Id	No	Dominio	FECHA DE INICIO PROGRAMADA	FECHA DE TERMINACION PROGRAMADA	DESCRIPCIÓN DEL HALLAZGO	ACCION (ES) DE MEJORAMIENTO	EVIDENCIA	RESPONSABLE	SEGUIMIENTO_AUDITORIA	EVIDENCIA_PRESENTADAS	ESTADO	CODIGO CALOR
1	20	Planeación y Organización de la Gestión TIC - Gestión Estratégica de TI	1/07/2022	30/11/2022	Actualizar el PETI 2019 de tal manera que el desarrollo de las fases y dominios del MRAE refleje el estado actual de la entidad en materia de servicios, Gobierno y plataforma TIC. Atender las recomendaciones que sobre el diagrama de red se emiten en el numeral 2.2 del presente informe. De igual manera incluir los avances del área en el dominio de uso y apropiación. De acuerdo a los lineamientos emitidos por Mintic el resultado final del PETI debe ser la identificación de proyectos y la estructuración de instrumentos que permitan su planeación detallada y control de cumplimiento en términos de costos, alcance y calidad. Así las cosas, se recomienda revisar el PETI 2019 para garantizar que existe una correlación entre los objetivos estratégicos de la entidad, la atención de resultados DOFA y la atención de requerimientos normativos y los proyectos TIC identificados, los cuales a su vez deben verse reflejados en los planes de acción y los planes operativos de seguimiento táctico OBSERVACIÓN 2021: - Instaurar el Grupo para la construcción del PETI, y el comité técnico involucrando como mínimo a las siguientes áreas o procesos que deben ser convocados por demanda: • OAP: para articular el Plan con los demás Planes de la Entidad y con los objetivos estratégicos de la Planeación Estratégica a construir para el siguiente cuatrienio 2022-2025. • Sistemas de Gestión: para articular las políticas, procedimientos, formatos e instructivos que se construyan en el marco del MRAE y del MSPI, con el sistema integrado de gestión atendiendo los cruces entre las normas ISO. • Áreas Misionales: Definir las oportunidades de mejora y requisitos de solución • Atención al Ciudadano: Identificar los requisitos de ciudadanos y entidades correlacionadas. • Control Interno: hacer seguimiento al tratamiento y articulación de los riesgos TIC a los de la entidad, hacer seguimiento a las acciones de las cláusulas 9. Evaluación y Desempeño y 10 Mejora del MSPI. • Gestión del conocimiento: para articular los dominios de información, uso y apropiación del MRAE	1. Instaurar un grupo para la construcción de PETI involucrando la oficina asesora de planeación, los sistemas de gestión, áreas misionales, servicio al ciudadano y control interno 2. Actualización plan estratégico de tecnológicas con fechas de meta de la hoja de ruta de proyectos 3. Incluir en el dominio de servicios tecnológicos del PETI lineamientos y estándares de arquitectura de la infraestructura tecnológica y análisis de capacidad, procesos de operación monitoreo y supervisión de servicios,	Plan estratégico de tecnologías PETI	Emerson Cruz	FECHA DE TERMINACION 30/11/2022 En cuanto al PETI se ha avanzado en las mesas de trabajo con las diferentes áreas y se han adoptado las nuevas directrices de la G.ES.06 Guía versión 2 de MinTic para la construcción del PETI 2023-2026. Como insumo del PETI se trabajó con las dependencias en las necesidades básicas de Tecnología a través del diligenciamiento del formato "Necesidades tecnológicas para el 2023". A la auditoría le fue entregado el documento "Anexo_1.Herramienta_para_la_construccion_del_PETI.xls", donde se relacionan las sesiones a desarrollar por cada fase y los avances de algunas sesiones. Así las cosas, en la sesión 1, se determinó el grupo interdisciplinario para la construcción del PETI, desde el Comité Directivo se estableció el punto focal de cada una de las áreas para apoyar la elaboración del documento, el proceso auditado aportó el correo electrónico donde se notificaron los responsables por cada área, sin embargo, en el instrumento guía de estructuración del PETI no se han diligenciado los responsables. En la sesión 3, se realizó una caracterización de los servicios ofrecidos a los ciudadanos y se realizó el análisis DOFA por dependencias, como evidencia se aportaron los archivos JAM_PETI_DOFA_2022, JAM_PETI_DOFA_2022_OAJ_TH y JAM_PETI_DOFA_2022_SGE_SPD. El proceso auditado informó que el nuevo plan estratégico institucional se articulará con el PETI 2023-2026, y en este mismo proceso se definirán los proyectos estratégicos a desarrollar en la próxima vigencia, estableciendo los recursos y adquisiciones requeridas para su implementación. Se han realizado varias de las acciones recomendadas, pero aún faltan algunas para concretar el resultado final que es la creación del PETI 2023-2026, en el cual se deben reflejar y verificar la totalidad de las recomendaciones, por lo tanto, el hallazgo continua abierto.	Anexo_1.Herramienta_para_la_construccion_del_PETI.xls Archivos: JAM_PETI_DOFA_2022, JAM_PETI_DOFA_2022_OAJ_TH y JAM_PETI_DOFA_2022_SGE_SPD Correo con los puntos focales del grupo del interdisciplinario	ABIERTO	EN PROCESO
2	21	Planeación y Organización de la Gestión TIC - Gestión Estratégica de TI	1/07/2022	30/11/2022	Con relación a los Planes operativos para control acciones y/o proyectos se recomienda: • 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, establecer fechas viables de cumplimiento y ponderar las actividades de acuerdo con el esfuerzo requerido y no a la importancia para el negocio, ya que este último criterio es determinante para priorizar, pero no para gestionar avance . • Antes del cálculo de capacidad disponible deben sustraerse los tiempos requeridos por cada recurso para la atención de funciones de rutina. • Incluir actividades No rutinarias que requieren acompañamiento de recursos del área • 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 (DOFA) o Prioridad 4: atender innovación TIC o Prioridad 5: de valor agregado para los procesos de apoyo • Establecer criterios de aceptación de los entregables para garantizar que el resultado obtenido realmente cumple con la mejor práctica y lo incluido en los documentos se ve reflejado en la implementación sobre procesos y plataforma tecnológica • Calcular los avances de acuerdo al nivel de cumplimiento de los entregables con los criterios establecidos. Si es posible hacer revisión de pares.	Incluir en el PETI la hoja de ruta de los proyectos relacionando los objetivos estratégicos institucionales, análisis DOFA y proyectos identificados	Plan estratégico de tecnologías PETI	Emerson Cruz	FECHA DE TERMINACION 30/11/2022 El proceso auditado aportó el docuemento PETI 2023-2026, incluyendo la hoja de ruta de los proyectos relacionados con los objetivos estratégicos institucionales, además de aportar el análisis DOFA y proyectos identificados cumpliendo con la acción de mejora propuesta, sin embargo, la acción planteada no cubre con todos las recomendaciones emitidas en la descripción del hallazgo, por lo tanto, se recomienda incluir las acciones faltantes en el nuevo plan de mejoramiento.	PETI 2023-2026	ABIERTO	EN PROCESO
3	22	Planeación y Organización de la Gestión TIC - Gestión Estratégica de TI	1/07/2022	30/11/2022	Continuar con los análisis de la situación actual incorporados en el PETI y en el "INFORME FINAL DE EJECUCIÓN -Componente Estratégico de Tecnología y Gobierno Digital - Agosto 2015 – septiembre 2018", optimizándolo con un análisis tipo DOFA que permita identificar proyectos de fortalecimiento de la gestión y plataforma TIC además del aprovechamiento de las oportunidades del entorno OBSERVACIÓN 2021: Adelantar el DOFA en la estructuración del PETI e identificar proyectos de trasformación digital, establecimiento los recursos y adquisiciones requeridas para su implementación.	Incluir en el PETI análisis DOFA y proyectos de transformación digital en adquisiciones requeridas para su implementación	Plan estratégico de tecnologías PETI	Emerson Cruz	FECHA DE TERMINACION 30/11/2022 El proceso auditado aportó los documentos JAM_PETI_DOFA_2022, JAM_PETI_DOFA_2022_OAJ_TH y JAM_PETI_DOFA_2022_SGE_SPD, donde se evidencian las matrices DOFA realizadas con las diferentes dependencias de la entidad. En el documento PETI 2023-2026 se identificaron proyectos relacionados con los objetivos estratégicos institucionales, sin embargo, se evidencia que las adquisiciones fueron catalogadas como proyectos. Se recomienda revisar nuevamente el listado de proyectos y las adquisiciones incluirlas como parte de los recursos necesarios para su implementación. Todo proyecto debe contar con un responsable, recursos, cronogramas de actividades, cumplimiento, entre otros. Aunque se cumple con la elaboración del documento, la acción planteada no cubre con todos las recomendaciones emitidas en la descripción del hallazgo, por lo tanto, se recomienda reformular la acción de mejora, de tal forma que permita tener un control de la ejecución del PETI.	Archivos: JAM_PETI_DOFA_2022, JAM_PETI_DOFA_2022_OAJ_TH y JAM_PETI_DOFA_2022_SGE_SPD PETI 2023-2026	ABIERTO	EN PROCESO
4	23	Planeación y Organización de la Gestión TIC - Gestión Estratégica de TI	1/04/2022	31/12/2022	Incorporar en el PETI indicadores asociados a la medición de cumplimiento, productividad y calidad en los servicios TIC y proyectos, seleccionando aquellos que sean pertinentes de acuerdo con los lineamientos del Marco de Referencia de Arquitectura Empresarial de TI, específicamente en el dominio Gobierno de TI: • Indicador de beneficio del servicio. • Indicador de ANS de incidentes bajo responsabilidad de terceros. • 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. • Cumplimiento de terceros. • Desviación en capacidad de los servicios. • Dificultades por capacidad en proyectos de TI. • Calidad en los entregables. • 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. • Implementación Modelo de Gestión Estratégica Para los indicadores del MSPI deben diseñarse indicadores que midan la implementación de los controles no cumplimiento de actividades. Por ejemplo: disponibilidad de los servicios, indicadores sobre alertas del Firewall, incumplimientos en instalaciones no autorizadas con base en escaneos de equipos de red, etc. Para el caso de desarrollo de software interno o contratado con terceros utilizar dicionalmente el	1. Reportar en el plan operativo, plan de acción e indicadores el cumplimiento del proceso TI	1. Hoja de vida de indicadores, aplicativo plan de acción, plan operativo	Emerson Cruz - Giselle Muñetón	Como evidencia a la Auditoría se presentaron los documentos HV Indicadores Estratégicos 2022_AUD.xls, seguimiento plan de acción.xls e indicador PETI 2022.xls, donde se puede apreciar que se tienen definidos dos indicadores, uno para medir el nivel de cumplimiento del plan de acción, el cual se mide trimestralmente y se tiene en cuenta el avance ponderado de los productos del plan de acción, sobre el avance proyectado de cumplimiento de los productos plan de acción (acumulado), según los resultados cuantitativos y cualitativos se evidencia su cumplimiento por encima de lo esperado para los tres trimestres. El otro indicador estratégico es el nivel de cumplimiento en el avance de los proyectos del PETI, también se mide trimestral y para su cálculo se tiene en cuenta el porcentaje de avance de los proyectos en el periodo sobre 100, este avance se calcula con base en la hoja de ruta de los proyectos establecidos en el PETI, donde a cada proyecto se le asigna un peso porcentual. Según los resultados cuantitativos para los tres trimestres el nivel de cumplimiento ha superado la meta del período y también se hace una descripción cualitativa sobre el avance. Respecto a este indicador se hacen las siguientes observaciones: El documento indicador PETI 2022.xls solo contiene la relación de los proyectos que en su mayoría son adquisiciones y un porcentaje de avance, a criterio de los responsables, porque no se cuenta con cronogramas detallados con desglose de las actividades que permitan llevar un control de las tareas y avances individuales. También le fue entregado a la auditoría el archivo Hv Indicadores Gestión Tic 2022.xls que corresponde a los indicadores definidos para el proceso Gestión de las TICs, donde se tiene definido un indicador de cumplimiento para el plan operativo, el cual se calcula con base en las actividades ejecutadas en el período contra las proyectadas en el período, según los resultados durante los tres trimestres el proceso Gestión de las TICS ha cumplido con todas las actividades proyectadas, el otro indicador mide el nivel de oportunidad en la atención de los servicios tecnológicos, donde se tiene en cuenta el total de las solicitudes atendidas sobre el total de solicitudes generadas, según los	HV Indicadores Estratégicos 2022 - Hv Indicadores Gestión Tic 2022 HV MSPI 2022 - Plan Operativo - Política de Gestión TIC Seguimiento Plan Acción 2022 Trimestre III Pantallazos aplicativo avance plan operativo	ABIERTO	EN PROCESO

5	24	Planeación y Organización de la Gestión TIC - Gestión Estratégica de TI	1/03/2022	31/12/2022	Incluir en los planes de mejoramiento el resultado de los indicadores optimizados y el resultado del seguimiento a riesgos TIC, incluir los tiempos requeridos para la atención de estas acciones en el proceso de cálculo de esfuerzo para asignación de tareas. OBSERVACIÓN 2021: Orientar la fase "Revisión y/o actualización de los indicadores de Gestión TIC atendiendo las recomendaciones emitidas en las auditorías anteriores (2019, 2020). Diseñar los indicadores para contar con herramientas para tratamiento de riesgos y facilitar la toma de acciones correctivas, usando en lo posible fuentes automáticas, para no generar carga operativa adicional.	1. Plantear y ajustar los indicadores de Gestión TIC	1. Hoja de vida de indicadores, acta de reunión ajuste indicadores	Emerson Cruz - Giselle Muñetón	El proceso auditado presentó a la auditoría el acta de la mesa de trabajo que se llevó a cabo el 14 de marzo de 2022 con planeación y control interno para establecer los indicadores de gestión del proceso de TIC para la vigencia 2022. Se dejaron los mismos indicadores de Gestión, se realizó un ajuste en los valores para la línea base y meta final de todos y se formularon nuevos indicadores relacionados al MSPI. Se cumplió con la acción de mejora propuesta pero aún no se ha cubierto todas las recomendaciones de la auditoría. Por lo tanto, el hallazgo continúa abierto.	Hv Indicadores Gestión Tic 2022 HV MSPI 2022 Acta reunión indicadores TIC	ABIERTO	EN PROCESO
6	25 .1	Planeación y Organización de la Gestión TIC - Estructura Organizacional y Gobierno de TI	1/03/2022	30/11/2022	• Adelantar una identificación de los conocimientos específicos que deben ser trasferidos y que documentos de procedimientos e instructivos deben incorporarse a la transferencia y el cargo de contingencia. • Formalizar un Plan de Transferencia de Conocimiento hacia el INSOR, 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 al conocimiento a trasferir o Capacitación incluyendo incidentes y recuperaciones para el colaborador 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 el personal con conocimientos específicos es objeto de tratamiento de riesgos por ausencia temporal o permanente. OBSERVACIÓN 2021: - Alinear la Matriz de catálogo de sistemas de información al documento de ARQUITECTURA DE SOLUCIÓN DE LOS SISTEMAS DE INFORMACIÓN DEL INSOR. Establecer formalmente en los contratos de personas naturales a cargo de desarrollos y/o mantenimientos de sistemas de información que actualicen este documento cada vez que se realicen cambios. - Continuar con el proceso de generación del plan de continuidad de la entidad, tomando como	1. Actualizar la matriz de catálogo de Sistemas de Información con los datos del contrato vigente con terceros (proveedores o contratistas).	1. Matriz catálogo de sistemas de información	Web master	FECHA DE TERMINACION 30/11/2022 El proceso auditado aportó el documento "Matriz Catalogo de Sistemas de Información 2022", aprobado el 10/10/2022, donde están relacionados todos los aplicativos que actualmente están en uso en la entidad, en esta matriz se indican los responsables a nivel técnico y funcional, tipo de licenciamiento, sistema operativo, lenguaje de programación, plataforma de bases de datos, documentación técnica y funcional con acceso a su consulta a través de link, arquitectura tecnológica y observaciones si aplica y también aportó los documentos "Dominio de los Sistemas de Información del Insor", aprobado y publicado en el SGC el día 12/10/2022, donde se presenta en más detalle técnico lo que contiene la matriz, detallando la interacción que se presenta al interior de la entidad entre las distintas áreas y los sistemas de información, para dar cumplimiento a los objetivos trazados en el INSOR y el documento "ARQUITECTURA DE SOLUCIÓN DE LOS SISTEMAS DE INFORMACIÓN DEL INSOR" el cual está alineado con la matriz catálogo de sistemas de información. La responsabilidad de la actualización del documento "Matriz Catalogo de Sistemas de Información 2022" quedó a cargo del equipo de Tecnología, si surge algún cambio en los sistemas de información los responsables del desarrollo o mantenimiento lo deben informar oportunamente. Se atendió la recomendación y la evidencias presentadas fueron pertinentes, por lo tantó el hallazgo se cierra.	Matriz Catalogo de Sistemas de Información 2022.xls ODGT09 Arquitectura de solución de los sistemas de información del INSOR	CERRADO	ATENDIDO
7	25 .2	Planeación y Organización de la Gestión TIC - Estructura Organizacional y Gobierno de TI	1/03/2022	31/12/2022	• Adelantar una identificación de los conocimientos específicos que deben ser trasferidos y que documentos de procedimientos e instructivos deben incorporarse a la transferencia y el cargo de contingencia. • Formalizar un Plan de Transferencia de Conocimiento hacia el INSOR, 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 al conocimiento a transferir o Capacitación incluyendo incidentes y recuperaciones para el colaborador 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 el personal con conocimientos específicos es objeto de tratamiento de riesgos por ausencia temporal o permanente. OBSERVACIÓN 2021: - Alinear la Matriz de catálogo de sistemas de información al documento de ARQUITECTURA DE SOLUCIÓN DE LOS SISTEMAS DE INFORMACIÓN DEL INSOR. Establecer formalmente en los contratos de personas naturales a cargo de desarrollos y/o mantenimientos de sistemas de información que actualicen este documento cada vez que se realicen cambios.	2. Desarrollar plan de continuidad de la entidad tomando referencia las guías de MINTIC y plantillas entregadas por MEN	2. Plantillas y plan de continuidad	Giselle Muñetón	FECHA DE TERMINACION 31/12/2022 Con respecto al plan de continuidad se adelantaron mesas de trabajo con el Ministerio de Educación y la universidad EAFIT quienes facilitaron la documentación del MEN y plantillas como base inicial para la generación del plan de continuidad y análisis de impacto del negocio BIA. El proceso auditado avanzó en la elaboración de los documentos "MANUAL ANÁLISIS DE IMPACTO DE NEGOCIO – BIA" y en la plantilla "ANALISIS DE IMPACTO DEL NEGOCIO-BIA", falta revisión por parte de planeación para su publicación en el Sistema de Gestión de Calidad. Para la socialización y posterior diligenciamiento de la plantilla "análisis de impacto del negocio BIA" se realizará mesa de trabajo con los líderes de proceso para identificar los procesos críticos de la entidad y definir los tiempos de recuperación porque hay unos tiempos que definen las áreas y otros Tecnología, en conjunto, se deben definir los procesos alternos para la continuidad del negocio. Se recomienda incluir en la plantilla un campo para describir el proceso de retorno a la normalidad después de aplicar la contingencia. Como complemento a la documentación del plan de continuidad el proceso auditado elaboró el documento "MANUAL PARA RESPALDO Y RECUPERACIÓN DE DATOS DE LA INFRAESTRUCTURA TECNOLÓGICA", versión 1, aprobado y publicado el 25/0/2022 en el SGC y actualizó a la versión 2 la "GUIA PARA COPIAS DE SEGURIDAD", publicada y aprobada el 10/10/2022 en el SGC. En la elaboración del documento plan de continuidad no se ha avanzado aún y no se ha formalizado un plan de transferencia de conocimiento al interior de la entidad. Por lo tanto, el hallazgo continua abierto	MANUALANALISISDE IMPACTODENEGOCIO-BIA Plantilla Formato Informe BIA FOGT18 Formato DE SOLICITUD Y GESTIÓN DE CAMBIOS (RFC) GUIA PARA COPIAS DE SEGURIDAD_V2 MANUALRESPALDO Y RECUPERACIÓN DE DATOS DE LA INFRAESTRUCTURA TECNOLÓGICA Procedimiento GESTIÓN del Cambio_V2	ABIERTO	EN PROCESO
8	26	Planeación y Organización de la Gestión TIC - Estructura Organizacional y Gobierno de TI	1/05/2020	31/12/2022	De ser posible, incluir en los contratos, cláusulas que obliguen al contratista a realizar un empalme y dar capacitación de su cargo, frente a un retiro temporal o permanente o en su defecto incluir en las obligaciones especificar la documentación de instructivos	1. Determinar obligaciones dentro de los contratos de prestación de servicios para garantizar que se realice entrega de la información manejada y una sensibilización sobre las actividades realizadas, en caso de que el supervisor lo solicite. 2. Determinar obligaciones de entrega de productos de manera concreta, incluyendo aspectos cuantitativos y cualitativos, en caso de requerirse.	1. Actas de reuniones 2. Formato entrega de información manejada contratistas/funcionarios proceso TI.	Giselle Muñetón Emerson Cruz Contratación	FECHA DE TERMINACION 31/12/2022 El proceso auditado manifestó que se realizaron varias mesas de trabajo con el área de contratación para incluir en los contratos las cláusulas de sensibilización e información entregada por el contratista, sin embargo, no hubo consenso, por esta razón, desde el área de TI para los contratos donde su objeto contractual está relacionado con tecnología se diseñó y se incluyó el "ANEXO 3 – RELACIÓN DE INFORMACIÓN ENTREGADA Y SENSIBILIZACIÓN REALIZADA TIC (PROPUESTA)" en el formato "FOCT07 INFORME FINAL DE DESARROLLO DEL CONTRATO". Este anexo está pendiente de revisión y aprobación por parte de la jefe de la OAP. En la revisión de los contratos allegados por el proceso auditado, únicamente el de Carlos Andrés Molina contempla una obligación específica relacionada con elaboración y/o actualización de los formularios, tutoriales, protocolos y manuales y los contratos de Soledad Martínez y César Augusto González Jiménez tienen como obligación específica la transferencia de conocimiento. En el documento "METODOLOGÍA PARA EL DESARROLLO DE SOFTWARE DEL INSOR" en el capítulo final se menciona que en los documentos FOGT07 ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN (FUNCIONARIOS - CONTRATISTAS) y/o FOGT08 ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN (PROVEEDORES DE TECNOLOGÍA) se va a incluir como cláusula que dentro de las obligaciones de los contratos de prestación de servicios se garantice la entrega de la información manejada y una sensibilización sobre las actividades realizadas, en caso de que el supervisor lo solicite y entrega de productos de manera concreta, incluyendo aspectos cuantitativos y cualitativos, en caso de requerirse. Esta cláusula aún no se ha incluido. Se recomienda que todos los contratos de contratistas y funcionarios que tienen alto impacto en la operación contemplen cláusulas de transferencia de conocimiento y documentación de instructivos.	Citación a mesas de trabajo ANEXO 3 – RELACIÓN DE INFORMACIÓN ENTREGADA Y SENSIBILIZACIÓN REALIZADA TIC (PROPUESTA) Contratos: Carlos Molina, David Andrés Bello, Soledad Carolina Martínez, Emerson Cruz Aldana, César Augusto González Jiménez y Gerson Leonardo Barreto Flórez. -Metodología para el desarrollo de software del INSOR	CERRADO	ATENDIDO

9	27	Planeación y Organización de la Gestión TIC - Estructura Organizacional y Gobierno de TI	1/05/2020	31/12/2022	Con respecto a contratos de adquisición o SAAS de sistemas de información comerciales, se emiten las siguientes recomendaciones: • solicitar al proveedor las licencias de uso a favor del INSOR • incluir en los estudios previos la prohibición de ceder los derechos patrimoniales del sistema a terceros durante la vigencia del contrato y un tiempo adicional que deberá ser determinado de acuerdo al impacto que pueda causar para la entidad no contar con los servicios se soporte y mantenimiento del sistema Para el caso del contratista ITS, hacer alusión explicita al cumplimiento de la ficha técnica en las obligaciones específicas del contratista de los Estudios Previos y solicitar que la oferta se adecúe exactamente a lo establecido en los estudios previos en cuanto a los tiempos máximos de "solución" y no solo de "respuesta" de los ANS	1. Determinar y aplicar las condiciones dentro de los procesos de contratación de software como servicio (SAAS).	1.Actas de reuniones 2. Acuerdo de confidencialidad, documento metodología de Software.	Giselle Muñetón Emerson Cruz Equipo de Contratación	A la auditoria le fue presentado el documento "ACTUALIZACION SISTEMA ITS SEP" que corresponde al "FORMATO ESTUDIOS PREVIOS DE CONTRATACIÓN DIRECTA" con la empresa ITS SOLUCIONES ESTRATEGICAS SAS, donde en la primera obligación específica se hace alusión al cumplimiento de la ficha técnica. En los estudios previos no se hace referencia explicita a los ANS de solución de casos. El proceso auditado manifestó que realizaron varias mesas de trabajo con el área de contratación para evaluar la factibilidad de incluir los ANS en los estudios previos y en las fichas técnicas de los contratos pero como no es un requisito general que aplique a todos los contratos, entonces estos se incluirán en aquellos estudios previos que sean generados desde el área de TI. Respecto a la cesión de derechos patrimoniales a favor del INSOR , la auditoría había propuesto un formato que no se pudo implementar, según el correo atendido por el área jurídica y aportado por el proceso auditado, lo procedente es dar aplicación a lo dispuesto en el Art. 28 de la Ley 1450 de 2011, que regula los derechos patrimoniales de autor creados en virtud de un contrato de prestación de servicios, al modificar el Art. 20 de la ley 23 de 1982. Con la aclaración dada por el proceso auditado y las evidencias presentadas se cierra el hallazgo.	Citación a mesas de trabajo Metodología para el desarrollo de software del INSOR Estudios Previos ITS Compromiso Formato Cesión de derechos de autor	CERRADO	ATENDIDO
10	28 .1	Planeación y Organización de la Gestión TIC - Estructura Organizacional y Gobierno de TI	1/07/2022	30/09/2022	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, vincular a los contratistas como funcionarios para mitigar el riesgo de continuidad y fuga de conocimiento frente a los vencimientos de contrato	1. Realizar análisis del proceso de Gestión TIC	1. Plan de Trabajo Intervención proceso TIC	Jefe Oficina Asesora de Planeación y Sistemas	FECHA DE TERMINACION 30/09/2022 Si bien el proceso auditado adelantó la ficha de caracterización del proceso, aún no se ha realizado el análisis de capacidad de los recursos humanos actuales con que cuenta la OAP para cumplir con las actividades del proceso. Por lo tanto, el hallazgo continúa abierto.	No se presentó avance en ninguna de las evidencias relacionadas	ABIERTO	EN PROCESO
11	28 .2	Planeación y Organización de la Gestión TIC - Estructura Organizacional y Gobierno de TI	1/10/2022	31/12/2022	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, vincular a los contratistas como funcionarios para mitigar el riesgo de continuidad y fuga de conocimiento frente a los vencimientos de contrato	2. Estructuración y actualización de la documentación para la obtención de los productos o prestación de los servicios del proceso de TIC	2. Ficha de caracterización actualizada del proceso de Gestión TIC	Jefe Oficina Asesora de Planeación y Sistemas	FECHA DE TERMINACION 31/12/2022 El proceso auditado aportó la ficha de caracterización CARACTERIZACIÓN DEL PROCESO GESTIÓN DE LAS TIC, donde se evidencian las diferentes actividades que adelantan.	FICHACARACTERIZACION	CERRADO	ATENDIDO
14	31	Activos de Información, Mantenimiento y Mesa de ayuda	1/10/2019	31/08/2022	En el marco del proyecto de implementación de la mesa de ayuda incluir los requerimientos de desarrollo como una tipología de solicitud, registrar las historias de usuario de cada requerimiento, asignar responsable y usar la funcionalidad de documentos anexos para llevar la base documental de cada desarrollo.	1. Actualización documento ANS de la mesa de servicio GLPI 2. Parametrizar la Herramienta mesa de Servicios de acuerdo a la actualización de los ANS.	1. Parametrización de herramienta de mesa de ayuda 2. Documento actualizado ANS de la mesa de servicio GLPI	Emerson Cruz - Giselle Muñetón	Ya se encuentran correctamente parametrizadas en la herramienta de mesa de ayuda GLPI los requerimiento de desarrollo para la gestión de cambio y control de nuevos desarrollos. Sin embargo, aun no se han registrado nuevos requerimientos y por lo tanto no se puede validar su correcto funcionamiento. Se han realizado capacitaciones a los usuarios para la correcta identificación y diferenciación entre incidentes y requerimientos. Las acciones de mejoramiento presentadas para cumplir con esta recomendación fueron correctamente adelantadas por el proceso auditado, en la revisión de la parametrización se evidencia la actualización de los ANS y se encuentra habilitado el proceso de gestión de cambios para la atención y control de los requerimientos, sin embargo, aún no se cuenta con registro de actividades relacionadas con la recomendación, por lo tanto, el hallazgo se mantiene en estado abierto, se debe incluir una acción de mejora relacionada con el uso y efectividad en el plan de mejoramiento de la próxima vigencia.	Imagen parametrización requerimientos en GLPI. Imagen control de cambios en GLPI.	ABIERTO	EN PROCESO
15	32	Planeación y Organización de la Gestión TIC - Plan de Administración de Riesgos y Contingencias	1/07/2022	30/11/2022	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 Incluir en la Guía de administración de riesgo los dominios 14 y 15 OBSERVACIÓN: - Desarrollar el dominio de seguridad de la información que incluya otros: • Referencia a la relación con los activos de información y la estrategia para garantizar la disponibilidad, integridad y confidencialidad de los activos de información. • Planes de implementación, lineamientos y procedimientos del MSPI, incluyendo temas legales y normativos externos e interno concernientes a la seguridad informática. • Estrategias de capacitación con el fin de apropiar los temas de seguridad informática. • Mecanismos de seguimiento a los controles implementados. - Complementar la identificación de riesgos de seguridad y tecnológicos de manera articulada con los activos de información y los objetivos de control de MSPI, incluir la relación entre el tratamiento de riesgos y los planes de continuidad, tenga en cuenta la correlación entre activos, riesgos y planes	1. Incluir en el PETI el dominio de seguridad de la información incluyendo activos de información, planes y procedimientos del MSPI, estrategia de capacitación y mecanismo de seguimiento a controles 2. Articular la identificación de riesgos de seguridad y tecnológicos con los activos de información relacionando el tratamiento de riesgos y planes de continuidad	1. Plan estratégico de tecnologías PETI 2. Matriz de activos de información de la entidad	Emerson Cruz	FECHA DE TERMINACIÓN 30 DE OCTUBRE DE 2022 El proceso auditado aportó a la auditoría el documento "GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO", versión 6, aprobada y publicada en el SGC el día 31/03/2022, donde se establecen los lineamientos para la identificación, análisis, valoración de riesgos, determinación de roles y responsabilidades, así como el establecimiento de planes de tratamiento dirigidos a fortalecer el enfoque preventivo para facilitar el tratamiento de los riesgos o minimizar su impacto en caso de materialización u ocurrencia de eventos que puedan afectar negativamente el logro de los objetivos institucionales en el marco de los procesos, proyectos y planes de la entidad. Atendiendo las recomendaciones de la auditoría se evidencia que se incluyó la Identificación de Controles del Modelo de Seguridad y Privacidad de la Información MSPI para los dominios 14 y 15. El INSOR avanzó en la actualización del "FORMATO REGISTRO ACTIVOS DE INFORMACIÓN", donde se incluyeron los demás activos establecidos en el Manual de Seguridad de la información de la entidad y en los lineamientos ISO 27001. En el mes de octubre se avanzó en la verificación de la criticidad de los activos de información, pero aún no se tiene la versión final para su aprobación, por esta razón está pendiente la matriz de riesgos relacionados con la seguridad de la información, ya que éstos y sus controles deben asociados a los activos de información y por lo tanto, articulados con el plan de continuidad y el plan de tratamiento de riesgos. A la auditoría se le presentó el documento "PETI-2019-2022", el cual se ajustó atendiendo las recomendaciones de la Auditoría en el tema de indicadores. Debido a que aun no se cuenta con una versión final aprobada de los activos de información y su relacionamiento con los planes el estado de este hallazgo continúa abierto.	PETI 219-2022 FORMATO REGISTRO ACTIVOS DE INFORMACIÓN GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO	ABIERTO	EN PROCESO
17	33 .1	Planeación y Organización de la Gestión TIC - Plan de Administración de Riesgos y Contingencias	1/01/2020	31/07/2021	Se recomienda adelantar el ejercicio de identificación de riesgos de seguridad de la información orientado a activos críticos que en caso de materialización de amenazas afectan la continuidad de la operación y/o la disponibilidad, integridad y resguardo de la información. Tener en cuenta que los riesgos deben contemplar también los diferentes aspectos de la gestión TIC para garantizar que los controles de la norma han sido incorporados en los riesgos. Tal es el caso de los riesgos relacionados con la relación con terceros que no necesariamente se originan en activos tecnológicos, sino en debilidades contractuales o de control.	1. Categorizar por criticidad los activos de información de la entidad.	1. Matriz de activos de información de la entidad	Giselle Muñetón	FECHA DE TERMINACION 31 DE JULIO DE 2022 En el mes de octubre se avanzó en la verificación y categorización de la criticidad de los activos de información, pero aún no se tiene la versión final para su aprobación, por esta razón está pendiente la matriz de riesgos relacionados con la seguridad de la información, ya que éstos y sus controles deben asociados a los activos de información y por lo tanto, articulados con el plan de continuidad y el plan de tratamiento de riesgos. La recomendación y evidencia aun no han sido atendidas en su totalidad y por lo tanto el estado de este hallazgo continúa abierto.	FORMATO REGISTRO ACTIVOS DE INFORMACIÓN GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO SEGUIMIENTO GESTIÓN DE RIESGOS 2022	ABIERTO	EN PROCESO

19	33 .3	Planeación y Organización de la Gestión TIC - Plan de Administración de Riesgos y Contingencias	1/10/2019	31/07/2022	Se recomienda adelantar el ejercicio de identificación de riesgos de seguridad de la información orientado a activos críticos que en caso de materialización de amenazas afectan la continuidad de la operación y/o la disponibilidad, integridad y resguardo de la información. Tener en cuenta que los riesgos deben contemplar también los diferentes aspectos de la gestión TIC para garantizar que los controles de la norma han sido incorporados en los riesgos. Tal es el caso de los riesgos relacionados con la relación con terceros que no necesariamente se originan en activos tecnológicos, sino en debilidades contractuales o de control.	3. Aplicación de tratamiento de riesgos de seguridad de la información	3. Matriz de riesgos del proceso TIC	Giselle Muñetón	Se entregó el documento "SEGUIMIENTO GESTIÓN DE RIESGOS 2022.xls", donde están relacionados los riesgos identificados desde el proceso de medición y mejora del INSOR con su respectivo seguimiento cuatrimestral. Se evidencia que se tienen identificados 2 clases de riesgo, de corrupción y de Gestión, los cuales están discriminados por proceso, sin embargo, estos riesgos no dan cubrimiento a la totalidad de los riesgos tecnológicos de manera alineada con la implementación MSPI y lo establecido en la "Guía para la Administración del riesgo_V6", que en ambos casos establecen la relación entre los riegos, los activos de información y los controles de la norma ISO 27002:2013. En cuanto al riesgo de corrupción "Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros por modificar, filtrar, extraer y divulgar información considerada reservada y clasificada contenida en los diferentes sistemas de la Entidad", los controles definidos como contar con los mecanismos de backup para recuperar en caso de daño o perdida de la información y la actualización del procedimiento de Gestión de usuarios y contraseñas son efectivos, sin embargo, se deben considerar otras fuentes de fuga de información como acceso a correos personales y almacenamientos en nube personales. Vale aclarar que este tipo de riesgo es de responsabilidad compartida con los responsables de los colaboradores de las áreas ya sea en calidad de jefe o de supervisor. En cuanto al riesgo de Gestión "Posibilidad de afectación reputacional por pérdida de disponibilidad, integridad y confidencialidad de la información institucional debido a falla en la infraestructura tecnológica, desconocimiento en la aplicación de la política de seguridad y privacidad de la información, deficiencias en la infraestructura tecnológica para respaldo de Información e intrusión o Ataques informáticos." Se emiten las siguientes observaciones: Se incluye un único riesgo de gestión que pretende incluir todos los elementos en una sola descriptiva, sin discriminación de los activos críticos relacionados con el riesgo, lo cual dificulta el establecimiento de controles de manera independiente. Existen 4 causas asociadas al riesgo, pero los controles establecidos solo se relacionan con la	SEGUIMIENTO GESTIÓN DE RIESGOS 2022	ABIERTO	EN PROCESO
20	33 .4	Planeación y Organización de la Gestión TIC - Plan de Administración de Riesgos y Contingencias	1/04/2021	31/12/2023	Se recomienda adelantar el ejercicio de identificación de riesgos de seguridad de la información orientado a activos críticos que en caso de materialización de amenazas afectan la continuidad de la operación y/o la disponibilidad, integridad y resguardo de la información. Tener en cuenta que los riesgos deben contemplar también los diferentes aspectos de la gestión TIC para garantizar que los controles de la norma han sido incorporados en los riesgos. Tal es el caso de los riesgos relacionados con la relación con terceros que no necesariamente se originan en activos tecnológicos, sino en debilidades contractuales o de control.	4.Revisión de activos críticos para el análisis de herramientas de criptografía	4. Evidencia del análisis de herramientas de criptografía	Giselle Muñetón	En cuanto a la acción "Revisión de activos críticos para el análisis de herramientas de criptografía", el proceso auditado informó que están revisando estudios de mercado para hacer un ponderado de los costos y se hace la siguiente observación: La criptografía es una herramienta de mitigación o para evitar que se materialice un riesgo relacionado con la confidencialidad, autenticidad y/o integridad de la información crítica, se pueden usar herramientas que no impliquen un alto costo y articularse con el dominio A10 del MSPI. Lo primero que se debe hacer es identificar los activos críticos que salgan de la entidad y que contengan información sensible que amerite controles criptográficos e implementarlos usando las herramientas de criptografía que incluyen Windows y office 365. En la matriz de activos de información ya se tienen identificados los activos que ameritan controles criptográficos, sin embargo, no se han establecido los controles y tampoco se presenta evidencia. Por lo tanto, el hallazgo continúa abierto.	NINGUNA	ABIERTO	EN PROCESO
21	34	Planeación y Organización de la Gestión TIC - Plan de Administración de Riesgos y Contingencias	1/08/2020	31/12/2022	Construir el Plan de Continuidad para que coincida en lo relacionado con Guía de administración de riesgo, 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. Una vez adelantado el Plan de Continuidad, ejecutar las pruebas integrales al Plan 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 OBSERVACIÓN 2021: Adelantar el Análisis de Impacto al Negocio BIA para establecer los tiempos, los protocolos de contingencia y recuperación y las estrategias de fidelidad de la data entre ambientes.	1. Diseñar, crear e implementar Plan de Continuidad del Negocio 2. Realizar el análisis de Impacto al negocio BIA articulándolo con el plan de continuidad del negocio	1. Plan de continuidad del negocio implementado 2. Análisis de impacto al negocio BIA	Emerson Cruz - Giselle Muñetón	FECHA DE TERMINACIÓN 31/13/2022 El plan de continuidad no ha iniciado su implementación. Como avance se han generado los siguientes procedimientos, formatos y guías que son insumo parcial para la planificación y desarrollo del mismo: Matriz Catalogo de Sistemas de Información 2022, MANUAL ANÁLISIS DE IMPACTO DE NEGOCIO – BIA, plantilla "ANALISIS DE IMPACTO DEL NEGOCIO-BIA", MANUAL PARA RESPALDO Y RECUPERACIÓN DE DATOS DE LA INFRAESTRUCTURA TECNOLÓGICA, GUIA PARA COPIAS DE SEGURIDAD, PROCEDIMIENTO GESTIÓN DEL CAMBIO, FOGT18 FORMATO DE SOLICITUD Y GESTIÓN DE CAMBIOS (RFC), GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO, SEGUIMIENTO GESTIÓN DE RIESGOS 2022.xls y formato "REALIZACION Y RESTAURACION DE COPIAS DE SEGURIDAD. Si bien se han realizado avances en esta recomendación, aun no se ha atendido en su totalidad y por lo tanto el hallazgo continúa abierto.	Matriz Catalogo de Sistemas de Información 2022 MANUAL ANÁLISIS DE IMPACTO DE NEGOCIO – BIA plantilla "ANALISIS DE IMPACTO DEL NEGOCIO-BIA" MANUAL PARA RESPALDO Y RECUPERACIÓN DE DATOS DE LA INFRAESTRUCTURA TECNOLÓGICA GUIA PARA COPIAS DE SEGURIDAD PROCEDIMIENTO GESTIÓN DEL CAMBIO FOGT18 FORMATO DE SOLICITUD Y GESTIÓN DE CAMBIOS (RFC) GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO SEGUIMIENTO GESTIÓN DE RIESGOS 2022.xls	ABIERTO	EN PROCESO
23	35	Planeación y Organización de la Gestión TIC - Plan de Administración de Riesgos y Contingencias	15/01/2022	31/12/2022	Establecer como política de seguridad del MSPI dominio 15 la inclusión de criterios de aceptación, políticas de gestión de cambios y requisitos de seguridad de manera alineada con lo establecido en el Plan de continuidad en los contratos con terceros. Establecer instrumentos de seguimiento y control a las obligaciones de los contratos y en especial a las relacionadas con seguridad de la información. Estas políticas y procedimientos deben incluir el control de proveedores TIC centralizado en la OAP, no en las áreas. OBSERVACIÓN 2021: En el marco del desarrollo del dominio 15 de MSPI, establecer para los contratos con personas naturales con obligaciones relacionadas con desarrollo de software: • Condiciones generales de transferencia de conocimiento, • Propiedad sobre los desarrollos, • Seguridad en desarrollo de software • Cumplimiento explicito con los formatos y metodología establecidos por la entidad con respecto al desarrollo de software • Condiciones de acuerdo de niveles de servicio de soporte (cuando aplique) - En el marco del dominio 15 de GLPI, hacer extensiva por contrato la aplicación de los instrumentos de la metodología de ciclo de desarrollo de software a todos los proveedores o contratistas cuyas	1. Establecer en los contratos de personas naturales con obligaciones relacionadas a desarrollo de software los criterios de propiedad sobre los desarrollos, seguridad, formatos en metodología de software y acuerdos de niveles 2. Realizar seguimiento a los desarrollos mediante las herramientas determinadas para tal finde servicio	1. Mesa de trabajo con grupo de contratación y formato de estudios previos contratación directa 2. Clausulados de contratos	Emerson Cruz - Giselle Muñetón	FECHA DE TERMINACION 31 DE DICIEMBRE DE 2022 El proceso auditado manifestó que se realizaron varias mesas de trabajo con el área de contratación para incluir en los contratos las cláusulas de sensibilización e información entregada por el contratista, sin embargo, no hubo consenso, por esta razón, desde el área de TI para los contratos donde su objeto contractual está relacionado con tecnología se diseñó y se incluyó el "ANEXO 3 – RELACIÓN DE INFORMACIÓN ENTREGADA Y SENSIBILIZACIÓN REALIZADA TIC (PROPUESTA)" en el formato "FOCT07 INFORME FINAL DE DESARROLLO DEL CONTRATO". Este anexo está pendiente de revisión y aprobación por parte de la jefe de la OAP. En la revisión de los contratos allegados por el proceso auditado, únicamente el de Carlos Andrés Molina contempla una obligación específica relacionada con elaboración y/o actualización de los formularios, tutoriales, protocolos y manuales y los contratos de Soledad Martínez y César Augusto González Jiménez tienen como obligación específica la transferencia de conocimiento. En el documento "METODOLOGÍA PARA EL DESARROLLO DE SOFTWARE DEL INSOR" en el capítulo final se menciona que en los documentos FOGT07 ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN (FUNCIONARIOS - CONTRATISTAS) y/o FOGT08 ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN (PROVEEDORES DE TECNOLOGÍA) se va a incluir como cláusula que dentro de las obligaciones de los contratos de prestación de servicios se garantice la entrega de la información manejada y una sensibilización sobre las actividades realizadas, en caso de que el supervisor lo solicite y entrega de productos de manera concreta, incluyendo aspectos cuantitativos y cualitativos, en caso de requerirse. Respecto a la cesión de derechos patrimoniales a favor del INSOR se menciona en el documento "METODOLOGÍA PARA EL DESARROLLO DE SOFTWARE DEL INSOR y en los contratos existe una cláusula relacionada con propiedad intelectual.	Citación a mesas de trabajo ANEXO 3 – RELACIÓN DE INFORMACIÓN ENTREGADA Y SENSIBILIZACIÓN REALIZADA TIC (PROPUESTA) Contratos de: Carlos Molina, David Andrés Bello, Soledad Carolina Martínez, Emerson Cruz Aldana, César Augusto González Jiménez y Gerson Leonardo Barreto Flórez. Metodología para el desarrollo de software del INSOR	CERRADO	ATENDIDO
27	36 .2	Planeación y Organización de la Gestión TIC - Plan de Administración de Riesgos y Contingencias	1/06/2021	30/11/2022	Actualizar los documentos "GUGT04 Guía para copias de seguridad_copia_no_controlada.pdf" y PRGT08 Procedimiento copias de respaldo de Información_copia_no_controlada.pdf a las condiciones actuales. OBSERVACIÓN 2021: - Incluir en la programación de copias de respaldo el Backup de los archivos de configuración de los sistemas manejadores de bases de datos (RDBMS), Backup de las bases de datos, las imágenes de los servidores físicos, configuraciones de switches, firewall routers, y en general de todas las configuraciones de los elementos activos de red." - Actualizar los documentos "GUGT04 Guía para copias de seguridad_copia_no_controlada.pdf" y PRGT08 Procedimiento copias de respaldo de Información_copia_no_controlada.pdf a las condiciones actuales. Incluir en la documentación del proceso registros de Planeación de copias de respaldo, de novedades de procesos y de restauraciones aleatorias en cumplimiento del objetivo de control 12.3 del MSPI.	3. Generar un formato del plan de copias de seguridad y un formato de novedades de procesos y restauraciones aleatorias de las copias de seguridad	3. Formato plan de copias de seguridad y novedades de restauración	Emerson Cruz - Giselle Muñetón	Si bien en la guía para copias de seguridad se determinan las frecuencias, tipos de backups y retención de las copias de seguridad, no se cuenta aún con un único formato de plan de copias de seguridad que permita identificar de forma detallada y en un único documento la información respaldada, la frecuencia, retención, ubicaciones intermedias y finales, ubicación de logs, permisos de acceso y de seguridad de todos los backups generados en la Entidad. Esto además de generar dependencia de la herramienta utilizada para programar y realizar las copias, podría generar retrasos en las restauraciones y genera dependencia de conocimiento de los encargados del proceso. Este insumo debe articularse con el plan de continuidad. No se ha implementado la recomendación, por lo tanto, el hallazgo continúa abierto.	No se cuenta con la evidencia	ABIERTO	EN PROCESO

28	37	Planeación y Organización de la Gestión TIC - Plan de Administración de Riesgos y Contingencias	1/11/2019	30/11/2022	Llevar control sobre las novedades de los procesos, especialmente sobre los fallidos o alertados. Establecer acciones correctivas e incluirlas en los procedimientos.	Incluir en la Guía para copias de seguridad_copia_no_controlada (GUGT04) y en el Procedimiento copias de respaldo de Información_copia_no_controlada(PRGT08) el registro de las restauraciones y control de novedades de las copias de seguridad.	Documentos actualizados	Emerson Cruz - Giselle Muñetón	FECHA DE TERMINACIÓN 31/11/2022 La auditoría recibió del proceso auditado el documento "GUIA PARA COPIAS DE SEGURIDAD", en su versión 2, actualizada y publicada en el SGC el día 10 de octubre de 2022, en la cual se define correctamente la estrategia de Backups adoptada por la Entidad, la información a respaldar, el proceso de restauración, plan de pruebas de las restauraciones, la estrategia de copias de seguridad de los correos electrónicos de la Entidad y se emiten algunas recomendaciones. También se aportó el documento "MANUAL PARA RESPALDO Y RECUPERACIÓN DE DATOS DE LA INFRAESTRUCTURA TECNOLÓGICA", versión 1, aprobado y publicado en el SGC el 25/08/2022, donde se describen las generalidades para la gestión de copias de respaldo y su recuperación cuando sea necesario para garantizar la disponibilidad, seguridad y confidencialidad de la información del INSOR Aún no se ha avanzado en el diseño de los formatos de novedades de backups con sus respectivas acciones correctivas y el plan de copias de seguridad que permita identificar de forma detallada y en un único documento la información respaldada, la frecuencia, retención, ubicaciones intermedias y finales, ubicación de logs, permisos de acceso y de seguridad de todos los backups generados en la Entidad y que no dependa de la herramienta actualmente en uso. Se reitera incluir un formato de novedades de procesos y de restauraciones aleatorias en cumplimiento del objetivo de control 12.3 del MSPI No se ha atendido en su totalidad la recomendación, por lo tanto, el hallazgo continúa abierto.	GUIA PARA COPIAS DE SEGURIDAD MANUAL RESPALDO Y RECUPERACIÓN DE DATOS DE LA INFRAESTRUCTURATECNOLÓGICA	ABIERTO	EN PROCESO
31	39 .2	Planeación y Organización de la Gestión TIC - Políticas de seguridad	1/02/2022	30/04/2022	Continuar la implementación del modelo MSPI en tres proyectos paralelos: • La elaboración del marco documental de políticas, procedimientos, instructivos y formatos • Un programa de concientización, educación y capacitación sobre la seguridad de la información (control 7.2.2 ISO 27002:2013). • 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 OBSERVACIÓN 2021: - En la siguiente actualización del instrumento de evaluación MSPI, relacionar como evidencias los documentos evolucionados para cada control de MSPI y registrar el avance teniendo en cuenta que la implementación 100% de cada componente incluye: Planear, elaborar los instrumentos, implementar los controles, sensibilizar, evaluar efectividad y mejorar. - Una vez implementados los controles MSPI y los instrumentos definir métricas o indicadores de efectividad.	2. Instrumento de evaluación MSPI actualizado con evidencias de cada control	2. Instrumento de evaluación MSPI	Emerson Cruz - Giselle Muñetón	Si bien se ha actualizado el instrumento de evaluación del MSPI y se han relacionado como evidencia los documentos que se han elaborado con su respectivo link, aún se encuentran controles sin su respectiva evidencia, no se han relacionado la totalidad de documentos elaborados por el área de TI y de los controles implementados. Debido a que MINTIC obliga mediante la RESOLUCIÓN 500 DE MARZO 10 DE 2021, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", y en especial su Anexo 1 de febrero de 2021 que establece los lineamientos y el alcance enmarcado en los 114 controles de la norma ISO 27002 y las cláusulas de la norma ISO 27001 a integrar en el sistema integrado de gestión de la entidad como eje de Sistema de Gestión de Seguridad de la Información, y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; estructurado en cinco (5) fases las cuales permiten que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Se hace necesario que todos los controles queden correctamente implementados y tengan evidencia de su correcto funcionamiento con sus respectivos soportes documentales. Independiente del avance de implementación del MSPI, el proceso auditado ha avanzado en el seguimiento y la evidencia presentada es pertinente. En el plan de implementación del MSPI se debe continuar con la evaluación aportando sus respectivos soportes documentales.	Anexo - Declaración de aplicabilidad Instrumento_Evaluacion_MSPI	CERRADO	ATENDIDO
32	39 .3	Planeación y Organización de la Gestión TIC - Políticas de seguridad	1/03/2022	31/12/2022	Continuar la implementación del modelo MSPI en tres proyectos paralelos: • La elaboración del marco documental de políticas, procedimientos, instructivos y formatos • Un programa de concientización, educación y capacitación sobre la seguridad de la información (control 7.2.2 ISO 27002:2013). • 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 OBSERVACIÓN 2021: - En la siguiente actualización del instrumento de evaluación MSPI, relacionar como evidencias los documentos evolucionados para cada control de MSPI y registrar el avance teniendo en cuenta que la implementación 100% de cada componente incluye: Planear, elaborar los instrumentos, implementar los controles, sensibilizar, evaluar efectividad y mejorar. - Una vez implementados los controles MSPI y los instrumentos definir métricas o indicadores de efectividad.	3. Indicadores de efectividad	3. Hoja de vida de indicadores, acta de reunión ajuste indicadores	Emerson Cruz - Giselle Muñetón	Al no tener implementados todos los controles que forman parte del MSPI, aún no es posible definir todos los indicadores de efectividad para el control de su implementación y correcto funcionamiento de los mismos. Los indicadores que se han elaborado e implementado no constituyen la totalidad de los requeridos en el proceso de implementación y monitoreo del MSPI. Por lo tanto, la recomendación permanece abierta y se debe evaluar e implementar al completar la definición, documentación e implementación de todos los controles del MSPI.	Hoja de vida de indicadores, acta de reunión ajuste indicadores	ABIERTO	EN PROCESO
33	40	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/02/2020	31/07/2022	Procedimiento para el cambio periódico de las claves de administrador para el Dominio, Routers y Firewalls e instructivos de la configuración y operación del firewall OBSERVACIÓN 2021: Desarrollar instructivos de configuración y operación del Firewall	Identificar controles de seguridad que se pueden usar para la implementación del modelo MSPI	Declaración de aplicabilidad	Emerson Cruz - Giselle Muñetón	TERMINACION PROYECTADA PARA EL 31/07/2022. Se realizó la actualización del procedimiento:"PRGT02 Procedimiento Gestión usuarios y contraseñas_v2" entregado a la auditoria, en donde se hace referencia de forma adecuada al instructivo "ITGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION", en este instructivo se describe adecuadamente el manejo de contraseñas de administradores. En el procedimiento entregado, además de determinar el control y cambio periódico de contraseñas de usuarios para los servicios y aplicaciones ofrecidos por el área, se adiciona un paso enfocado al control de contraseñas administrativas y de dispositivos y elementos de red. Aún no se encuentran elaborados los instructivos de configuración y operación del Firewall, sin embargo se evidencia un mayor conocimiento de las configuraciones por parte del contratista encargado de su administración. La evidencia que se debe aplicar a este hallazgo es el procedimiento "PRGT02 Procedimiento Gestión usuarios y contraseñas_v2" y el instructivo "ITGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION", por lo cual la que esta registrada en el plan de mejoramiento no es la pertinente. Falta adicionar como evidencia el instructivo de configuración y operación del Firewall para cerra el hallazgo.	"PRGT02 Procedimiento Gestión usuarios y contraseñas_v2" "ITGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION"	ABIERTO	EN PROCESO

35	41 .2	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/06/2022	31/07/2022	Cambiar todas las contraseñas de cualquier servicio expuesto sobre la red y ocultarlos para que no sea posible su visualización por parte de cualquier usuario sin autenticación en dominio. OBSERVACIÓN 2021: Se debe tramitar con el proveedor de Solgein la entrega de usuario y contraseña de la base de datos ya que ningún tercero debe tener acceso a los datos de producción de la Entidad, esto además de generar alertas de advertencia en la generación de las copias de seguridad, deja abierta la posibilidad de accesos directos a la base de datos al proveedor para alterar, copiar o eliminar información perteneciente a la Entidad y por ende incumplir con las políticas de seguridad del INSOR. - Tomar el control y conocimiento de las contraseñas de los sistemas de información las manejan los proveedores, esto genera un alto riesgo de dependencia y va en contra de la confidencialidad y seguridad de la informa de la Entidad, ya que el tercero tiene el control total de la información almacenadas en las bases de datos de estos sistemas de información.	2. Proveedor SOLGEIN debe realizar entrega de usuario y contraseña de la Base de datos	2. Documento con usuario y contraseña de base de datos SOLGEIN	Emerson Cruz - Giselle Muñetón	En cuanto este hallazgo, se evidencia que se realizaron las acciones necesarias para obtener del proveedor de SOLGEIN el usuario y contraseña de usuario administrador, sin embargo el proveedor se negó a este requerimiento por motivos de seguridad en la integridad de la base de datos, y entregó un usuario al área con permisos de solo lectura para labores de revisión. El usuario entregado no permite solucionar el problema con las copias de seguridad generadas desde el Veam Backup, por lo cual aún existe la dependencia de la gestión del proveedor, y va en contra de la confidencialidad y seguridad de la información generada por la Entidad, ya que el tercero tiene el control total de la información almacenada en las bases de datos de este sistema de información. Si bien existen acuerdos de confidencialidad el riesgo continúa. Se recomienda fortalecer el acuerdo ya que en este caso específico la información la maneja el tercero y no la entidad, y por ende debe ser directo responsable de la administración , confiabilidad y seguridad de los datos y presentar informes de las labores administrativas que realizan para asegurar la integridad y buen funcionamiento de la base de datos, ya que la entidad no puede realizar estas acciones con el usuario suministrado. Este hallazgo continua abierto debido a la negativa del proveedor de suministrar la clave, si bien se realizaron las acciones por parte del área, en el nuevo plan de mejoramiento se deben reformular las acciones orientadas a controlar este riesgo o consultar juridicamente qué se puede hacer al respecto.	Se presentan la generación de backups de la base de datos de solgein por parte del proveedor en una unidad del servidor de SOLGEIN.	ABIERTO	EN PROCESO
41	45	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/03/2020	31/03/2022	Acta entrega personal- servicios tecnológicos - formatos dominio 9- privilegios entrega de equipos - privilegios	Revisar junto con el Proceso de Gestión de Bienes y Servicios el procedimiento Gestión de almacén e inventarios para identificar cuales serian los ajustes al procedimiento y formatos para la asignación y devolución de bienes y servicios tecnológicos y realizar la respectiva actualización de la documentación.	1.Actas de reunión 2.Documentación actualizada	Emerson Cruz - Giselle Muñetón	El proceso auditado aportó el acta donde se revisó junto con el Proceso de Gestión de Bienes y Servicios el procedimiento Gestión de almacén e inventarios para identificar cuáles serían los ajustes al procedimiento y formatos para la asignación y devolución de bienes y servicios tecnológicos y realizar la respectiva actualización de la documentación. Se actualizaron los documentos: Procedimiento de baja de bienes devolutivos Procedimiento reintegro y traslado de activos Procedimiento gestión de bienes Procedimiento de inventarios La recomendación fue atendida y las evidencias presentadas fueron pertinentes, por lo tanto, el hallazgo se cierra.	Acta de reunión Procedimientos	CERRADO	ATENDIDO
42	46	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/06/2020	30/11/2022	Monitoreo y control de eventos Dominio 12 12-4 y 12-7 - procedimientos - Correlacionador de eventos - todos los sistemas solo un procedimiento y una aplicación - activos	Implementar un mecanismo de seguimiento a los eventos de los sistemas que conforman la plataforma tecnológica	Mecanismo (Correlacionador de eventos) implementado	Emerson Cruz	Se implementó la herramienta de uso gratuito para el monitoreo y control de la infraestructura de red: Observium, que se ha parametrizado principalmente para monitorear la disponibilidad y salud de los equipos en cuanto a temperatura, almacenamiento de los principales equipos de TI. El contratista encargado del monitoreo entrega mensualmente un informe de la disponibilidad de los equipos. Se reitera que se debe completar el proceso de parametrización y seleccionar informes ejecutivos generados desde las herramientas como evidencias de las acciones de seguimiento y control sobre la infraestructura de TI. Esta herramienta complementa el proceso de monitoreo con las consolas de Firewall y antivirus que a su vez forman parte del monitoreo y control de eventos y que aun no se cuenta con informes de revisión del estas consolas y las acciones de remediación recomendadas. La recomendación no se ha atendido en su totalidad, por lo tanto, el hallazgo continúa abierto.	Imagen del panel de control de observium. Magen de consola del firewall. SEGUIMIENTO INFRAESTRUCTURA_AGOSTO SEGUIMIENTO INFRAESTRUCTURA_SEPTIEMBRE	ABIERTO	EN PROCESO
43	47	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/06/2020	30/11/2022	Generar un procedimiento de revisión periódica de los informes generados por el antivirus y tomar acciones correctivas frente a alertas	Implementar un mecanismo de seguimiento a los eventos de los sistemas que conforman la plataforma tecnológica	Mecanismo (Correlacionador de eventos) implementado	Emerson Cruz	Se elaboró el procedimiento: PRGT13 PROCEDIMIENTO DE SEGUIMIENTO DE INFRAESTRUCTURA, pero este está enfocado en la revisión de la disponibilidad de la infraestructura y no hace referencia a las consolas de monitoreo del firewall, ni del antivirus, ni al registro de las acciones correctivas de las alertas emitidas por las consolas mencionadas. El objetivo de esta recomendación es tener una evidencia de la verificación y seguimiento a los eventos y alertas emitidas por las consolas administrativas disponibles en la infraestructura de la Entidad: Consola del firewall, antivirus, observium, vmware, etc. Como solo se están teniendo en cuenta los eventos relacionados con la disponibilidad de los equipos de la infraestructura no se han atendido en su totalidad las recomendaciones y por lo tanto el hallazgo continúa abierto.	RGT13 PROCEDIMIENTO DE SEGUIMIENTO DE INFRAESTRUCTURA	ABIERTO	EN PROCESO
44	48	Administración de accesos y Seguridad Lógica - Elementos de protección de red	1/06/2020	31/08/2022	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	1. Diseñar el diagrama de VLAN´S y aplicar configuración de los switch acorde al diagrama. 2. Realizar pruebas con herramientas .	Diagrama de VLAN implementado	Emerson Cruz	Si bien ya se tiene correctamente configurada en el firewall la segmentación de la red wifi de invitados y se presenta avance en la configuración de segmentos de red por cada área del Insor mediante el DHCP del directorio activo. Se está esperando la adquisición de los nuevos switches para completar este configuración. En las pruebas realizadas por el auditor se evidencia que a pesar de existir los segmentos, aún se pueden realizar escaneos de un segmento a otro, desde el segmento del equipo asignado al auditor se realizaron escaneos hacia el segmento de servidores, permitiendo así búsquedas de objetivos y de recursos o archivos no protegidos de usuarios conectados a la red local. En cuanto a la red WIFI es importante adjuntar pruebas de escaneos hacia los segmentos administrativos como evidencia de su correcto funcionamiento, ya que no se pudieron realizar estas pruebas debido a la pandemia. Se recomienda implementar los segmentos en la instalación de los nuevos switches y configurarlos para evitar escaneos a los otros segmentos. Si es necesario tener servicios expuestos para todos los usuarios de la red local, dejarlos en un segmento aparte sin que se expongan los otros equipos o servidores. Por lo anterior esta recomendación aun no se encuentra totalmente implementada, continúa en estado abierto.	Imagen de configuración de VLAN's en el Firewall.	ABIERTO	EN PROCESO

45	49	Administración de accesos y Seguridad Lógica - Elementos de protección de red	1/01/2020	31/07/2021	Fortalecer la capacitación a los funcionarios de la OAP para disminuir la dependencia de conocimiento del proveedor del firewall y elaborar un procedimiento para el cambio periódico de las claves de administrador para el Dominio, Routers y Firewalls e instructivos de la configuración y operación del firewall OBSERVACIÓN 2021: Elaborar procedimientos formales para el seguimiento, indicadores y formato de seguimientos a acciones de mejora como resultado del monitoreo de la infraestructura realizados desde las consolas del firewall, antivirus y Observium.	1.Incluir en los RFP las obligaciones de los contratistas de soporte de la plataforma tecnológica, para realizar las capacitaciones en las distintas herramientas tecnológicas. 2.Verificar las obligaciones en el contrato y acordar con el proveedor el cronograma de capacitaciones. 3. Elaboración de procedimientos para seguimiento, indicadores y acciones de mejora del monitoreo de la infraestructura tecnológica.	1. RFP incluyendo capacitaciones 2. Acta de inicio y Cronograma - 3. Procedimientos de infraestructura tecnológica	Emerson Cruz	Se evidencia un mayor conocimiento y apropiación en el manejo del firewall, su configuración y monitoreo por parte de funcionario a cargo de la administración. Se adicionó en los RFP de los contratos del firewall y antivirus dentro de los objetivos específicos la capacitación en el uso y configuración de las herramientas entregadas por el proveedor. Aún no se han elaborado los procedimientos formales para el seguimiento, indicadores y formato de seguimientos a acciones de mejora como resultado del monitoreo de la infraestructura realizados desde las consolas del firewall, antivirus y Observium, por lo tanto, el hallazgo continúa abierto. Se recomienda dejar la acción 3 en el plan de mejoramiento para la próxima vigencia.	No se presentan evidencias	ABIERTO	EN PROCESO
47	50	Administración de accesos y Seguridad Lógica - Elementos de protección de red	1/10/2019	31/12/2022	Configurar las políticas de firewall y las políticas de dominio para impedir descargas de archivos ejecutables o de instalación. La restricción se debe generar independientemente del cargo del usuario. Todo archivo ejecutable que se requiera debe ser autorizado por la OAP. OBSERVACIÓN 2021: Incluir las acciones de revisión de las restricciones de seguridad implementadas en políticas de dominio, del firewall y del antivirus en los mantenimientos preventivos.	1. Realizar la configuración de políticas para impedir descarga de archivos ejecutables 2. Incluir acciones de restricciones de seguridad en políticas de dominio, firewall y antivirus	1. Evidencia configuración realizada en Firewall 2. Pantallazo de restricciones en consolas de dominio, firewall y antivirus	Emerson Cruz	Si bien se han realizado configuraciones en el firewall para evitar las descargas de archivos ejecutables, en las pruebas realizadas por el auditor en la visita presencial de la auditoria, se evidenció que aún se pueden descargar y ejecutar archivos ejecutables. Por lo tanto, esta recomendación no se ha implementado correctamente. El antivirus se encuentra correctamente configurado para eliminar descargas de archivos peligrosos, pero en cuanto a software portable no considerado como peligroso, si se permite. En las pruebas el auditor logró descargar y ejecutar software de escaneo de red y para el descubrimiento de puertos abiertos y recursos compartidos en los equipos de red la entidad. Las acciones de revisión de las restricciones de seguridad implementadas en políticas de dominio, del firewall y del antivirus aun no están incluidas como parte de las acciones de los mantenimientos preventivos. La recomendación no está totalmente implementada, por lo tanto el hallazgo permanece abierto.	Imagen de ejecución de Advanced port escáner en equipo de la entidad. Imagen de configuración en el Firewall para el bloqueo de descargas.	ABIERTO	EN PROCESO
49	51 .1	Administración de accesos y Seguridad Lógica - Elementos de protección de red	1/10/2019	30/08/2021	Configurar la red y el DHCP para restringir la conexión al dominio solo a equipos cuya Mac Address este registrada en la lista autorizada OBSERVACIÓN 2021: Crear tener una versión del diagrama de red para la OAP en la cual se relacionen y se puedan identificar detalladamente los rangos de direcciones IpV4 y las equivalencias de IPv6, tanto de servidores como de los segmentos de red configurados (incluyendo los de WIFI) además, que permita identificar los equipos de DHCP y DNS, y elementos de contingencia.	1. Configuración en el directorio activo (AD) para restringir acceso a equipos no autorizados	1. Evidencia de la configuración de AD/DC de usuarios y equipos		Se tiene configurado en el dominio, los rangos de direcciones Ip que se pueden asignar a equipos conectados a la red en grupos administrativos y por usuarios. Sin embargo, aún no se tienen restricciones por las direcciones de tarjetas de red como se especifica en la recomendación. Si bien el control que se implementó aumenta la seguridad, no garantiza que equipos no autorizados puedan conectarse ya que cambiando la configuración de red del equipo no autorizado y su nombre, sería posible evadir esta restricción. Este configuración se puede implementar también en el DHCP del directorio activo. Como evidencia valida del funcionamiento de esta recomendación, el proceso de gestión TIC, debe adjuntar la prueba de conexión de un portátil externo a los de los funcionarios del INSOR y verificar que no asigne, ni permita configurar la IP del equipo dentro del rango de direcciones configuradas en el DHCP del dominio. Por lo tanto, el hallazgo permanece abierto	Imagen de asignación de IP en la pruebas realizadas.	ABIERTO	EN PROCESO
50	51 .2	Administración de accesos y Seguridad Lógica - Elementos de protección de red	1/08/2022	31/12/2022	Configurar la red y el DHCP para restringir la conexión al dominio solo a equipos cuya Mac Address este registrada en la lista autorizada OBSERVACIÓN 2021: Crear tener una versión del diagrama de red para la OAP en la cual se relacionen y se puedan identificar detalladamente los rangos de direcciones IpV4 y las equivalencias de IPv6, tanto de servidores como de los segmentos de red configurados (incluyendo los de WIFI) además, que permita identificar los equipos de DHCP y DNS, y elementos de contingencia.	2. Diagrama de red en la cual se relacionen y se puedan identificar detalladamente los rangos de direcciones IpV4 y las equivalencias de IPv6, tanto de servidores como de los segmentos de red configurados (incluyendo los de WIFI) además, que permita identificar los equipos de DHCP y DNS, y elementos de contingencia.	2. Diagrama de red rangos IPV4 IPV6		En el esquema de red que se presentó a la auditoria aun no se tienen relacionadas las equivalencias de IPv4 -IPv6, se pueden identificar los diferentes segmentos de red, los servicios de TI y elementos de contingencia de forma adecuada. Se atendió la recomendación y la evidencia es pertinente, por lo tanto, el hallazgo se cierra.	Red_INSOR2022.jpg	CERRADO	ATENDIDO
51	52	Administración de accesos y Seguridad Lógica - Elementos de protección de red	1/10/2019	30/08/2021	En el marco de la construcción del inventario de activos de información, identificar equipos de computo que almacenan de manera local información de carácter confidencial e implementar medidas de seguridad que impidan su acceso por alguien distinto al responsable del equipo. OBSERVACIÓN 2021: - Actualizar el inventario de activos de información incluyendo los demás activos establecidos en el Manual de Seguridad de la información de la entidad y en todo caso los lineamientos ISO 27001. - Configurar en la consola de antivirus la opción de control de dispositivos para deshabilitar todos los dispositivos extraíbles como unidad de CD, USB, bluetooth, celulares, etc. Y solo permitir aquellos que sean aprobados para su uso dependiendo del usuario con privilegios que lo necesite para las funciones de su cargo. El uso de CD o USB 's de arranque permite violar la seguridad de cualquier equipo, ya que podría cambiarse la contraseña de administrador local de los mismos. - Implementar un control sobre las unidades de almacenamiento local en las que se guardar información los usuarios, es importante informar a los usuarios que si a información se guarda fuera de las carpetas propias de su sesión (Mis Documentos, Descargas, etc.), quedan sin la protección adecuada y es visible por otros usuarios del equipo. - Implementar un procedimiento de monitoreo sobre las cuentas administrativas y sin actividad, existen herramientas gratuitas como el 10-strike network scanner, que permiten generar informe con	1. Configuración en el directorio activo (AD) para restringir acceso a equipos no autorizados 2. Matriz de activos de información 3. Presentar un plan de uso de dispositivos extraíbles a la alta dirección - 4. Dentro del plan de mantenimiento de equipos de computo implementar el control sobre las unidades de almacenamiento local. - 5. Implementar un procedimiento de monitoreo sobre las cuentas administrativas y sin actividad	1. Evidencia de la configuración de AD/DC de usuarios y equipos 2. Matriz de activos de información de la entidad 3. Plan de uso de dispositivos extraíbles - 4. Plan de mantenimiento de equipos de computo 5. Procedimiento formalizado	1. Emerson Cruz	Si bien ya se ha actualizado la matriz de activos de información de la entidad, aún no se han identificado, ni implementado políticas para que en los equipos de cómputo que almacenan de manera local información de carácter confidencial impidan su acceso por alguien distinto al responsable del equipo. La evidencia relacionada no es la pertinente para la atención de esta recomendación, debe se el informe de la configuración de las políticas de seguridad del dominio para permitir solo el almacenamiento de archivos en las carpetas de usuario del dominio autenticado en el equipo. En cuanto al plan de usos de dispositivos extraíbles se encuentra correctamente implementada la política de seguridad del dominio: USB_Restricción, en la cual se restringe el acceso a la ejecución, lectura y escritura sobre medios de almacenamiento extraíbles en los equipos del dominio de la Entidad. Sin embargo, no se presenta evidencia de la elaboración del plan de uso de dispositivos extraíbles. Aún no ha sido incluida la revisión de los controles de seguridad implementados para las unidades de almacenamiento local dentro del listado de acciones del mantenimiento preventivo de los equipos de la entidad. No se ha adelantado la elaboración del procedimiento de monitoreo sobre las cuentas administrativas y sin actividad. Ni se presenta evidencia del uso de herramientas para su control El estado de este hallazgo se mantiene en abierto	Registro activos de información INSOR 2022 Consolidado criticidad GPO USB_Restricción	ABIERTO	EN PROCESO

56	53	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/10/2019	31/07/2022	Restringir en todos los equipos de escritorio y portátiles el acceso al panel de control y en especial al centro de redes y recursos compartidos. Restringir de igual manera la ejecución de comandos desde el símbolo del sistema de Windows (CMD), RegEdit y del PowerShell en los equipos de usuario Igualmente configurar los navegadores para impedir el almacenamiento de contraseñas en texto plano Impedir en todos los equipos la creación de conexiones ODBC En los equipos donde se encuentra instalado SOLGEIN eliminar las herramientas ejecutables que se usan para desarrollo y conexión a la base de datos Oracle	1. Realizar la validación y configuración del GPO-ODBC 2. Eliminar las herramientas ejecutables que se usan para desarrollo y conexión a base de datos Oracle en los equipos donde esta instalado SOLGEIN 3. Realizar la depuración de herramientas de acceso a base de datos en los equipos que usan Solgein	1 y 2 Evidencia de la configuración 3. Matriz de seguimiento	Técnico de soporte, Emerson Cruz	En las pruebas realizadas por la auditoria en un equipo de usuario del INSOR, se evidencia que estas restricciones aun no están configuradas correctamente , en las evidencias recolectadas en las pruebas el auditor obtuvo acceso sin restricción al panel de control y al centro de redes y recursos compartidos. En la nueva política aportada por el proceso auditado se evidencia que las restricciones están configuradas en las políticas de dominio, por lo tanto, se cierra el hallazgo. Sin embargo, se debe validar que estas políticas estén correctamente implementadas en las pruebas de mantenimiento.	Default Domain Controllers Policy GPO-Usuario-Base - Directiva Insor	CERRADO	ATENDIDO
58	55	Administración de accesos y Seguridad Lógica - Elementos de protección de red	1/03/2020	31/12/2022	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	1. Elaborar matriz de Perfiles y Roles de usuarios para determinar qué navegación debe tener cada usuario 2. Aplicar privilegios de navegación acorde con la matriz 3. Realizar sensibilización de perfiles y roles de usuarios	Matriz de perfiles aplicada en la navegación, evidencias de sensibilización	Emerson Cruz	Se elaboró el documento: "MATRIZ ROLES Y RESPONSABILIDADES.xls", en el cual se definen los permisos de navegación de usuarios de acuerdo a sus cargos y funciones. Sin embargo aún la matriz no está diligenciada totalmente debido a que las áreas no han presentado toda la información necesaria para su implementación. Los perfiles propuestos para el control de navegación son: GENERAL, VIP, REDES SOCIALES Y TECNOLOGIA y se relacionan con cada usuario de la matriz. Para el perfil Redes sociales se permite y tiene habilitado el uso de las mismas, pero queda como responsabilidad de los usuarios su correcto uso y se deja abierta la posibilidad de acceso a cuentas personales. Debido a que aún no se ha terminado la matriz la recomendación y no ha sido implementada en su totalidad, el hallazgo continúa abierto.	MATRIZ ROLES Y RESPONSABILIDADES.xls	ABIERTO	EN PROCESO
59	56	Administración de accesos y Seguridad Lógica - Pruebas de seguridad Externas	1/10/2019	31/12/2021	Atender las vulnerabilidades de los portales Orfeo y Reni de manera inmediata OBSERVACIÓN 2021: Atender las oportunidades de mejora en rendimiento de los portales web de la Entidad	1. Realizar la configuración de seguridad en los portales de ORFEO Y RENI 2. Informe con oportunidades de mejora a portales web	1. Evidencia de pruebas de vulnerabilidad a portales 2. Atender las oportunidades de mejora en rendimiento de los portales web de la Entidad	Emerson Cruz	Las correcciones realizadas al portal de Orfeo, continuan correctamente implementadas. Cabe anotar que el escaneo de vulnerabilidades Web debe ser periódico, ya que cada día se descubren vulnerabilidades y por ende este proceso es dinámico, Aún no se evidencia el uso de herramientas gratuitas para este propósito como OWASP -ZAP y los de escaneos gratuitos en línea del sitio:"pentest-tools". En cuanto al portal RENI se encuentra en restructuración y nuevos desarrollos y por tanto aún no se ha podido verificar sus vulnerabilidades, se tiene planificado por parte del área la realización de este análisis una vez sea entregado el desarrollo. El proceso auditado presentó el informe portales Web donde se hace un análisis del rendimiento y de algunas opciones de seguridad de los portales Web. Cumplieron con las acciones previstas, se recomienda adelantar esta tarea periodicamente como parte de la mejora continua.	Informe portales Web Oct 2022	CERRADO	ATENDIDO
61	57 .1	Seguridad Física	1/07/2020	31/12/2022	Se debe adelantar un plan de etiquetado y generación de diagrama en todos los closets de comunicaciones (Racks) del centro de cómputo para permitir la fácil ubicación de equipos, puntos de red y proveer en todos los closets los organizadores de cables y organizarlos con el fin de agilizar la identificación y ubicación de cualquier falla. OBSERVACIÓN 2021: Incluir un diagrama de distribución de puntos, equipos y elementos activos de red en los closets de cableado para facilitar la rápida referenciación de puntos y equipos al personal de soporte y o contratistas en caso de contingencia.	1. Realizar inventario y etiquetado de conexiones de red en Rack de Data Center	1. Evidencia del etiquetado del cableado de Data Center	Emerson Cruz	FECHA DE TERMINACION 31/12/2022 El proceso auditado aportó la documentación correspondiente al contrato adjudicado para la adquisición de los insumos para el etiquetado. El hallazgo continúa abierto.	Anexo Tecnico Estudios Previos Aceptacion de oferta No 141-2022	ABIERTO	EN PROCESO
62	57 .2	Seguridad Física	1/08/2022	30/11/2022	Se debe adelantar un plan de etiquetado y generación de diagrama en todos los closets de comunicaciones (Racks) del centro de cómputo para permitir la fácil ubicación de equipos, puntos de red y proveer en todos los closets los organizadores de cables y organizarlos con el fin de agilizar la identificación y ubicación de cualquier falla. OBSERVACIÓN 2021: Incluir un diagrama de distribución de puntos, equipos y elementos activos de red en los closets de cableado para facilitar la rápida referenciación de puntos y equipos al personal de soporte y o contratistas en caso de contingencia.	2. Generar diagrama de distribución de puntos, equipos y elementos activos de red en los closets de cableado	2. Diagrama de distribución closets de cableado	Emerson Cruz	Aún no se evidencia avance en esta recomendación debido a que se van a realizar actualizaciones de equipo y elementos del centro de cómputo y por lo tanto se aplazó la actividad, ya que se va a incluir como parte de este contrato.		ABIERTO	EN PROCESO
63	58	Desarrollo y Adquisición de Software Aplicativo	1/03/2020	31/12/2022	Adoptar una metodología para la adquisición y desarrollo de sistemas de información que incluya como mínimo los siguientes instrumentos de control; • Documentos de requisitos de la adquisición RFP • Formatos de especificación de requerimientos para desarrollos internos y contratados con terceros y apalancar su firma por parte del solicitante como requisito para iniciar desarrollo • Procedimientos para el protocolo de pruebas y gestión de defectos que se constituyan en criterios de aceptación para productos de desarrollo • Establecer criterios de aceptación para todo tipo de entregables: documentos, servicios y productos • Condiciones mínimas de documentación técnica de acuerdo a cada caso: adquisición de software comercial, desarrollo por encargo a terceros o desarrollo interno • Procedimientos de aceptación y despliegue en ambientes En ningún caso los proveedores deben hacer despliegues autónomos a ambientes productivos OBSERVACIÓN 2021: - Incorporar al documento de "METODOLOGIA PARA EL DESARROLLO DE SOFTWARE INSOR" una técnica de estimación de esfuerzo para los desarrollos de software. - Incorporar al documento de "METODOLOGIA PARA EL DESARROLLO DE SOFTWARE INSOR", los lineamientos del MSPI para el dominio 14, dando cobertura a los 3 escenarios en los cuales se da la adquisición y desarrollo de software aplicativo - Incorporar al documento de "METODOLOGIA PARA EL DESARROLLO DE SOFTWARE INSOR", las mejoras a los instrumentos mencionados en el presente informe: - Identificación y documentación de requerimientos No Funcionales al igual que los funcionales	1. Diseñar y adoptar metodología para la adquisición y/o desarrollo de sistemas de información para la entidad. 2. Actualizar documento Metodología para el desarrollo de software Insor según las recomendaciones	1. Documento de Metodología para desarrollo y adquisición de sistemas de información 2. Actualizar documento Metodología para el desarrollo de software Insor según las recomendaciones	Emerson Cruz	TERMINACION PROYECTADA PARA 31/12/2022 El proceso auditado aportó el documento "METODOLOGÍA PARA EL DESARROLLO MANTENIMIENTO DE SOFTWARE DEL INSOR" actualizada versión 2, aprobada el 26 de octubre de 2022 y publicada en el Sistema de gestión de Calidad. Esta tiene en cuenta los lineamientos del MSPI para el dominio 14, dando cobertura a los 3 escenarios en los cuales se da la adquisición y desarrollo de software aplicativo: Desarrollo de software in house, desarrollo de software por encargo de terceros y adquisición de sistemas de información comerciales, sin embargo, la institución no ha avanzado en la política de desarrollo seguro de software independiente si desarrolla software por encargo, in house o adquiere sistemas de información comerciales, tal como lo exige el dominio 14 del MSPI. Para el proceso de desarrollo de software se hace la solicitud a través del GLPI, donde se indica si es por primera vez, una actualización de software o mantenimiento de algún sistema informático usado en INSOR, las categorías ya están debidamente creadas en la herramienta. Dentro de la metodología se definen los procesos, métodos y herramientas para el desarrollo de software para el INSOR, enfocándose principalmente en los procesos asociados a la planeación y control de un proyecto de construcción o actualización de software propio o de terceros. En el documento se hace referencia a los formatos: FOGT09 Formato Implementación de software, FOGT10 Formato pruebas de software, FOGT11 Formato Diseño de arquitectura de solución, FOGT12 Formato Levantamiento del requerimiento detallado, FOGT13 Formato Planeación y gerencia de proyecto, FOGT14 Formato Análisis de requisitos y requerimientos, FOGT15 Formato Descripción y Formalización general de requerimiento, los cuales se encuentran aprobados y publicados en el Sistema de Gestión de Calidad desde el 14 de octubre de 2021. Si bien se cuenta con la metodología y los formatos establecidos, no se incluyen explícitamente en las especificaciones los requisitos de parametrización, seguridad, auditoría, desempeño y reportes o consultas asociados a cada especificación. A la auditoria se presentaron diligenciados por parte del desarrollador de RENI los formatos de implementación de software, prueba de software y diseño de requerimos de la solución. Sin	PRGT11 PROCEDIMIENTO ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN FOGT07 ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN (FUNCIONARIOS - CONTRATISTAS) FOGT08 ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN (PROVEEDORES DE TECNOLOGÍA) FOGT09 Formato Implementación de software - FOGT10 Formato pruebas de software FOGT11 Formato Diseño de arquitectura de solución - FOGT12 Formato Levantamiento del requerimiento detallado FOGT13 Formato Planeación y gerencia de proyecto - FOGT14 Formato Análisis de requisitos y requerimientos FOGT15 Formato Descripción y Formalización general de requerimiento - Formatos FOGT09, FOGT10 y FOGT11 diligenciados para RENI	CERRADO	ATENDIDO

65	59	Desarrollo y Adquisición de Software Aplicativo	1/03/2020	31/12/2022	Incluir en los sets de prueba, casos de pruebas no funcionales cuando el desarrollo implique procesamiento de altos volúmenes de datos o alta concurrencia de usuarios. Aplicar siempre pruebas no funcionales cuando son desarrollos de cara a la ciudadanía	Diseñar y adoptar metodología para la adquisición y/o desarrollo de sistemas de información para la entidad.	Documento de Metodología para desarrollo y adquisición de sistemas de información	Emerson Cruz	TERMINACION PROYECTADA PARA EL 31 DE DICIEMBRE DE 2022 En el documento "METODOLOGÍA PARA EL DESARROLLO MANTENIMIENTO DE SOFTWARE DEL INSOR" se hace mención a la fase de pruebas, describiendo a nivel general los criterios que se deben tener en cuenta para el desarrollo de las pruebas de software de aceptación y aseguramiento de la calidad antes de su puesta en producción, sin embargo, no se incluyó lo referente a los set de pruebas, se recomienda incluir en los entregables un set de pruebas no funcionales con carga de trabajo sobre todo para aquellos sistemas de información que son para la ciudadanía. Se cuenta con la metodología de desarrollo y adquisición de software que es el producto de la acción de mejora, sin embargo, se debe incluir en el nuevo plan de mejoramiento acciones orientadas al cumplimiento de la implementación de esta metodología.	METODOLOGÍA PARA EL DESARROLLO MANTENIMIENTO DE SOFTWARE DEL INSOR	CERRADO	ATENDIDO
66	60	Desarrollo y Adquisición de Software Aplicativo	1/01/2021	31/12/2022	En el marco del proyecto de implementación MSPI adelantar el procedimiento de gestión de cambios en concordancia con los controles ISO 27001 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. 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 productivo. 14.2.4 Restricciones a los cambios en los paquetes de software. Incluir la valoración de la pertinencia de los cambios para el negocio: regulatorio, de valor misional, de valor no misional o de apoyo a la operación	Revisar con el grupo de subsistema que hacen parte del sistema integrado de la entidad, la articulación de la gestión de cambio e identificar la documentación asociada que se requiere para su implementación	Plan de gestión del cambio	Giselle Muñetón Emerson Cruz Sistema Integrado de Gestión	El proceso auditado aportó el documento "PROCEDIMIENTO GESTIÓN DEL CAMBIO" actualizado y publicado en el SGC el 10 de octubre de 2022 y el formato "FOGT18 FORMATO DE SOLICITUD Y GESTIÓN DE CAMBIOS (RFC)", el cual tiene versión y fecha del 10 de octubre de 2022, sin embargo, este documento aún no se encuentra publicado en el SGC. En la documentación aportada se evidencia la articulación del procedimiento con los controles ISO 27001 para llevar trazabilidad e impacto de los cambios solicitados. En el formato de solicitud se reitera incluir la valoración de la pertinencia de los cambios para el negocio, si es regulatorio, de valor misional, de valor no misional o de apoyo a la operación. El control de cambios según el procedimiento se solicita a través de la herramienta GLPI, donde se encuentra debidamente creada esta categoría. A la fecha de la auditoría no se evidencia ningún "FOGT18 FORMATO DE SOLICITUD Y GESTIÓN DE CAMBIOS (RFC)" diligenciado. Dentro de las evidencias se tiene relacionado el plan de Gestión de Cambio de la entidad, sin embargo, se avanzó en el procedimiento y en el formato pero no se ha formalizado el plan de Gestión de Cambio, por lo tanto, el hallazgo permanece abierto.	No se aportó el Plan de gestión de cambio, en su lugar se presentó avance en la actualización del "PROCEDIMIENTO GESTIÓN DEL CAMBIO" y el formato "FOGT18 FORMATO DE SOLICITUD Y GESTIÓN DE CAMBIOS (RFC)"	ABIERTO	EN PROCESO
67	61	Desarrollo y Adquisición de Software Aplicativo	1/02/2020	31/12/2022	Para los contratistas o funcionarios que desarrollen software, se recomienda suscribir una cesión de derechos patrimoniales a favor del Instituto. El auditor se permite adjuntar un modelo de formato de cesión para que sirva de base a la entidad: FORMATO CESION DERECHOS PATRIMONIALES_Borrador_INSOR.doc En todos los casos solicitar al contratista la documentación técnica del producto antes de la finalización de su contrato OBSERVACIÓN 2021: Ajustar el documento de "LICENCIAMIENTO DE SOFTWARE INSOR" para que diferencie claramente el caso de desarrolladores por encargo que deben ceder sus derechos patrimoniales a favor del Insor y referenciar el manual de imagen institucional en la sección de imagen corporativa y visibilidad. Igualmente diferenciar el licenciamiento en el caso de sistemas OnPremise de las modalidades SAS donde opera el concepto de formalidad de uso por suscripción	1. Elaborar , aprobar y publicar formato de cesión de derechos patrimoniales 2. Actualizar documento Licenciamiento de Software Insor	1. formato de cesión de derechos patrimoniales 2. Documento Licenciamiento de Software		En el documento "METODOLOGÍA PARA EL DESARROLLO MANTENIMIENTO DE SOFTWARE DEL INSOR", en el numeral 10 se hace referencia a los derechos patrimoniales que surjan de la producción intelectual de actividades propias de su contrato de funcionarios, contratistas o practicantes y su cesión a favor del INSOR. Al revisar los contratos de Carlos Molina, David Andrés Bello Pardo, Soledad Carolina Martínez Gamba, Cesar Augusto González Jiménez y Gerson Leonardo Barreto Flórez, se evidencia la existencia de la cláusula "VIGÉSIMA CUARTA- DERECHOS DE AUTOR" donde se especifica que el titular de los derechos patrimoniales de las obras que se produzcan con ocasión o en desarrollo del objeto del contrato serán del INSOR. La recomendación fue atendida, por lo tanto, el hallazgo se cierra.	Las evidencias relacionadas no fueron aportadas por el proceso auditado ni se encuentran en el SGC . Clausulados de contratos	CERRADO	ATENDIDO
70	63	Activos de Información, Mantenimiento y Mesa de ayuda	1/07/2020	31/08/2022	Establecer un procedimiento aplicable a todos los proveedores de sistemas de información que actualmente tienen acceso vía AnyDesk o VPN con los ambientes productivos del INSOR que incluya: • La disposición de un ambiente de QA (ambiente de pruebas con datos de prueba) para el cual se aísle el acceso de cada proveedor exclusivamente a este ambiente. • Monitoreo y supervisión de actividades durante la conexión, la cual solo debe otorgarse con previa autorización y en una franja de tiempo restrictiva previamente programada. • La gestión de cambios a sistemas mediante la entrega por parte del proveedor de un documento detallado de cambios (RFC) y los objetos impactados para efectos de que sea el responsable de infraestructura del INSOR quien ejecute los despliegues a ambientes productivos. Esta dinámica además de otorgar seguridad ofrece transferencia de conocimiento hacia el INSOR y disminución de la dependencia de conocimiento del proveedor OBSERVACIÓN 2021: Usar la funcionalidad de RFC de GLPI para llevar las pilas de producto y su trazabilidad.	1. Diseñar, elaborar e implementar un procedimiento para los proveedores de Sistemas de Información que requieren acceso remoto a los ambientes productivos del INSOR, así como la implementación de documento detallado de cambios. 2. Parametrización GLPI	1. Procedimiento y documento formato RFC 2. Incluir la funcionalidad de RFC de GLPI para llevar las pilas De producto y su trazabilidad.	1. Emerson Cruz Giselle Muñetón 2. Técnico de soporte Emerson Cruz	La primera parte de esta recomendación que es la elaboración de un procedimiento para el control de acceso remoto de los proveedores de los sistemas de información, no se ha adelantado y las evidencias y acciones relacionadas para el cumplimiento de la recomendación no son las pertinentes. Se debe entregar el procedimiento y la disposición del el ambiente de prueba para cada proveedor. Este procedimiento debe definir la supervisión y monitoreo que se realice cuando los proveedores se conecten remotamente y el control de la gestión de cambios a sistemas información por medio de documento detallado de cambios (RFC) creados específicamente para un cambio que afecte sistemas productivos y sirvan como insumo para verificar el impacto de los objetos en producción y correcta aplicación del cambio, además de poder realizar una reversión de los cambios en caso de presentarse alguna falla. Se evidencia que la gestión de cambios y manejos de RFC ya se encuentran implementados en la herramienta del GLPI, pero no se presenta evidencia de los ambiente de prueba (QA), ni se tienen identificadas la herramientas de monitoreo y supervisión de las actividades relacionados con el cambio, por lo tanto el hallazgo permanece en estado abierto		ABIERTO	EN PROCESO
76	122 .2	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/06/2021	30/11/2022	Google Workspace - Habilitar desde la consola del Google Worspace la configuración de verificación de dos pasos y su implementación obligatoria para los usuarios del correo electrónico. - Elaborar un manual o guía de la administración y gestión de cuentas de correo electrónico, en cuanto a configuración de parámetros, políticas de seguridad y protecciones desde la consola administrativa de Google WorkSpace	2. Elaboración de manual de administración y gestión de cuentas de correo electrónico con parámetros, políticas de seguridad de la consola de Google Works pace.	2. Manual administración y gestión de cuentas	Emerson Cruz	FECHA PROGRAMADA DE TERMINACION 30/12/2022. El proceso auditado atendió la recomendación elaborando el MANUAL ADMINISTRACIÓN Y GESTIÓN DE CUENTAS DE CORREO ELECTRÓNICO DESDE LA CONSOLA ADMINISTRATIVA (GOOGLE WORKSPACE) DEL INSOR	Manual Administración Y Gestión De Cuentas De Correo Electrónico	CERRADO	ATENDIDO
77	123	Activos de Información, Mantenimiento y Mesa de ayuda	1/06/2022	31/12/2022	Implementar el uso de herramientas gratuitas para los mantenimientos lógicos de los equipos que permitan comprobar el estado de salud y temperaturas de los discos duros (CrystalDiskInfo, HD Tune), estado de la memoria y procesadores (HWiNFO), de diagnóstico del pc (Glary utilities)	Implementar herramientas gratuitas en mantenimientos lógicos de equipos de cómputo	Uso de herramientas para mantenimientos lógicos	Técnico de soporte, Emerson Cruz	FECHA DE TERMINACION 31/12/2022 El proceso auditado aportó el INFORME MANTENIMIENTO LOGICO DE LOS EQUIPOS DE COMPUTO, donde se evidencia el uso de la herramienta HWinFo y Glary utilities para el mantenimiento lógico de los equipos, por lo tanto el hallazgo se cierra.	INFORME MANTENIMIENTO LOGICO DE LOS EQUIPOS DE COMPUTO	CERRADO	ATENDIDO
78	124	Activos de Información, Mantenimiento y Mesa de ayuda	1/06/2022	31/12/2022	Creación de las Matrices de cargos Vs Perfiles que establezcan los privilegios requeridos a servicios TIC de acuerdo con las funciones del cargo.	creación de las Matrices de cargos Vs Perfiles que establezcan los privilegios requeridos a servicios TIC de acuerdo con las funciones del cargo.	Matriz de cargos y perfiles con privilegios de servicios TI	Técnico de soporte, Emerson Cruz	TERMINACION PROYECTADA PARA EL 31/12/2022 No se presenta evidencia de atención a esta actividad. Se ha elaborado el documento : "MATRIZ DE ROLES Y RESPONSABILIDADES.xls", pero en esta se definen los roles y responsabilidades para los controles de navegación web y perfiles definidos en el firewall, el objetivo de esta matriz es el poder validar las configuraciones de permisos y perfiles de usuarios de acuerdo a su cargo en los sistemas de información, y se constituye como una herramienta para verificar que los usuarios estén configurados correctamente en los sistemas de información. Si bien el proceso auditado presenta evidencia de validación de permisos al momento de generar o actualizar los usuarios para los servicios de TI y en los sistemas de información de la Entidad en el procedimiento: "PRGT02 Procedimiento Gestión usuarios y contraseñas V2", aún no se cuenta con una matriz documentada para validar estos permisos. Se avanzó en la elaboración del formato matriz cargos Vs perfiles, sin embargo, aún no se ha definido los privilegios a los servicios TIC según el perfil. El hallazgo continua en estado abierto, la evidencia que se debe presentar para cerrar este punto es el documento con la matriz	MATRIZ DE ROLES Y RESPONSABILIDADES.xls MATRIZ CARGOSVSPERFILES	ABIERTO	EN PROCESO

12	29	Planeación y Organización de la Gestión TIC - Estructura Organizacional y Gobierno de TI	1/07/2019	31/03/2022	Implementar la suscripción de acuerdos de confidencialidad con terceros, contratistas o servidores públicos con acceso a información confidencial, reservada o sensible. El auditor se permite adjuntar un modelo de acuerdo de confidencialidad para que sirva de guía a la entidad - MODELO ACUERDO CONFIDENCIALIDAD.docx.	Elaborar modelo de acuerdo de confidencialidad	Modelo de Acuerdo de confidencialidad Publicado en SGC	Jefe Oficina Asesora de Planeación y Sistemas Oficina Asesora Jurídica	FECHA DE TERMINACIÓN 31/03/2022 El proceso auditado aportó los documentos "ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN (FUNCIONARIOS Y/O CONTRATISTAS)" y "ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN (PROVEEDORES DE TECNOLOGÍA)", en su versión 1, aprobados y publicados en el SGC el 14 de septiembre de 2021. La auditoría evidenció su aplicabilidad y uso en la suscripción de contratos con terceros, contratistas o servidores públicos. La recomendación fue atendida y la evidencia presentada es la adecuada, por lo tanto, el hallazgo se cambia a estado cerrado.	FOGT07 ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN (FUNCIONARIOS - CONTRATISTAS) FOGT08 ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN (PROVEEDORES DE TECNOLOGÍA)	CERRADO	ATENDIDO
13	30	Activos de Información, Mantenimiento y Mesa de ayuda	1/10/2019	31/07/2022	Incluir en las categorías de GLPI los incidentes y requerimientos a sistemas de información, crear los proveedores como agentes de soporte e iniciar la práctica de registrar los incidentes en la mesa de ayuda con el debido registro de tiempos de respuesta y solución (resuelto). Integrar a GLPI los GLPI Plugins que permitan aprovechar las funcionalidades liberadas para la herramienta tanto de registro, como de control y generación de reportes estadísticos (Dashboard). De ser posible incluir en la FORMA DE PAGO de los estudios previos sanciones relacionadas con el incumplimiento de los ANS durante el periodo que corresponde a cada pago.	1.Actualización documento ANS de la mesa de servicio GLPI 2. Parametrizar la Herramienta mesa de Servicios de acuerdo a la actualización de los ANS.	1.Parametrización de herramienta de mesa de ayuda 2.Documento actualizado ANS de la mesa de servicio GLPI	Emerson Cruz - Giselle Muñetón	En la revisión por parte de la auditoría de la configuración de los ANS en el GLPI, se videncia que ya se encuentran correctamente configurados y se incluyeron de forma adecuada las categorías de GLPI para los incidentes y requerimientos a sistemas de información. Se crearon como agentes de soporte los proveedores de los sistemas de información, de acuerdo a la recomendación emitida por la auditoría. Ya se encuentran implementadas las herramientas de panel de control, de informes estadísticos de casos y soportes en el GLPI. Por lo anterior se determina que la recomendación fue atendida y la evidencia presentada es la adecuada y el hallazgo se cambia a estado cerrado.	Imagen de la parametrización de ANS y proveedores como agentes en el GLPI. Imagen de panel de control (Dashboard) del GLPI.	CERRADO	ATENDIDO
18	33 .2	Planeación y Organización de la Gestión TIC - Plan de Administración de Riesgos y Contingencias	1/10/2019	31/07/2022	Se recomienda adelantar el ejercicio de identificación de riesgos de seguridad de la información orientado a activos críticos que en caso de materialización de amenazas afectan la continuidad de la operación y/o la disponibilidad, integridad y resguardo de la información. Tener en cuenta que los riesgos deben contemplar también los diferentes aspectos de la gestión TIC para garantizar que los controles de la norma han sido incorporados en los riesgos. Tal es el caso de los riesgos relacionados con la relación con terceros que no necesariamente se originan en activos tecnológicos, sino en debilidades contractuales o de control.	2. Actualización de la guía de administración del riesgo de la entidad en lo referente al tratamiento de riesgos de seguridad de la información (relacionar dominio 10 y 14)	2. Guía administración del riesgo de la entidad	Giselle Muñetón	El proceso auditado presentó a la auditoría el documento "FORMATO REGISTRO ACTIVOS DE INFORMACIÓN", el cual está actualizado y definida su criticidad. También actualizó la "GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO", versión 6, donde se incluyeron los dominios 14 y 15 del MSPI. La recomendación de la actualización de la Guía fue atendida, por lo tanto, el hallazgo se cierra.	GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO ACTUALIZADA FORMATO REGISTRO ACTIVOS DE INFORMACIÓN	CERRADO	ATENDIDO
25	36 .1	Planeación y Organización de la Gestión TIC - Plan de Administración de Riesgos y Contingencias	1/11/2019	30/11/2022	Actualizar los documentos "GUGT04 Guía para copias de seguridad_copia_no_controlada.pdf" y PRGT08 Procedimiento copias de respaldo de Información_copia_no_controlada.pdf a las condiciones actuales. OBSERVACIÓN 2021: - Incluir en la programación de copias de respaldo el Backup de los archivos de configuración de los sistemas manejadores de bases de datos (RDBMS), Backup de las bases de datos, las imágenes de los servidores físicos, configuraciones de switches, firewall routers, y en general de todas las configuraciones de los elementos activos de red." - Actualizar los documentos "GUGT04 Guía para copias de seguridad_copia_no_controlada.pdf" y PRGT08 Procedimiento copias de respaldo de Información_copia_no_controlada.pdf a las condiciones actuales. Incluir en la documentación del proceso registros de Planeación de copias de respaldo, de novedades de procesos y de restauraciones aleatorias en cumplimiento del objetivo de control 12.3 del MSPI.	1. Actualizar los documentos de copia de seguridad y establecer formatos, incluyendo los reportes de realización y restauración de copias de seguridad. 2. Dentro de la programación de copias de respaldo el Backup de los archivos de configuración de los sistemas manejadores de bases de datos (RDBMS), Backup de las bases de datos, las imágenes de los servidores físicos, configuraciones de switches, firewall routers	1. Documentos actualizados - 2. Programación copias de seguridad	Emerson Cruz - Giselle Muñetón	FECHA DE TERMINACION 30 DE NOVIEMBRE DE 2022 El proceso auditado avanzó en la actualización de los documentos GUIA PARA COPIAS DE SEGURIDAD", en su versión 2, actualizada y publicada en el SGC el día 10 de octubre de 2022 y MANUAL PARA RESPALDO Y RECUPERACIÓN DE DATOS DE LA INFRAESTRUCTURA TECNOLÓGICA", versión 1, aprobado y publicado en el SGC el 25/08/2022, donde definen el proceso y las generalidades para gestionar las copias de seguridad y la restauración de la información del INSOR y se creó el formato "REALIZACION Y RESTAURACION DE COPIAS DE SEGURIDAD", el cual aún no se encuentra publicado en el SGC. Con este formato se realiza la solicitud a través del GLPI de mesa de ayuda. Ya se encuentran implementadas y en funcionamiento la generación de copias de respaldo de las bases de datos y de las imágenes de los servidores físicos, configuraciones de switches, firewall router. Se entrega como evidencia la configuración y programación realizada para estas copias en la herramienta Veeam Backup utilizada para su generación. Se evidencia que se atendió la recomendación, por lo tanto, el hallazgo se cierra.	GUIA PARA COPIAS DE SEGURIDAD - MANUAL RESPALDO Y RECUPERACIÓN DE DATOS DE LA INFRAESTRUCTURA TECNOLÓGICA Configuración de copias de seguridad en la herramienta Veeam Backup FOGT17 Formato Restauración Copias Seguridad El Formato plan de copias de seguridad y novedades de restauración que se relaciona aún no se ha implementado	CERRADO	ATENDIDO
29	38	Planeación y Organización de la Gestión TIC - Plan de Administración de Riesgos y Contingencias	1/10/2019	31/12/2020	Reforzar la capacitación a los usuarios sobre las políticas de Backup	Generar campañas de sensibilización dirigidas a los usuarios sobre las políticas de Backup	Evidencias de la campaña	Oficina Asesora de Planeación y Sistemas	FECHA DE TERMINACIÓN 31/12/2020 En el documento entregado a la auditoría CronogramaCapacitacion.xls se evidencia la programación de capacitaciones en Backup y uso del Drive para los funcionarios del INSOR en los meses de noviembre y diciembre, donde la última sesión está programada para el 09 de diciembre de 2022. Además del cronograma también se aportó pantallazos de algunas sesiones de capacitación. Con el cumplimiento de este cronograma se cerraría esta recomendación. Esta actividad debe ser permanente dentro del plan de uso y apropiación de la entidad y debe ser parte del proceso de entrega de servicios tecnológicos a los nuevos funcionarios y/o contratistas. La recomendación fue atendida en su totalidad y por lo tanto el hallazgo se cierra.	Cronograma de capacitación Pantallazos de sesiones	CERRADO	ATENDIDO
30	39 .1	Planeación y Organización de la Gestión TIC - Políticas de seguridad	1/01/2020	1/12/2021	Continuar la implementación del modelo MSPI en tres proyectos paralelos: • La elaboración del marco documental de políticas, procedimientos, instructivos y formatos • Un programa de concientización, educación y capacitación sobre la seguridad de la información (control 7.2.2 ISO 27002:2013). • 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. OBSERVACIÓN 2021: - En la siguiente actualización del instrumento de evaluación MSPI, relacionar como evidencias los documentos evolucionados para cada control de MSPI y registrar el avance teniendo en cuenta que la implementación 100% de cada componente incluye: Planear, elaborar los instrumentos, implementar los controles, sensibilizar, evaluar efectividad y mejorar. - Una vez implementados los controles MSPI y los instrumentos definir métricas o indicadores de efectividad.	1. Actualizar la política de seguridad y privacidad de la información y por tanto la resolución 622	1. Resolución actualizada	Emerson Cruz - Giselle Muñetón	Se realizó de forma adecuada la actualización de la resolución 057 - 2021 (20de abril de 2021) , mediante la cual se actualiza la política de seguridad y privacidad de la información y se deroga la resolución 622 del 5 de diciembre de 2016. Por lo anterior, también se presenta a la auditoría evidencias de la actualización y publicación de la política de seguridad y privacidad de la información, dando cumplimiento a la recomendación, por lo tanto, el hallazgo se cierra.	Imagen resolución 057 2021 Política actualizada	CERRADO	ATENDIDO

34	41 .1	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/02/2020	31/08/2022	Cambiar todas las contraseñas de cualquier servicio expuesto sobre la red y ocultarlos para que no sea posible su visualización por parte de cualquier usuario sin autenticación en dominio. OBSERVACIÓN 2021: Se debe tramitar con el proveedor de Solgein la entrega de usuario y contraseña de la base de datos ya que ningún tercero debe tener acceso a los datos de producción de la Entidad, esto además de generar alertas de advertencia en la generación de las copias de seguridad, deja abierta la posibilidad de accesos directos a la base de datos al proveedor para alterar, copiar o eliminar información perteneciente a la Entidad y por ende incumplir con las políticas de seguridad del INSOR. - Tomar el control y conocimiento de las contraseñas de los sistemas de información las manejan los proveedores, esto genera un alto riesgo de dependencia y va en contra de la confidencialidad y seguridad de la informa de la Entidad, ya que el tercero tiene el control total de la información almacenadas en las bases de datos de estos sistemas de información.	1. Elaborar e implementar procedimiento para el cambio periódico de contraseñas en la de plataforma TI	1. Procedimiento elaborado, aprobado e implementado	Emerson Cruz - Giselle Muñetón	Se evidencia que han realizado correctamente el cambio de contraseñas de los servicios expuesto en la red. Se realizó la actualización del procedimiento:"PRGT02 Procedimiento Gestión usuarios y contraseñas_v2" entregado a la auditoría, en donde se hace referencia de forma adecuada al instructivo "ITGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION". En el procedimiento aportado, además de determinar el control de contraseñas de usuarios para los servicios y aplicaciones ofrecidos por el área, se adiciona un paso enfocado al control de contraseñas administrativas y su control mediante el instructivo de custodia mencionado . En el instructivo "ITGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION", se determina la administración y control de contraseñas criticas (administrativas) de forma adecuada y su custodia con el uso de la herramienta Kee Pass. Por lo tanto este hallazgo se ha atendido de forma adecuada, la evidencia es pertinente y puede cerrase.	PRGT02 Procedimiento Gestión usuarios y contraseñas_v2 TGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION	CERRADO	ATENDIDO
36	42 .1	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/06/2020	31/08/2022	Adicionar a la declaración de Aplicabilidad - Instructivo de Custodia contraseñas OBSERVACIÓN 2021: - Actualizar la declaración de aplicabilidad relacionando los instrumentos en cada caso. Ajustar la aplicabilidad de todos los controles. - Habilitar nuevamente las políticas de cambio periódico de contraseña y de reutilización, para todos los sistemas de información y servicios de TI (Dominio, correos electrónicos, etc.) y asegurar que se cambie siempre en el primer inicio de sesión.	1. Elaborar e implementar instructivo de custodia y gestión de contraseñas	1. Instructivo elaborado, aprobado e implementado	Emerson Cruz - Giselle Muñetón	Se entrega a la auditoria correctamente elaborado el instructivo "ITGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION", se determina la administración y control de contraseñas criticas (administrativas) de forma adecuada y su custodia con el uso de la herramienta Kee Pass. Se evidencia la correcta implementación de la gestión de contraseñas. Por lo tanto este hallazgo se ha atendido de forma adecuada, la evidencia es pertinente y puede cerrase.	TGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION"	CERRADO	ATENDIDO
37	42 .2	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/04/2022	30/11/2022	Adicionar a la declaración de Aplicabilidad - Instructivo de Custodia contraseñas OBSERVACIÓN 2021: - Actualizar la declaración de aplicabilidad relacionando los instrumentos en cada caso. Ajustar la aplicabilidad de todos los controles. - Habilitar nuevamente las políticas de cambio periódico de contraseña y de reutilización, para todos los sistemas de información y servicios de TI (Dominio, correos electrónicos, etc.) y asegurar que se cambie siempre en el primer inicio de sesión.	2. Declaración de aplicabilidad	2. Declaración de aplicabilidad	Emerson Cruz - Giselle Muñetón	En la declaración de aplicabilidad del MSPI entregada a la auditoría se hace referencia al instructivo en los controles respectivos del dominio A9 Control de acceso, sin embargo no se enuncian el procedimiento y el instructivo especifico. Se recomienda hacer referencia al instructivo específico en la declaración de Aplicabilidad y el instrumento de evaluación, sin embargo al existir un link a los documentos relacionados se pasa el hallazgo a estado cerrado.	PRGT02 Procedimiento Gestión usuarios y contraseñas_v2 TGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION Anexo - Declaración de aplicabilidad.	CERRADO	ATENDIDO
38	42 .3	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/04/2022	30/11/2022	Adicionar a la declaración de Aplicabilidad - Instructivo de Custodia contraseñas OBSERVACIÓN 2021: - Actualizar la declaración de aplicabilidad relacionando los instrumentos en cada caso. Ajustar la aplicabilidad de todos los controles. - Habilitar nuevamente las políticas de cambio periódico de contraseña y de reutilización, para todos los sistemas de información y servicios de TI (Dominio, correos electrónicos, etc.) y asegurar que se cambie siempre en el primer inicio de sesión.	3. Ajustar políticas de contraseñas en los sistemas e información	3. Políticas de contraseñas en los sistemas de información	Emerson Cruz - Giselle Muñetón	En las sesiones realizadas para la revisión de políticas de contraseña y control de accesos implementados en el correo y el directorio activo del INSOR se evidencia que están correctamente configuradas y se encuentran en funcionamiento. También se tiene correctamente configurado el cambio de contraseña al primer inicio de sesión.	Default Domain Policy (política de seguridad del dominio) Directiva Insor - políticas de seguridad implementadas para la entidad en el directorio activo de Windows.	CERRADO	ATENDIDO
39	43	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/06/2020	31/08/2022	De ser posible instalar un software para la administración y almacenamiento seguro de las contraseñas de administración	1. Elaborar e implementar instructivo de custodia y gestión de contraseñas 2. Declaración de aplicabilidad 3. Ajustar políticas de contraseñas en los sistemas e información	1. Instructivo elaborado, aprobado e implementado 2. Declaración de aplicabilidad 3. Políticas de contraseñas en los sistemas de información	Emerson Cruz - Giselle Muñetón	Ya se encuentra elaborado el procedimiento "PRGT02 Procedimiento Gestión usuarios y contraseñas V2" y el instructivo: "ITGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION", en el cual se determina el uso de la herramienta Kee Pass como software para la administración y custodia de contraseñas de administración. En la declaración de aplicabilidad del MSPI entregada a la auditoría se hace referencia al instructivo en los controles respectivos del dominio A9 Control de acceso, sin embargo no se enuncian el procedimiento y el instructivo especifico. Las políticas de contraseñas se encuentran correctamente configuradas en el directorio activo y en los correos de la entidad de acuerdo a las recomendaciones emitidas por la auditoría. Se debe complementar este hallazgo con la referencia especifica al procedimiento y guía especifica en la declaración de aplicabilidad. Se atendió la recomendación, por lo tanto el hallazgo se cierra.	ITGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION PRGT02 Procedimiento Gestión usuarios y contraseñas V2 Anexo - Declaración de aplicabilidad	CERRADO	ATENDIDO
40	44	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/06/2020	31/08/2022	Por ningún motivo exponer información de claves de acceso en archivos sin encriptación ni en correos.	Elaborar e implementar instructivo de custodia y gestión de contraseñas	Instructivo elaborado, aprobado e implementado	Emerson Cruz - Giselle Muñetón	Ya se encuentra elaborado el procedimiento: "PRGT02 Procedimiento Gestión usuarios y contraseñas V2" y el instructivo: "ITGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION", en el cual se determina el uso de la herramienta Kee Pass como software para la administración y custodio de contraseñas de administración. Se atendió la recomendación y las evidencias presentadas son pertinentes, por lo tanto, el hallazgo se cierra.	ITGT06 INSTRUCTIVO CUSTODIA Y GESTIÓN DE CONTRASEÑAS CRITICAS EN SISTEMAS DE INFORMACION PRGT02 Procedimiento Gestión usuarios y contraseñas V2	CERRADO	ATENDIDO
57	54	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/09/2019	31/07/2021	Configurar correctamente todos los clientes del antivirus para que no permita excluir archivos del análisis de virus ni quitarlos de la cuarentena	Aplicar las políticas de restricción para la gestión del antivirus	Evidencia de la política aplicada en consola de antivirus	Emerson Cruz	En las pruebas realizadas por la auditoria se evidencia que estas restricciones están implementadas y en correcto funcionamiento, todos los intentos de descargar software considerado como virus o peligroso, fue bloqueado por el antivirus y no permitió sacados de la cuarentena. La evidencia del la configuración de la política en la consola del antivirus no fue presentada debido a problemas de ingreso a la consola, pero debido a la comprobación de su funcionamiento, se evidencia que esta configurada de forma adecuada. La recomendación fue atendida e implementada correctamente y se pasa a estado Cerrado	Imagen de bloqueo a descargas de virus en las pruebas Imagen de evidencia de no permitir retirar archivos de la cuarentena	CERRADO	ATENDIDO
69	62	Activos de Información, Mantenimiento y Mesa de ayuda	1/09/2019	31/12/2022	Complementar el inventario de sistemas de información incluyendo todos los sistemas en uso estén o no alojados en la plataforma del INSOR, incluir igualmente sistemas autorizados de uso libre. Incluir en el inventario el soporte de la legalidad de uso del sistema de información. Estos elementos son insumo para el inventario de activos y para el desarrollo del dominio 18 del MSPI Cumplimiento	Actualizar el inventario de sistemas de información utilizados por el INSOR	Matriz de inventario y documentos de dominio de sistemas de información	Giselle Muñetón	Se adelantado la actualización del inventario de sistemas de información utilizados por el INSOR y se incluyeron en el Registro activos de información INSOR 2022 Consolidado criticidad.xls También se encuentran relacionados todos los sistemas de uso libre en el inventario de software de la herramienta GLPI. Se debe complementar la evidencia de esta recomendación con el informe de inventario de software generado desde el agente fusión Inventory del GLPI. La recomendación ha sido atendida y su estado pasa ha cerrado	Imágenes de la configuración y funcionamiento del agente de inventarios en el GLPI. Registro activos de información INSOR 2022 Consolidado criticidad	CERRADO	ATENDIDO

72	119	Activos de Información, Mantenimiento y Mesa de ayuda	1/06/2022	31/12/2022	Reanudar la implementación de agente fusión inventory en los equipos de usuarios que permita generar el inventario de software y hardware automáticos y actualizado, con información centralizada y permita la obtención de información histórica y estadística.	Realizar implementación de agente fusión inventory en la herramienta GLPI	Inventario de equipos de computo en GLPI	Técnico de soporte, Emerson Cruz	En la revisión de la herramienta de mesa de ayuda GLPI, se evidencia la correcta implementación del agente de inventarios de hardware y software automatizado: "Fusión Inventory" y su correcto funcionamiento, se evidencia que efectivamente está tomando los datos de los equipos de la entidad y se puede realizar seguimiento a los componentes de hardware de los equipos y el software instalado. Si bien ya se encuentra instalado y en funcionamiento el agente y se elaboró el procedimiento:"PRGT12 PROCEDIMIENTO DE LICENCIAMIENTO CONTROL DE SOFTWARE GLPI", se debe complementar con la definición y generación periódica de informes desde el GLPI, que permitan mantener el control del inventarios de hardware y licenciamiento de software, el seguimiento a la presencia y/o ausencia de software y hardware, la gestión de activos y configuraciones, hoja de vida de los equipos con su respectiva relación de software instalado, adicionalmente generar un procedimiento y manual de este control. La acción realizada es la adecuada y la recomendación fue atendida, se puede cerrar el hallazgo, sin embargo es importante que se complemente con la definición de informes periódicos, procedimientos y manuales de uso.	Imágenes de la configuración y funcionamiento del agente de inventarios en el GLPI. Imagen de Hoja de vida de Equipo de la Entidad, generada desde el GLPI. PRGT12 PROCEDIMIENTO DE LICENCIAMIENTO CONTROL DE SOFTWARE GLPI	CERRADO	ATENDIDO
73	120	Activos de Información, Mantenimiento y Mesa de ayuda	1/06/2022	31/12/2022	Luego de implementar el agente de inventarios habilitar el control de licenciamiento de software en el GLPI y generar un procedimiento y manual de este control.	Habilitar control de licenciamiento de software en el GLPI y generar procedimiento de control de licenciamiento	Procedimiento de control de licenciamiento	Técnico de soporte, Emerson Cruz	Se entrega a la auditoría el procedimiento: "PRGT12 PROCEDIMIENTO DE LICENCIAMIENTO CONTROL DE SOFTWARE GLPI", en el cual se definen correctamente los pasos que se deben seguir para el registro y control de licencias desde la herramienta del GLPI. Si bien la acción fue implementada correctamente se debe complementar con la apropiación y uso de la funcionalidad, debido a que en las sesiones se evidenció que si bien ya se tiene implementado el control y existe el procedimiento aún están en proceso de definición de informes a utilizar y se sigue llevando el control de licenciamiento de windows y office desde la herramienta proporcionada por Microsoft para este propósito. Deben complementar unificando y estandarizando este control desde la funcionalidad ya implementada, lo cual facilita el control y administración del licenciamiento. La acción fue ejecutada correctamente y por tanto el hallazgo se puede cerrar, se debe complementar con lo registrado en este seguimiento.	PRGT12 PROCEDIMIENTO DE LICENCIAMIENTO CONTROL DE SOFTWARE GLPI.	CERRADO	ATENDIDO
74	121	Activos de Información, Mantenimiento y Mesa de ayuda	1/06/2022	31/12/2022	Incluir el registro del cronograma de mantenimientos preventivos y el resultado de los mismos en la herramienta de mesa de ayuda con evidencias de las acciones realizadas.	Incluir cronograma de mantenimientos preventivo y resultado en la herramienta GLPI	Evidencia de cronograma de mantenimiento preventivo en GLPI	Técnico de soporte, Emerson Cruz	Se adelantó la planificación y registro del cronograma de mantenimiento preventivo desde la herramienta de mesa de ayuda GLPI de forma adecuada, se están registrando las acciones realizadas en esta planificación y se tiene un control de avance de las tareas realizadas durante el mantenimiento. Se debe complementar este punto con la relación de estos mantenimientos en las hojas de vida de los equipo en el GLPI, para poder validar y verificar acciones de mantenimiento preventivo La recomendación fue atendida de forma adecuada y el hallazgo puede cerrarse. Se debe complementar con lo indicado en este seguimiento como mejoramiento de la implementación.	Imagen de cronograma de mantenimientos preventivos implementado en el GLPI.	CERRADO	ATENDIDO
75	122 .1	Administración de accesos y Seguridad Lógica - Gestión de Accesos	1/03/2022	30/04/2022	Google Workspace - Habilitar desde la consola del Google Workspace la configuración de verificación de dos pasos y su implementación obligatoria para los usuarios del correo electrónico. - Elaborar un manual o guía de la administración y gestión de cuentas de correo electrónico, en cuanto a configuración de parámetros, políticas de seguridad y protecciones desde la consola administrativa de Google WorkSpace	1. Habilitar la configuración de verificación de dos pasos y su implementación en la consola de Google Worspace	1. Configuración consola Google Workspace	Emerson Cruz	En la revisión de la configuración de cuentas de correo electrónico desde la consola de Google Workspace, se evidencia que se tiene correctamente configurada la verificación de dos pasos para todos los usuarios con cuenta de correo del Insor, y su implementación obligatoria esta activada. Para la primera acción de este hallazgo, la implementación es adecuada y la evidencia e pertinente por lo cual su estado es cerrada.	Imagen de la configuración desde la consola de Google Workspace.	CERRADO	ATENDIDO