INFORMACIÓN GENERAL DE AUDITORÍA			
TIPO DE AUDITORÍA	AUDITORIA DE SISTEMAS		
INFORME PRELIMINAR	**25/03/2019**	**INFORME FINAL**	**04/04/2019**
PROCESO AUDITADO	Proceso de Gestión Tecnológica.		
LÍDER DEL PROCESO	OLGA LUCÍA SÁNCHEZ MENDIETA - JEFE OFICINA ASESORA DE PLANEACIÓN		
OBJETIVO DE LA AUDITORÍA	Evaluar el desarrollo y cumplimiento de las actividades asociadas al proceso de Gestión Tecnológica, así como la efectividad de los controles establecidos.		
ALCANCE DE LA AUDITORÍA	Controles generales de la gestión tecnología con respecto a los escenarios: • Planeación Estratégica del proceso. • Desarrollo y adquisición de software aplicativo • Administración de datos y seguridad lógica • Administración de recursos de TI.		
CRITERIOS DE LA AUDITORÍA	• PRO-GT-12-05 Mantenimiento de Infraestructura Tecnológica • PRO-GT-12-07 Registro de Activos de Información tipo Software, Hardware y Servicios • PRO-GT-12-08 Formulación y Seguimiento al PETIC • PRO-GT-12-10 Mesa de Servicios • Normatividad legal asociada al proceso.		
MARCO LEGAL			
LIMITACIONES DE LA AUDITORIA	**NINGUNA**		
EQUIPO AUDITOR:	**AUDITOR LÍDER:** YAMILE MORALES LAVERDE **EQUIPO AUDITOR:** YADIRA VELOSA		

1 METODOLOGÍA.

La auditoría de controles generales de la gestión TIC incluye las siguientes técnicas de auditoría aplicadas por el equipo auditor:

1. Levantamiento de información mediante entrevista
2. Análisis documental de políticas, procedimientos, planes y registros asociados a la gestión TIC y a la gestión de seguridad de la información
3. Entrevistas con una muestra de usuarios finales de los servicios TIC
4. Verificación de controles sobre una muestra de equipos de la red
5. Pruebas básicas de seguridad sobre la red

2 DESARROLLO DE LA AUDITORIA.

2.1 Planeación y Organización de la Gestión TIC

2.1.1 Gestión Estratégica de TI

La Oficina Asesora de Planeación quien es la responsable del proceso de Tecnologías de la Información y las Comunicaciones ha estructurado el procedimiento *PRO-GT-12-08_Formulacion_y_Seguimiento_al_PETIC_V4.pdf* y presentó para la vigencia 2019 el Plan Estratégico de Tecnologías de la Información actualizado a enero de 2019 (*PL-GT-12-01_PETIC_V9.pdf*), el cual refleja el interés de la OAP por dar cumplimiento a los lineamientos el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado colombiano y constituye un documento de base que puede ser fortalecido para que se establezca como guía estratégica para el mantenimiento y mejoramiento de la función tecnológica alineada a los objetivos estratégicos institucionales y garantizando la seguridad de la información del instituto.

Por su parte el Plan Operativo anual 2019 incluye correctamente las actividades de alto nivel que hacen parte de la gestión tecnológica de la entidad y que se perciben más estratégicas que los 6 proyectos formulados en el PETIC para el 2019 los cuales están más orientados al mantenimiento operativo de la plataforma tecnológica. El POA es también uno de los instrumentos de seguimiento trimestral a los objetivos planeados para cada año.

El Plan de adquisiciones 2019 por su parte, está alineado con el PETIC 2019 y refleja correctamente la planeación de la inversión tecnológica del instituto.

Con base en los dos documentos de planeación estratégica (POA y PETIC) y los planes tácticos entregados a la auditoría: *PL-GT-12-02_Plan_Contingencia _Tecno_V7*, *PL-GT-12-04_Plan_Seguridad_y_Privacidad_de_la_Info_V1 y PL-GT-12-05_ Plan Tratamiento_ de_riesgos_info_V1*, se presenta el análisis de cascada de su gestión a nivel estratégico, táctico y operativo:

NIVEL ESTRATEGICO POA	NIVEL ESTRATEGICO PETIC	NIVEL TACTICO PLAN DE ACCIÓN	NIVEL OPERATIVO Control periódico de actividades puntuales por Proyecto
Actualizar el plan de contingencia tecnológica	La actualización del plan de contingencia se menciona dentro de las actividades ejecutadas, pero no en los proyectos del PETIC	Se ha construido el documento *PL-GT-12-02_Plan_Contingencia _Tecno_V7*, sobre el cual se emiten observaciones en el numeral 3.1.3.2	Los avances registrados en el seguimiento al POA 2018 están orientados al avance en el documento, pero no incluye actividades de prueba sobre el plan de contingencia. Se entiende que el documento se encuentra en construcción.
Formular, ejecutar y hacer seguimiento del PETIC 2019	El PETIC presenta 6 proyectos 2019 orientados al mantenimiento de la Plataforma TIC	No se observan planes tácticos asociados a los proyectos.	En los seguimientos a los planes de acción 2018 se refleja el seguimiento trimestral a las actividades de adquisición y contratación

NIVEL ESTRATEGICO POA	NIVEL ESTRATEGICO PETIC	NIVEL TACTICO PLAN DE ACCIÓN	NIVEL OPERATIVO Control periódico de actividades puntuales por Proyecto
Formular y ejecutar el plan de trabajo de acuerdo a los lineamientos establecidos en las políticas de "Seguridad digital", "Gobierno digital" y "Transparencia acceso a la información y lucha contra la corrupción" de MIPG para la implementación de estas políticas.	Si bien en el Proyecto 5 del PETIC se incluye la contratación de "*Prestación de servicios profesionales para la implementación de las políticas de Gobierno Digital y Seguridad Digital del MIPG y la sostenibilidad del Subsistema de Seguridad de la Información y del proceso de Gestión Tecnológica, así como el soporte técnico a la infraestructura tecnológica del IDEP*", en la realidad el contrato 28 de 2019 que corresponde a la profesional JULIETT YAVER quien, de acuerdo a la entrevista, no es experta en esta implementación y cuyas funciones están orientadas principalmente al soporte GOOBI	El contrato 28 de 2019 incluye dentro de las obligaciones del contratista la entrega del cronograma de actividades de Tl y que permitan dar cumplimiento a la implementación de las políticas de i) Gobierno Digital y ii) Seguridad Digital que hacen parte del MIPG. Pero se observa que ni las actividades del cronograma ni el informe al 20 de febrero de 2019 entregado por el contratista publicado en SECOP II tienen trazabilidad con los porcentajes de cumplimiento de las herramientas de autodiagnóstico presentadas por el IDEP	A la fecha de la auditoría se encuentra publicado en SECOP II el primer producto de ejecución del contrato 28 de 2019 que incluye "Producto 3 Informe de actividades TI con las actividades a ejecutar por el contratista para dar cumplimiento a la implementación de i) Gobierno Digital y ¡i) Seguridad Digital". Se observa que las actividades asignadas tienen relación parcial, pero no tienen trazabilidad con los porcentajes de cumplimiento de las herramientas de autodiagnóstico presentadas por el IDEP ni con los lineamientos del MIPG al respecto. No se observa en el documento cuales son los criterios de aceptación para estos entregables ni su relación con los dominios de la implementación del MSPI
Formular, ejecutar y hacer seguimiento del Plan de tratamiento de riesgos de seguridad y privacidad de la información 2019	Se nombran dos riesgos en el numeral 7.1 Indicadores y Riesgos de TI del PETIC. No hay proyecto explícito al respecto	Se ha construido el documento *PL-GT-12-05_Plan_Tratamiendo_de_riesgos_info_V1*, sobre el cual se emiten observaciones en el numeral 3.1.3	Se llevan los documento *Mapa_Riesgos_Institucional_y_de_Corrupcion_por_Proceso_ 2019.xlsx* y *Plan_Mejoramiento_Procesos* los cuales son objeto de seguimiento trimestral

NIVEL ESTRATEGICO POA	NIVEL ESTRATEGICO PETIC	NIVEL TACTICO PLAN DE ACCIÓN	NIVEL OPERATIVO Control periódico de actividades puntuales por Proyecto
Formular y hacer seguimiento al plan de acción del Subsistema de Seguridad de la información	Se informa el avance al respecto y la conformación del Gobierno para su gestión e implementación	Se ha construido el documento *PL-GT-12-04_Plan_Seguridad_y_Privacidad_de_la_Info_V1*, sobre el cual se emiten observaciones en el numeral 3.1.4	En los seguimientos a los planes de acción 2018 se refleja el seguimiento trimestral a las actividades relacionadas.

- Con lo anterior se puede concluir que la OAP cuenta con instrumentos de planeación estratégica y táctica con asignación de fechas y responsables al igual que instrumentos de seguimiento a las actividades. Sin embargo, se observa que varias actividades son asignadas a los 3 recursos de manera simultánea y no se evidencia que las fechas de cumplimiento están calculadas con base en una estimación de esfuerzo vs la capacidad de trabajo disponible.

- El PETIC no incluye un análisis de capacidad y efectividad de los elementos de operación, aseguramiento y administración la plataforma tecnológica como base para la identificación de debilidades, amenazas, fortalezas y oportunidades que permitan establecer acciones y/o adquisiciones para para asegurar la continuidad de operaciones y aseguramiento de la información bajo el mejor uso de recursos.

- En cuanto a las actividades puntuales incluidas en los documentos de planeación que están relacionadas con la adquisición de herramientas TIC, no se incluyen actividades que permitan asegurar la mejor configuración y operación para obtener el mayor aprovechamiento de la inversión, al igual que actividades de transferencia de conocimiento o formación a los colaboradores TIC para garantizar la mejor administración. Tal es el caso de las herramientas de Firewall, Antivirus y GSuite en las cuales el auditor encontró obviedades en su configuración y observo debilidades en el conocimiento de las personas a cargo de su administración. Ver 3.2.

- Con respecto a los instrumentos de medición, el PETIC declara dos indicadores de gestión, orientados a la medición de eficiencia de atención de solicitudes de la mesa de ayuda y de cumplimiento de actividades del PETIC y el documento *INDICADORES GT 2019.xls*, incluye un tercer indicador de cumplimiento de actividades del Plan de seguridad y privacidad de la información, pero no se han establecido indicadores de eficacia y calidad asociados a la función TIC ni a la disponibilidad de la plataforma. Sobre los indicadores declarados se emiten las siguientes observaciones:

- **Eficacia en la atención de solicitudes recibidas a través de mesa de ayuda**: este indicador no corresponde con la realidad del total de solicitudes de soporte bajo la responsabilidad de la OAP, ya que tanto los soportes de Humano como de GOOBI son direccionados a los proveedores sin que sean previamente registrados en OSTicket. De igual manera al no estar establecidos los ANS internos para la atención de incidentes el indicador no evidencia el cumplimiento de tiempos de atención oportunos.
- **Cumplimiento de las actividades del PETIC**: si bien el indicador mide cumplimiento en términos de fechas proyectadas en el Plan de adquisiciones, no ofrece resultados frente al cumplimiento de calidad de las actividades puntuales.
- **Cumplimiento de las actividades del Plan de Seguridad y privacidad de la información**: si bien el indicador mide cumplimiento en términos de fechas proyectadas de las actividades del Plan, no ofrece resultados de nivel de madurez en la implementación de controles de seguridad. Las debilidades en esta materia se evidencian en el numeral 3.2 del presente informe

- En cuanto al cumplimiento de requisitos legales, todos los documentos generados por la OAP incluyen las referencias normativas y regulatorias que aplican.

Frente a los dominios del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado colombiano (MRAE), el PETIC incluye 5 de los 6 dominios sobre los cuales se emiten observaciones:

- Acorde a la **Estrategia de TI** y conforme con lo establecido por el PEDI 2016-2020, se entiende que el PETIC se encuentra alineado al Proyecto de inversión 1039: *Fortalecimiento a la Gestión Institucional* cuya meta fundamental es garantizar la sostenibilidad del Sistema Integrado de Gestión en el IDEP entre los que se encuentra el Subsistema de Seguridad de la Información, lo cual es consistente con los compromisos del PETIC en *5.1.5 Políticas de Tecnologías de la Información y las Comunicaciones del IDEP,* sin embargo la implementación del MSPI a pesar de su envergadura no se encuentra como un proyecto independiente entre los 6 proyectos formulados para la vigencia 2019 y los planes y políticas establecidos no dan cobertura al alcance del MSPI (*Plan de seguridad y privacidad de la información 2019, Plan de tratamiento de riesgos de seguridad y privacidad de la información 2019, Política Seguridad y privacidad de la información*), sobre los cuales se emiten observaciones de mejora en el presente informe (3.1.3 y 3.1.4)
- En cuanto al **uso y apropiación de TI**, se contemplan campañas de divulgación vía correo electrónico las cuales se vienen aplicando de manera periódica. Los 7 usuarios entrevistados confirman recibir estos correos, pero manifiestan que no han recibido capacitaciones formales, que no se les aplica encuestas de satisfacción y que no les han sido entregadas formalmente políticas de seguridad de la información puntuales sobre su responsabilidad en el uso y protección de los activos de información del instituto. De igual manera los indicadores planteados en el PETIC no incluyen medición del uso y apropiación de las mismas.

- En el capítulo de **sistemas de información** se listan los actualmente existentes, pero no se desarrolla el dominio siguiendo los lineamientos (MRAE) en cuanto a la construcción de un modelo metodológico de estandarización, gestión de cambios y apropiación del control, mantenimiento y conocimiento. Este componente es relevante en la entidad ya que se observa una alta dependencia de conocimiento y control de los proveedores sobre los sistemas Humano y GOBBI, además de los problemas de integración entre estos dos sistemas.
- El dominio de **Servicios Tecnológicos** muestra una descripción de las mejoras realizadas a la plataforma tecnológica desde el año 2016, las condiciones de conectividad y el modelo de administración, sin embargo, no está desarrollada conforme a los lineamientos (MRAE) la estructura de modelo de servicios tecnológicos con su correspondiente planeación de capacidad, documentación suficiente de operación e infraestructura y mesa de servicios TIC centralizada con ANS y articulación de terceros.
- En cuanto al **Gobierno de TI**, el instituto ha instaurado de manera correcta el Comité de Sistemas, Informática y de Seguridad de la Información -Resolución 159 de 2009, el cual opera como órgano decisorio en materia de inversión TIC. El PETIC incluye la matriz de roles en la cual se establecen las responsabilidades, entre las que se observa la asignación del Técnico Operativo como Oficial de Seguridad de la Información, quien de acuerdo a la entrevista realizada no tiene las competencias de conocimiento para asumir el rol ni la disponibilidad que requiere la implementación del MSPI.
- **Gestión de Información**: este dominio no ha sido desarrollado, y es el que permite definir: el diseño de los servicios de información, la gestión del ciclo de vida del dato, al análisis de información y el desarrollo de capacidades para el uso estratégico de la misma mediante el desarrollo de los 4 componentes de información: Planeación y Gobierno, Diseño, Análisis y Aprovechamiento y Calidad y Seguridad.

2.1.1.1 Recomendaciones

N°.	
1.	Como insumo para la formulación del PETIC, adelantar un análisis DOFA sobre la plataforma tecnológica, recursos TIC y competencia y conocimiento de los recursos humanos del IDEP en relación con la capacidad de ofrecer continuidad, seguridad de la información y desempeño aceptable para soportar los requisitos externos, requisitos de la entidad, proyectos propios TIC y oportunidades de innovación. El análisis DOFA ofrecerá elementos para identificar necesidades de conocimiento y proyectos estratégicos además de proyectos orientados al mantenimiento de la plataforma tecnológica. Aprovechar la nueva formulación del PEDI para la vigencia 2020 - 2024 para proyectar el PETIC a 4 años como lo recomienda el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado colombiano.
2.	Realizar un análisis de los lineamientos del MIPG y del MSPI para construir un plan de proyecto proyectado al 2020 que permita dar cumplimiento a las políticas de "Seguridad digital", "Gobierno digital" y "Transparencia acceso a la información y lucha contra la corrupción" de MIPG y al MSPI. De ser posible contratar consultoría especializada o en su defecto fortalecer los conocimientos del funcionario de planta a través de procesos de formación.

N°.	
	Para la implementación del MSPI es recomendable que el oficial de seguridad tenga conocimientos en implementación de los controles de seguridad de la información con base en la norma ISO 27001:2013 y dedicación suficiente al proyecto.
3.	Con relación a los Cronogramas para Control del Proyecto se recomienda: • Garantizar que para cada proyecto del PETIC se establezcan planes de acción tácticos que incluyan las actividades a ser ejecutadas por personal interno o por terceros para garantizar que los activos de información adquiridos queden debidamente configurados de acuerdo a las mejores prácticas y que el conocimiento para su operación y administración quede transferido al instituto. • Para todos los planes tácticos establecer las fechas y responsables con base en un análisis de estimación de esfuerzo por tareas versus la capacidad de trabajo instalada. Esto con el fin de identificar necesidades de recurso humano y establecer fechas viables de cumplimiento. • Antes del cálculo de capacidad disponible deben sustraerse los tiempos requeridos por cada recurso para la atención de funciones de rutina. • Establecer criterios de aceptación de las actividades programadas para determinar su verdadero estado de cierre. De ser posible implementar pruebas cruzadas para verificar la calidad de los resultados. • Asignar tareas de manera individual con el fin de medir cumplimiento y productividad por recurso. • Priorizar las tareas de acuerdo con: o Prioridad 1: requisitos regulatorios o normativos o Prioridad 2: de valor agregado para los procesos misionales o Prioridad 3: de valor agregado para el desempeño o seguridad de la plataforma tecnológica o Prioridad 4: de valor agregado para los procesos de apoyo o Prioridad 5: relevancia particular del solicitante
4.	Incorporar en los Indicadores y Riesgos del PETIC indicadores asociados a la medición de cumplimiento, productividad y calidad en los servicios TIC y proyectos, seleccionando aquellos que sean pertinentes entre los recomendados por el Marco de Referencia de Arquitectura Empresarial de TI, especialmente en el dominio Gobierno de TI: • Indicador de beneficio del servicio. • Indicador de inversiones sustentadas. • Indicador de incidentes. • Indicador de seguimiento a riesgos de TI. • Indicador de entrenamiento relacionado con regulación y políticas de TI. • Indicador de no cumplimiento de regulaciones externas. • Indicador ejecución PETI. • Indicador de empoderamiento. • Índice de rotación de personal. • Desviación en capacidad de los servicios. • Dificultades por capacidad en proyectos de TI. • Calidad en los informes de gestión. • Satisfacción de usuarios. • Índice promedio de desempeño del Cronograma de los Proyectos de TI en Ejecución. • Índice promedio de desempeño de los Costos de los Proyectos de TI en Ejecución • Cumplimiento de proyectos de TI.

N°.	
	• Implementación Modelo de Gestión Estratégica de TI. Antes de formular el cálculo de indicadores se recomienda atender las recomendaciones de centralización de mesa de servicio del numeral 3.5.2, con tres propósitos: • No generar carga operativa adicional a los colaboradores de la OAP • Llevar un control centralizado de la información de servicios TIC • Llevar control centralizado de acuerdo de niveles de servicio internos y con terceros • Contar que una base de datos que permita establecer las dedicaciones del personal de sistemas en la atención de requerimientos
5.	Adelantar la estructuración de los proyectos de uso y apropiación de tecnología una vez hayan sido documentadas y formalizadas todas las políticas de seguridad de la información del MSPI de manera integrada con el control 7.2.2 Concientización, educación y capacitación sobre la seguridad de la información de la norma ISO 27002:2013

2.1.2 Estructura Organizacional y Gobierno de TI

2.1.2.1 Recomendaciones

N°.	
1.	• Adelantar una matriz de Cargos vs Funciones vs documentos, que incluya para cada cargo cuales son los conocimientos específicos que deben ser trasferidos, que documentos de procedimientos e instructivos deben incorporarse a la transferencia y el cargo de contingencia. • Formalizar un Plan de Transferencia de Conocimiento especifico especialmente entre funcionarios y contratistas, que haciendo uso de un número de horas a la semana por colaborador se ejecute: o La elaboración de los instructivos y procedimientos (que aún no existan) correspondientes a sus funciones de acuerdo con Matrices de Cargos vs Funciones vs documentos. o Capacitación en las funciones de su cargo, incluyendo incidentes y recuperaciones para el funcionario identificado como contingencia. o Elaborar un plan de rotación de funciones temporal, entre colaboradores principales y de contingencia. Evaluar resultados. Este ejercicio puede incorporarse a la documentación de Plan de continuidad de negocio y al desarrollo del dominio 17 (continuidad) del Modelo de Seguridad y Privacidad de la Información (MSPI) ya que conforme a la norma ISO 27001:2013 el personal con conocimientos específicos también es un activo de información y es objeto de tratamiento de riesgos por ausencia temporal o permanente.
2.	De ser posible, adelantar procesos de capacitación al funcionario de sistemas de la OAP para disminuir la dependencia de conocimiento de los proveedores del firewall, antivirus y hiperconvergencia y otros elementos de gestión de operaciones TIC. En los estudios previos de contratistas fortalecer los requisitos de conocimientos en seguridad

N°.	
3.	De ser posible incluir en las obligaciones de los contratistas la elaboración de instructivos de transferencia de conocimiento y un servicio de empalme al IDEP asociado al último producto del contrato que incluya por lo menos registros documentales de cambios, seguimiento a los contratos y procedimientos de operación.
4.	Adelantar acuerdos de confidencialidad con los contratistas.
5.	Solicitar a los proveedores de los sistemas Humano y Goobi las licencias de uso a favor del IDEP y para el caso de IT GOP SAS solicitar el registro de derechos de autor actualizado.
6.	Adelantar un análisis de capacidad de los recursos humanos actuales con que cuenta la OAP con respecto a los requisitos de esfuerzo para adelantar las funciones de la gestión TIC, de Gestión de Seguridad de la Información y la atención de proyectos. Esto con el fin de determinar si los recursos actuales son suficientes para atender la demanda funcional. De ser posible, mejorar los perfiles de los contratistas o vincular uno adicional para la implementación MSPI.
7.	Atender las recomendaciones de centralización de mesa de servicio del numeral 3.5.2 en la herramienta OSTicket con el fin de llevar control sobre el cumplimiento de los ANS de los proveedores.
8.	De ser posible, continuar con la búsqueda de alternativas para la adquisición de un sistema ERP en remplazo de Goobi. Analizar la opción de un sistema por servicio, lo cual podría resultar más económico que la instalación local. De igual manera no sesgar las especificaciones técnicas a una interfaz preexistente con el sistema Humano, sino a la capacidad de cargar archivos planos con información de nómina para su procesamiento contable.
9.	Establecer como política de seguridad del MSPI dominio 15 la inclusión de criterios de aceptación de entregables, políticas de gestión de cambios y requisitos de seguridad para futuros contratos con terceros
10.	Diseñar y aplicar anualmente encuestas de satisfacción a usuarios finales, sobre los servicios de TI, orientados a identificar mejoras con respecto a: servicio de soporte, disponibilidad de los recursos, uso responsable de los recursos, conocimiento de las políticas de seguridad, necesidades de capacitación, subutilización de herramientas, redundancia en fuentes de información, requerimientos para minimizar las labores operativas y almacenamiento y disponibilidad de documentos. Con base en los resultados diseñar acciones correctivas e incluirlas en el PETIC del siguiente periodo

2.1.3 Plan de Administración de Riesgos y Contingencias

2.1.3.1 Recomendaciones

N°.	OBSERVACIÓN
1.	Se establezcan actividades de prueba y verificación sobre los controles establecidos en la matriz de riesgos y las acciones del Plan de mejoramiento como requisito para dar por cerrada una acción o una actividad de control.
2.	Priorizar las acciones de acuerdo con el impacto para la entidad de su no ejecución, aplicar el mismo criterio para las decisiones de eliminación de acciones.

N°.	OBSERVACIÓN
3.	En el marco de la implementación del MSPI actualizar la identificación de la matriz de riesgos de acuerdo con los activos de información y depurar las acciones y controles reportados de acuerdo con las configuraciones de dichos controles en la plataforma TIC. Seguir los lineamientos de la Guía 7. Actualizar el Plan de Continuidad para que coincida en lo relacionado con el plan de tratamiento de riesgos, el formato de matriz de riesgos y la tipología de los riesgos Cabe anotar que el Plan de Continuidad está directamente relacionado con los riesgos que la entidad ha decidido tratar mediante aceptación
4.	De ser posible fortalecer el conocimiento en seguridad de la información del funcionario de la OAP o mejorar el perfil en esta materia para los contratistas.
5.	Ajustar el Plan de contingencias para que incluya como mínimo: • Todos los activos de información críticos • Los acuerdos ANS alcanzados con los responsables de procesos • Incluir respaldo de elementos de configuración de la plataforma TIC que permitan ya sea contar con ambientes replica o agilizar los tiempos de puesta en operación de la contingencia. • Ajustar las actividades y planes de contingencia específicos conforme a los acuerdos alcanzados con el negocio • Incluir los planes de recuperación a la operación normal con tiempos y responsables
6.	Adelantar las pruebas integrales al Plan de Continuidad y documentar los protocolos y resultados, contemplar los lineamientos de ISO 27002:2013 en el control 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
7.	Incluir en el inventario de programación de copias de respaldo el Backup de los archivos de configuración de los sistemas manejadores de bases de datos (RDBMS)
8.	En el marco de la implementación MSPI dominio 12.3 documentar las políticas, procedimientos e instructivos de gestión de copias de respaldo y recuperación.
9.	Incluir en los estudios previos de la adquisición de la herramienta de Backup, la configuración optima de la consola por parte del proveedor y la transferencia de conocimiento para establecer procedimientos efectivos de programación de copias de respaldo, suficiencia en la cobertura, control y monitoreo de logs, acciones correctivas oportunas y pruebas de restauración.

2.1.4 Políticas de Seguridad

2.1.4.1 Recomendaciones

N°.	OBSERVACIÓN
1.	Continuar la implementación del modelo MSPI dando prioridad a: • Optimización del inventario de activos • Identificación y valoración de riesgos por objetivos de control • Levantamiento de la declaración de aplicabilidad • La elaboración del marco documental de políticas, procedimientos, instructivos y formatos alineados a los controles aplicables • Fortalecer la política de seguridad de la información con los elementos puntuales que direccionan la actuación de los funcionarios, contratistas y proveedores en el uso y responsabilidad sobre los activos de información y privilegios.

N°.	OBSERVACIÓN
	• Adelantar un programa de programa de concientización, educación y capacitación sobre la seguridad de la información (control 7.2.2 ISO 27002:2013) y entregar formalmente la política. • Adelantar los planes de Implementación de los controles de seguridad de la información en la plataforma TIC Se recomienda adelantar una inspección de análisis de vulnerabilidades una vez finalizada la implementación para verificar su eficacia.

2.2 Administración de accesos y Seguridad Lógica

2.2.1 Recomendaciones

N°.	OBSERVACIÓN
1.	Dados los resultados de las pruebas de seguridad adelantadas por el auditor, se recomienda fortalecer y replantear el *PL-GT-12-04_Plan_Seguridad_y_Privacidad_de_la_Info_V1,* como un proyecto de implementación del MSPI atendiendo los controles establecidos por la norma ISO 27001:2013 que realmente garanticen el aseguramiento de la plataforma y no únicamente un cumplimiento documental parcial. Un sistema de gestión de seguridad de la información correctamente implementado es aquel que incluye los controles tecnológicos que aseguren la plataforma TIC y la información de la entidad. Se recomienda si es posible contratar consultoría especializada.
2.	Incluir en el *PL-GT-12-04* la adopción IPV6 incluyendo el diagnostico que permita identificar el alcance y acciones para una correcta implementación
3.	Ajustar el diagrama de infraestructura de acuerdo con las observaciones emitidas en el presente informe.
4.	Atender las debilidades en la configuración del Firewall con las siguientes acciones: activar las detecciones de seguridad para intrusos, virus, cambios de configuración de correo y exceso de cuota de disco.
5.	Para mejorar el nivel de monitoreo y seguridad, se recomienda separar el grupo de servidores a un segmento de la LAN diferente al de los equipos de usuario y configurarlo para que el Firewall pueda monitorear la interacción de los usuarios con los servidores.
6.	Configurar el sistema de protección de intrusos habilitando los filtros basados en firmas que permiten bloquear ataques de denegación de servicios y/o de fuerza bruta
7.	Como parte de la implementación del MSPI Dominio 12 Gestión de Operaciones, adelantar y poner en funcionamiento un procedimiento de registro, monitoreo y medición de capacidad y desempeño, que incluya las siguientes acciones y sus responsables: • Identificar los recursos tecnológicos y los sistemas operacionales que generarán logs de eventos de acuerdo con el nivel de criticidad establecido en el inventario de activos (incluyendo el firewall, antivirus, SO Red, sistemas de información, procesos de Backup, etc.) • Establecer las pautas requeridas para habilitar el registro de eventos, excepciones y fallas, utilizando logs y/o sistemas de registro.

N°.	OBSERVACIÓN
	• Realizar un monitoreo periódico de los logs y/o sistemas de registro que sean generados en la operación diaria de los activos de información, para identificar vulnerabilidades técnicas emergentes • Prevenir la modificación y eliminación de los logs y/o datos administrados en sistemas de registro por parte de usuarios con credenciales de acceso, incluyendo aquellos que tengan "acceso privilegiado" • Establecer y ejecutar tareas automáticas de respaldo de logs mediante su programación en el plan de copias respaldo • Definir un repositorio exclusivo donde se centralicen todos los logs generados a los cuales debe aplicarse mecanismos de encriptación durante la centralización, esto con el propósito de adelantar labores de monitoreo y análisis de eventos • Finalmente tomar control sobre los logs de auditoría generados por los sistemas de información Humano y Goobi.
8.	Como parte de la implementación del MSPI dominio 10. Cifrado, hacer el levantamiento de los activos de información en custodia o transito que requieren de algoritmos de encriptación. Atender como mínimo: • Aplicar un algoritmo de encriptación para el archivo que contiene las claves de administrador y establecer una política de cambio mensual y en caso del retiro de algún funcionario o contratista conocedor de las claves. Este elemento también hace parte del MSPI dominio 9 Gestión de accesos- accesos privilegiados • Archivos de alta confidencialidad almacenados en Drive o carpetas compartidas o en transito como adjuntos de correo electrónicos. • Dispositivos móviles o de almacenamiento externo que puedan tener información confidencial.
9.	Hacer extensivas las configuraciones de los equipos Windows a los equipos Mac en todo lo referente a políticas de seguridad de dominio, firewall y antivirus.
10.	Configurar las reglas de red de aplicación máximas del antivirus para aplicaciones de alta peligrosidad como sniffers, man in the middle, etc. Revisar las reglas de restricción mínima contra los listados de software permitido.
11.	Como parte de la implementación del MSPI dominio 8 Gestión de Activos, fortalecer el inventario de activos de información del instituto ya que el inventario actual se limita a Hardware y Software base y no incluye otros activos de información críticos tales como: bases de datos, documentos confidenciales, ficheros, aplicaciones, herramientas de desarrollo, publicación de contenidos, entre otros. Cada uno de los activos mencionados debe tener un responsable y calificación de criticidad de la información con base en su: Disponibilidad (importancia que tiene la ausencia del activo), Integridad (qué repercusiones tendría la modificación de este activo sin autorización) y confidencialidad. Vale aclarar que el inventario de activos de acuerdo con los lineamientos MSPI en concordancia con ISO 27001:2013 debe incluir todo aquel software autorizado para ser usado en la empresa independientemente de que sea software libre.
12.	Configurar correctamente las VLAN´s para evitar que se realicen escaneos a direcciones IP diferentes a la del segmento en la que se encuentra configurado cada equipo, incluyendo el segmento de la WIFI de invitados.
13.	Configurar la red y el DHCP para restringir la conexión al dominio solo a equipos cuya Mac Address este registrada en la lista autorizada

N°.	OBSERVACIÓN
14.	Configurar las restricciones de seguridad de GSuite en cuanto a: • Cambio periódico de contraseñas • No repetición de las ultimas 8 contraseñas • Alertas de ingreso en equipos distintos a los usuales a un correo alternativo • Configurar correctamente la autenticación de doble factor (pre-registro)
15.	Fortalecer la configuración de las políticas de firewall y las políticas de dominio para impedir descargas de archivos ejecutables. La restricción debe ser general independientemente del cargo del usuario. Todo archivo ejecutable que se requiera debe ser autorizado por la OAP.
16.	Instalar una herramienta gratuita que escanee periódicamente los recursos compartidos en la red e identifique cuales se encuentran sin protección y configurar las debidas restricciones de acceso (ejemplo: essential nettools, NetShareWatcher, etc)
17.	Restringir en todos los equipos de escritorio y portátiles el acceso al panel de control y en especial al centro de redes.
18.	Por ningún motivo exponer información de claves de acceso en el sistema de help desk o en correos sin la verificación inmediata del cambio de credenciales.
19.	Revisar los niveles de acceso a la navegación en internet con el fin de garantizar que todos los usuarios tengan privilegios acordes con las funciones de su cargo. No es recomendable que en las oficinas se ingrese a correos personales, redes sociales, etc a menos de que sean necesarios para la ejecución de sus funciones
20.	Establecer un plan para tomar control de la administración, configuración y control de cambios del sistema Goobi. Replantear la autorización de conectividad por VPN restringiendo el horario de conexión, asegurando el monitoreo durante la conexión y solicitar autorización antes de la conexión. Establecer un protocolo de cambios para que el IDEP ejecute los despliegues en producción con base en una entrega de objetos de despliegue, minutograma y procesos de rollback.
21.	Configurar todas las directivas de seguridad del dominio de acuerdo con las recomendaciones de Microsoft para entornos corporativos y las recomendaciones emitidas por el auditor. Implementar medidas automáticas o manuales para aplicar complejidad de contraseñas en el acceso a servicios TIC y para su cambio periódico y no reutilización
22.	Diseñar y formalizar un acta de entrega de activos TIC que incluya como mínimo: Equipos, Periféricos especiales, Software instalado, Accesos concedidos y privilegios, Controles de verificación de cambio de credenciales y accesos exitosos y Entrega de políticas de seguridad A continuación, se incluye un ejemplo de acta de alta:

N°.	OBSERVACIÓN

Fecha de entrega:		Compañía	
Nombre del funcionario:		Cargo	
Area		Jefe Inmediato	

Equipo o Herramienta	Características	
Computador y equipos	PC de escritorio ____ Portátil _____ Marca _____ Cargador _____ Id Inventario _____ Serial S/N _____ Estado _____	Impresora _____ Escáner _____ Diadema _____ Videoconferencia __ Nombre: _____ Serial _____ Cargador _____ Otro _____
Cámara fotográfica	Marca _____ Cargador _____ Estado _____	Serial S/N _____ Memoria _____ Capacidad _____
Unidad de almacenamiento externa	Tipo: Disco Duro_____ USB _____ Cables_____	Serial Disco Duro S/N _____ Estado _____
Telefonía	Telefonía Fijo __ Clave llamadas celular ___ Clave llamadas nacional ___ Clave llamadas internacional ___	Celular Plan Voz ___ Celular Plan Voz y Datos ___ Equipo marca: _____ Serial: _____ Numero: _____ Accesorios:_____
	¿El usuario valida la correcta funcionalidad de sus servicios de telefonía? SI ___ NO ____	
Otros: _____	Especificaciones: _____ _____	
Firma de aceptación de los equipos marcados (X)		

Servicio TIC	Características	
Usuario de Dominio	Nombre usuario: ----------	¿El usuario ingreso y realizo cambio de clave? SI ___ NO ____
Correo corporativo	Cuenta de correo: ----------	¿El usuario ingreso y realizo cambio de clave? SI ___ NO ____
Acceso a Internet	Nivel de privilegios A _____ B _____	¿El usuario navega con las restricciones establecidas? SI ___ NO ____
Acceso a Intranet	¿El usuario ingreso correctamente a la intranet y navega correctamente? SI ___ NO ___	

N°.	OBSERVACIÓN

Servicio TIC	Características	
Carpetas Compartidas	Listado de Carpetas: ¿El usuario ingreso correctamente únicamente a las carpetas asignadas? SI ___ NO ___	
Servicios de Impresión y Escáner	Usuario asignado _____ ¿El usuario ingreso correctamente su clave de acceso para imprimir? SI ___ NO ____	¿El usuario ingreso su clave para escáner y el archivo fue enviado a su correo corporativo? SI ___ NO ____
Aplicaciones instaladas en equipo	Office Standard _____ Office Professional _____ Project _____ NOD 32 _____ PC Backup ____ AutoCad ____ Visual Studio ___ Gestion 360 ____ Skype PC ____ SAP BO XI 3.2 (suite)____ SKETCH-UP_____	

Acceso a Sistemas de Información	NOMBRE DEL SISTEMA	PERFIL ASIGNADO	¿El usuario ingreso y cambio su clave?
	GOOBI		
	HUMANO		
	OSTickets		
	KOHA		
	OJS		
	DSPACE		

Otros: _____	Especificaciones: _____
Firma de aceptación de los servicios marcados (X)	

I. Condiciones

1. No se puede ceder las herramientas, equipos de trabajo o acceso a servicios sin previa autorización escrita.
2. El usuario se compromete a responder ante la empresa por daño a equipos, herramientas e información ocasionado por mal uso, hurto o pérdida.
3. Las herramientas, equipos de trabajo e información son de propiedad de la empresa.
4. Las claves de acceso otorgadas son de carácter reservado por lo tanto el usuario se compromete a no divulgarla ni exponerla.
5. El usuario se compromete a cumplir a cabalidad las Políticas de Seguridad de la Información relacionadas con el uso responsable y seguro de los activos de información que le han sido entregados.
6. Al momento de la desvinculación laboral se debe hacer devolución de las herramientas o equipos de trabajo conforme a las políticas establecidas por la compañía.
7. Cualquier cambio a los equipos, herramientas o accesos otorgados debe tramitarse con el Director de Área.
8. Para Celular: Autorización de descuento del pago del mes de consumos adicionales y/o extras que excedan el plan, por concepto del servicio del celular.

2.3 Seguridad física del Centro de Cómputo y oficinas

2.3.1 Recomendaciones

N°.	OBSERVACIÓN
1.	Evaluar la posibilidad de implementar el control de acceso biométrico al centro de cómputo, utilizando el ya adquirido por el IDEP
2.	Tener un control para el acceso al centro de cableado del piso 8°, en la visita del auditor se evidencio que no se mantiene cerrado bajo llave, las llaves de los closets no deben permanecer en las chapas, se recomiendo mantenerlas con supervisión del personal responsable del centro de cómputo.
3.	Incluir un diagrama de distribución de puntos en los closets de cableado para facilitar la rápida referenciación de puntos al personal de soporte en caso de contingencia

2.4 Desarrollo y Adquisición de Software Aplicativo

2.4.1 Recomendaciones

N°.	OBSERVACIÓN
4.	Como parte de la metodología de gestión de programas y proyectos TIC en atención al dominio de Gobierno Digital, elaborar, formalizar y poner en operación un procedimiento de control de cambios que permita llevar trazabilidad y control sobre los cambios impactados por los proveedores. Incluir formatos de documentación de cambios y medias de seguridad para mitigar las fallas en uso productivo por cambios no gestionados.
5.	Adelantar un plan de pruebas conjunta entre sistemas, las áreas de negocio y los proveedores de la interfaz de Humano a Goobi usando técnicas de puntos de control de calidad de la data en el proceso para identificar el momento en que se genera la falla y gestionar lo que corresponda para su corrección a la luz de los contratos vigentes.

2.5 Administración de Recursos de TI

2.5.1.1 Recomendaciones

N°.	OBSERVACIÓN
1.	Implementar una herramienta gratuita y de código abierto que permita hacer escaneo de hardware y software con el fin de mantener el control de los inventarios de manera centralizada y automatizada. Esta alternativa disminuye carga operativa de mantener el control manual, facilita el chequeo de instalaciones ilegales de los equipos de red y permite llevar control de los usuarios responsables de los equipos para verificar autenticaciones de usuario en equipos que no le han sido asignados.

N°.	OBSERVACIÓN
	De ser implementada la herramienta mantener la trazabilidad de las placas de activos fijos
2.	Como parte de la implementación del dominio 13 Gestión de comunicaciones, adelantar un formato de HV de servidores.
3.	Optimizar el procedimiento administrativo y la comunicación entre las áreas de servicios generales y sistemas para disminuir las inconsistencias entre registros. Incorporar en los registros de procesos y procedimientos de la OAP un acta de alta de activos de información que incluya equipos, software y accesos. Esta acta deberá suscribirse por el usuario una vez recibidos los activos y modificadas las claves de acceso a los sistemas y servicios. Esta acta es base para el control de devolución de activos de información al cese de la relación contractual de que habla el control ISO 27002:2013 9.2.6 Eliminación o ajuste de los derechos de acceso. Se sugiere usar un esquema similar al ejemplo presentado en el numeral 3.1.2
4.	Incluir en el Plan de adquisiciones el escalamiento a las versiones de productos Microsoft que pierden soporte del fabricante.

2.5.2 Help Desk

2.5.2.1 Recomendaciones

N°.	OBSERVACIÓN
1.	Se debe configurar el sistema de tickets para que únicamente los usuarios registrados pueden crear solicitudes y así evitar posibles incidentes de seguridad o pérdida de tiempo de los agentes de soporte.
2.	Centralizar y clasificar todos los soportes relacionados con los sistemas y plataforma tecnológica del IDEP, incluyendo los sistemas de información y configurar el direccionamiento de estos soportes a los proveedores de los mismos, con el objeto de poder generar indicadores de todos los servicios y soportes del área y sus proveedores, incluyendo el cumplimiento de ANS.
3.	Se recomienda revisar los siguientes criterios para la configuración de la herramienta de tickets y o la implementación de una nueva herramienta gratuita y de código abierto como el GLPI: • Que permita configurar diferentes tipos de solicitudes hasta mínimo dos niveles jerárquicos: incidentes soporte, requerimientos de desarrollo, incidentes de seguridad, requisitos de adquisiciones de software o hardware, propuestas, etc. • Que permita configurar diferentes agentes de atención externos e internos clasificados por Agentes internos TIC, Agentes internos de negocio, agentes externos proveedores • Que permita establecer ANS de acuerdo con la tipología de solicitudes y de agentes • Que permita una relación jerárquica entre solicitudes para aquellos casos en que una solicitud se segrega en varias tareas y de su cumplimiento dependa el estado de atención de la solicitud original • Que permita instalar un agente en los PC para que todas las solicitudes sean gestionadas por este medio con el fin de eliminar la carga operativa de la digitación de llamadas y correos y el riesgo de error humano. Adicionalmente la centralización de la información optimiza los tiempos de atención y la obtención de información estadística • Que permita generar reportes e indicadores de gestión

N°.	OBSERVACIÓN
	• Que permita instalar agente de escaneo de red para llevar la trazabilidad entre solicitud, usuario y equipo • Que permita adjuntar archivos tanto a la solicitud principal como a las tareas de la bitácora de atención • Que permita aplicar escalamientos. • Que integre un inventario de hardware y software por medio de agente.

2.5.3 Procedimientos e Instructivos de Operación

2.5.3.1 Recomendaciones

N°.	OBSERVACIÓN
1.	En el marco de atención del MSPI, al elaborar la declaración de aplicabilidad, definir el inventario de documentos que deben ser elaborados para atender los controles de la norma que sean aplicables. A continuación, se adjunta una relación resumen de los controles ISO 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.
10.1 Controles criptográficos.

10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).

18.1.3 Protección de los registros de la organización. 18.1.4 Protección de datos y privacidad de la información personal.	18.1.5 Regulación de los controles criptográficos. 18.2 Revisiones de la seguridad de la información.	18.2.1 Revisión independiente de la seguridad de la información. 18.2.2 Cumplimiento de las políticas y normas de seguridad. 18.2.3 Comprobación del cumplimiento.

3 RECOMENDACIONES Y/O ASPECTOS A MEJORAR

Las recomendaciones emitidas por el auditor se presentan en cada ítem del capítulo 3 de este documento

4 FORTALEZAS:

Una vez ejecutada la auditoría se identifican las siguientes fortalezas:

- La Oficina Asesora de Planeación quien es la responsable del proceso de Tecnologías de la Información y las Comunicaciones ha estructurado y presentado para la vigencia 2019 el Plan Estratégico de Tecnologías de la Información actualizado a enero de 2019 (*PL-GT-12-01_PETIC_V9.pdf*), el cual refleja el interés de la OAP por dar cumplimiento a los lineamientos el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado colombiano y constituye un documento de base que puede ser fortalecido para que se establezca como guía estratégica para el mantenimiento y mejoramiento de la función tecnológica alineada a los objetivos estratégicos institucionales y garantizando la seguridad de la información del instituto.
- La Oficina Asesora de Planeación pese al reducido grupo de funcionarios a cargo de la gestión TIC ha estructurado y presentado algunos instrumentos en aras de llevar control de la gestión, buscar mejorar los servicios tecnológicos y avanzar en la implementación de MIPG.
- Las adquisiciones de herramientas tecnológicas de: Sistema Operativo de Red, Firewall, Antivirus y solución de hiperconvergencia corresponden a productos de calidad, con la capacidad de ser configurados para satisfacer las necesidades de seguridad del IDEP
- Dado que la OAP tiene a su cargo la sostenibilidad y consolidación del sistema integrado de gestión, ya se cuenta con elementos de base para incorporar el Sistema de Gestión de Seguridad de la información en el marco de la implementación del MSPI.
- Se han implementado algunos elementos de protección que si bien deben ser mejorados ofrecen un nivel aceptable de protección de primera capa sobre los activos de información especialmente contra ataques de seguridad externos.
- Los usuarios de los servicios TIC tienen una percepción positiva sobre el servicio prestado por la OAP

5 CONCLUSIONES DE AUDITORÍA:

Si bien los resultados de la auditoría arrojan varias oportunidades de mejora especialmente en el ámbito de seguridad de la información, es evidente que la oficina asesora de planeación está comprometida con el mejoramiento continuo de la gestión a su cargo y con el cumplimiento del IDEP en cuanto a las regulaciones y normas relacionadas con el fortalecimiento de la gestión TIC en el estado colombiano

Es de anotar que pese al equipo humano reducido con que cuenta la OAP se evidencia su compromiso con la entidad.

(Original Firmado por)

HILDA YAMILE MORALES LAVERDE
Jefe Oficina de Control Interno

	Nombre/Cargo	**Firma**
Aprobó	Hilda Yamile Morales Laverde – Jefe Oficina de Control Interno	
Revisó	Hilda Yamile Morales Laverde – Jefe Oficina de Control Interno. Yadira Velosa Poveda – Contrato No. 26 de 2019	
Elaboró	Yadira Velosa Poveda – Contrato No. 26 de 2019	
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales y/o técnicas vigentes.		