha) denominado “Plan detallado del Proceso de Transición a IPv6” **Análisis de la respuesta y documentación:** Como se puede evidenciar, son documentos que aún no han sido objeto de publicación, es decir, no tienen vigencia, por tanto y en el entendido de que no se aporta documentación que corresponda al periodo evaluado, se mantiene la No Conformidad.
12	Modelo de Seguridad y Privacidad de la Información - Privacidad de la Información	Dentro de la revisión se evidenciaron debilidades en todas las fases que integran el componente de Privacidad de la Información del Modelo de Seguridad y Privacidad de la Información. Ver numeral 1.4.2 **Respuesta otorgada por el Auditado:** Se acepta la observación y se incluirá en los planes de seguridad y privacidad del 2021. **Análisis de la Respuesta:**

2.4 NO CONFORMIDADES - INCUMPLIMIENTOS		
No.	**Requisito**	**Descripción No Conformidad**
		Conforme a la respuesta otorgada, se acepta la No Conformidad, por tanto, esta se mantiene.
13	Procedimiento Atención de Requerimientos de Recursos Tecnológicos	No fue posible establecer los criterios de solución, término y efectividad de las solicitudes y soluciones en la mesa de ayuda, conforme a lo explicado en el numeral 1.5 **Respuesta otorgada por el Auditado:** El tiempo definido dentro de la parametrización de la Mesa de Ayuda es de máximo 24 horas para su atención y/o solución, tiempo que se cumple sin novedad alguna, como se puede evidenciar, no se tiene ninguna queja o reclamo donde algún usuario informe el incumplimiento de algún incidente o petición registrado en la Mesa de ayuda. No obstante, lo anterior la entidad cambiará el software de mesa de ayuda con el fin de mejorar estos informes. Por lo expuesto anteriormente, respetuosamente se solicita levantar la observación. **Análisis de la Respuesta:** Teniendo en cuenta que no se aporta documentación que pueda corroborar que estos seguimientos se hacen conforme al procedimiento, se mantiene la No Conformidad.
14	Caracterización del Proceso - Plan de Mantenimiento Preventivo y Correctivo	En relación con el Plan de Mantenimiento Preventivo y Correctivo se evidencian debilidades como: Ver numeral 1.5.6 ➢ No se realiza un plan de mantenimiento previo a la contratación del servicio. ➢ Se evidencia cronograma de mantenimiento de la vigencia 2019, el cual está firmado por el responsable de Almacén, sin contar con algún visto bueno desde el área de Sistemas, como expertos técnicos. ➢ No se evidencian soportes de todas las actividades programadas en el cronograma 2019. ➢ No se cuenta con Plan, ni cronograma de Mantenimiento definido para la vigencia 2020. **Respuesta y documentos aportados por el Auditado:** ● El plan de mantenimiento se realiza con base al diagnóstico realizado por el proponente al cual se le adjudica el contrato. ● El cronograma propuesto para el mantenimiento de los equipos tecnológicos, es firmado por el supervisor del contrato, no obstante, se cuenta con el apoyo y seguimiento del equipo de sistemas en la ejecución de las actividades. Lo anterior, toda vez que en el área de sistemas no se cuenta con funcionarios de planta. ● Las actividades programadas en el cronograma del mantenimiento

2.4 NO CONFORMIDADES - INCUMPLIMIENTOS		
No.	**Requisito**	**Descripción No Conformidad**
		realizado en el año 2019 fueron ejecutadas, por lo que se anexa evidencias del mantenimiento realizado a los switch y Planta Telefónica (equipos de comunicación), y los mantenimientos correctivos que fueron solicitados por la entidad. ● Se adjunta programación de actividades inicial del mantenimiento que se está llevando a cabo actualmente en el instituto, se anexa evidencia de los informes de mantenimiento que se han realizado a la fecha ya que este contrato actualmente se encuentra en ejecución ✓ Documento de "Julstar & Cía sas del 6/06/2019 "concepto técnico" de un vedo beam y cotización. ✓ Documento de "Julstar & Cía sas del 3/10/2019 "concepto técnico" de un vedo beam. ✓ Comunicación del 17/09/2020 de "Makro System Colombia S.AS.", en la que informa la relación de equipos existentes y cronograma propuesto para mantenimiento preventivo a realizarse en septiembre y octubre de 2020. ✓ Documentos diligenciados con el logo "Makro System Colombia S.AS.", relacionando uno a uno los equipos de la entidad y con la observación "se realiza mantenimiento físico preventivo del equipo" mantenimientos efectuados en septiembre y octubre de 2020 y cargado al contrato IDPC-PS-570-2020. ✓ Documento en Excel denominado "hoja de vida plante telefónica" con tres (3) hojas de cálculo, al parecer, contienen fotografías (no cargan) ✓ Documento en Excel denominado "hoja de vida switch fibra óptica" con tres (3) hojas de cálculo, con fotografías. **Análisis de la respuesta y documentación:** Es importante precisar que el plan de mantenimiento preventivo y correctivo debe ser definido de manera previa a la contratación, ya que este es el que determinará la necesidad de la Entidad para preservar el buen funcionamiento de los equipos que soportan la infraestructura. De igual manera, se observa que las debilidades evidenciadas no se subsanan con los documentos entregados, ya que si bien algunos de ellos corresponden al período auditado, la mayoría de ellos son posteriores al alcance de la auditoría, así mismo, la respuesta dada referente al acompañamiento de Sistemas en la formulación del plan, no cuenta con documento alguno que lo soporte. Teniendo en cuenta que no se atendió documentalmente con lo evidenciado en este numeral, se mantiene la No Conformidad.

3. CONCLUSIONES DE AUDITORIA

En el presente ejercicio de auditoria se concluye que el proceso Gestión de Sistemas de Información y Tecnología, el cual fue objeto de evaluación, cumple de manera parcial su objetivo, ya que se están desarrollando acciones para la mejora del mismo y se cuenta con los documentos requeridos normativamente, no obstante, se evidencian algunos incumplimientos legales susceptibles de mejoramiento, así como, observaciones y oportunidades de mejora, en su formulación, ejecución y seguimiento, debilidades que impiden determinar qué tan eficiente y efectivo es el proceso.

4. RECOMENDACIONES

- ✓ Revisar y adecuar la documentación del proceso, con el fin de contar con instrumentos que faciliten la planeación, ejecución y control de las actividades.
- ✓ Tener en cuenta las políticas propuestas por MinTIC, que si bien no son obligatorias, se tornan importantes para el desarrollo de los documentos del proceso en el IDPC.
- ✓ Unificar los lineamientos del Manual de Administración de Riesgos y el Plan de Tratamiento de Riesgos de Seguridad de la Información
- ✓ Tomar acciones que conlleven a la mejora en los acompañamientos realizados para el cargue y depuración de datos en aplicativos externos.
- ✓ Entregar información completa y que coincida con la solicitud que se le realice, que permita verificar el cumplimiento de las actividades planteadas en los diferentes documentos del proceso.
- ✓ Indicar en la normatividad descrita en los Planes y Procedimientos, de qué entidad es la normatividad, es decir, qué entidad la expidió. También que vayan en orden de importancia y fecha.
- ✓ Relacionar otras normas que tengan concordancia con el tema del PETI, es el caso del Decreto Nacional 1083 de 2015 (adicionado por el 415 de2016).
- ✓ Continuar documentando el apoyo técnico para la adquisición de bienes o contratación de servicios que incluyan un componente tecnológico.
- ✓ Incluir el componente de Privacidad de la Información, dentro del Modelo de Seguridad y Privacidad de la Información del IDPC.
- ✓ Revisar y actualizar los procedimientos existentes, con base en lo establecido en la Guía No. 3 de MinTIC Procedimientos de Seguridad de la Información.
- ✓ Desarrollar un adecuado Diagnóstico y Planificación para la generación de instrumentos como el PETI y el Modelo de Seguridad y Privacidad de la Información del IDPC.
- ✓ Adecuar el PETI y el Modelo de Seguridad de la información con base en los lineamientos establecidos en la materia.
- ✓ Establecer riesgos de Seguridad y Privacidad de la Información, con el fin de evitar su materialización o mitigar su impacto.
- ✓ Documentar los monitoreos realizados a los diferentes riesgos, así como a los relacionados con los contratistas o proveedores en relación a los objetos contractuales.
- ✓ Verificar el licenciamiento de todo el software instalado en el IDPC tanto en equipos propios como en los de alquiler y generar base de datos con información clara e identificación de la ubicación del software.
- ✓ Comprobar el estado de controles para el acceso a información restringida y confidencial.
- ✓ Formular e implementar Plan de Comunicaciones para los diferentes instrumentos del proceso Gestión de Sistemas de Información y Tecnología, tales como Manual de Seguridad y PETI
- ✓ Estructurar, ejecutar y monitorear Plan de transición de Ipv4 a Ipv6
- ✓ Implementar acciones y establecer mediciones que permitan evaluar los criterios de solución, término y efectividad de las solicitudes y respuestas en la mesa de ayuda, para identificar que los requerimientos se

4. RECOMENDACIONES

atendieron dentro de los términos y estos fueron efectivos.

- ✓ Formular, ejecutar y hacer seguimiento al Plan de Mantenimiento Preventivo y Correctivo, previo a la contratación de este servicio.

Este documento corresponde a los resultados del Informe Preliminar presentado y aprobado mediante acta de fecha 17-11-2020 con el Líder del Proceso Juan Fernando Acosta Mirkow y Responsable Operativo Mary Elizabeth Rojas Muñoz

EQUIPO AUDITOR (Firma)

ASESOR CONTROL INTERNO (firma)

No Radicado de entrega

20201200058633

FECHA DE ENTREGA	**30**	**11**	**2020**

5. RELACIÓN DE ANEXOS

No se cuenta con anexos