INFORME FINAL TRABAJO DE AUDITORÍA

Auditoria de Gestión con énfasis en riesgos evaluando la Oportunidad en la respuesta al desarrollo de los Proyectos de software

OFICINA DE CONTROL INTERNO

AUDITOR (ES):
LÍDER: FRANCISCO JAVIER PINTO GONZALEZ
Lead Auditor ISO27001:2013 registro ERCA No.1001545
CISM ISACA No. 221867531,
HSEQ, registro IAC No. GEC68940

REVISADO POR:
OLGA LUCIA VARGAS COBOS
JEFE OFICINA DE CONTROL INTERNO

BOGOTÁ, 21/05/2024

SECRETARÍA DISTRITAL DE SALUD

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Contenido

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Abreviaturas

- ITIL: Information Technology Infrastructure Library, que traduciría, Biblioteca de Infraestructura de Tecnologías de Información, lo cual es una guía de buenas prácticas para la gestión de servicios de tecnologías de la información.
- MIPG: Modelo Integrado de Planeación y Gestión
- POGD: Plan operativo de Gestión y Desempeño
- QA: Quality Assurance, que en español traduce “asegurar la calidad”
- SDLC: Systems Development Life Cycle, que en español traduce “ciclo de vida para desarrollo de sistemas”
- SGSI: Sistema de Gestión de la Seguridad de la Información
- TI: Tecnologías de la información
- WEB: World Wide Web que en español traduce “red informática mundial” o Sitio en Internet.

INTRODUCCION

En la actualidad las auditorias se convierte en una herramienta que las entidades utilizan, para conocer el estado actual de los procesos y productos, logrando determinar la eficiencia y la eficacia de los mismos por medio de una evaluación objetiva y metódica, que a su vez permite tomar decisiones y generar controles adecuados a las necesidades o debilidades identificadas. La auditoría especifica con énfasis en riesgo al procedimiento de gestión de soluciones de Software o desarrollo de software en la SDS, busca identificar las debilidades o falencias en el desarrollo software durante el ciclo de vida del mismo de acuerdo al procedimiento establecido, a fin de mejorar la capacidad de los mismos, mantener y darle continuidad a las prácticas que viene siendo exitosas y que han permitido al grupo de desarrollo en sus diferentes frentes o equipos, cumplir con los objetivos establecidos. De acuerdo a lo anterior, la auditoria se realizó bajo los siguientes marcos normativos para una evaluación integral desde diferentes frentes: ISO27001:2013: para evaluar la adquisición, desarrollo y mantenimiento de sistemas, ISO25000:2011: que permite evaluar la calidad del producto de software, ISO12207:2006: que define, controla y mejora los procesos del ciclo de vida del software, y PMBOOK: Metodología para Gestión de proyectos tradicionales y SCRUM: para la gestión de proyectos de software agiles. Se evaluó las fases del ciclo de vida de Software SDLC: Planificación y administración de requerimientos, diseño, implementación pruebas, despliegue y mantenimiento.

MARCO CONCEPTUAL

Se tuvo en cuenta el marco normativo vigente, que buscan proporcionar una guía para el desarrollo de software y los elementos esenciales para que sean implementados, permitiendo mejorar la calidad y productividad.

- **El ciclo de vida del desarrollo de software (SDLC):** Consiste en el paso a paso para la creación de un nuevo software desde la etapa de planificación inicial hasta la implementación y el mantenimiento a largo plazo. El software suele ser desarrollado por especialistas y es fundamental que cada persona que trabaje en el proyecto siga el mismo proceso o ciclo de vida, no seguir el procedimiento establecido, conlleva consistencias y sería casi imposible desarrollar un software exitoso y entregarlo al cliente en el tiempo acordado. El SDLC, da a cada proyecto un marco de trabajo y define un proceso ordenado, eficiente, en la procura de generar productos de software de alta calidad y a bajo costo.

- **Fases del Ciclo de Vida del Desarrollo de Software:** El ciclo de vida de desarrollo de software se compone de siete fases, cada fase cumple una función distinta y juntas proporcionan un framework o marco de trabajo para el desarrollo de software eficiente. Existen requisitos previos que deben cumplirse antes de que cada fase pueda comenzar o finalizar y estos se conocen como puntos de

entrada y puntos de salida. Todos los miembros o desarrolladores del equipo, deben seguir las fases de SDLC en orden secuencial para garantizar que el software se complete antes de la fecha límite del cliente. dichas fases son:

1. **Planificación y Análisis de Requerimientos:** Consiste en la recopilación de información del software que se desarrollará y para ello se debe conversar con el cliente para conocer el detalle del proyecto y luego identificar posibles riesgos, problemas y restricciones. El equipo de desarrollo, a menudo recibe aportes de múltiples partes interesadas y expertos. En esta fase, el equipo determina los costos y recursos que se requerirán para completar el proyecto.
2. **Definir requisitos:** Los requisitos del software se documentan en un documento de especificación de requisitos de software y estos deben ser aceptados por las partes interesadas antes de que el equipo de desarrollo pueda comenzar el proceso de diseño.
3. **Diseño y Prototipo:** Durante esta fase, toda la información recopilada en los dos pasos anteriores se reúne y el desarrollador comienza a diseñar la arquitectura del software.
4. **Desarrollo de software:** Esta fase es donde los desarrolladores comienzan a programar y dar vida al proyecto lo hacen utilizando una variedad de herramientas. El lenguaje de programación a utilizar dependerá de los requisitos del software.
5. **Pruebas de software:** Una vez que se completa el desarrollo del software, debe probarse para asegurarse de que cumple con los requisitos que se identificaron, las pruebas generalmente las realiza el equipo de control de calidad y pruebas de software comúnmente denominado QA y es aquí donde se realiza la comprobación de que no existan defectos en el código y que el software funcione de manera adecuada y entregado los resultados previstos. Si se encuentran defectos durante esta fase, el código se envía de vuelta al equipo de desarrollo para que lo corrijan o subsanen y esta fase continúa hasta que se corrigen todos los errores.
6. **Implementación del software:** Es aquí donde el software se entrega al cliente y se pone en uso.
7. **Operaciones y Mantenimiento:** Una vez que se implementa el software, el trabajo no ha terminado. Es probable que surjan problemas que no se detectaron durante la fase de prueba y durante la fase de mantenimiento continuo, los problemas que surgen se solucionan mediante actualizaciones y parches de software. También se pueden agregar nuevas características o funcionalidades que derivan en nuevos requerimientos y comienza nuevamente el ciclo.

- **Qué es la gestión de proyectos de software**: Es la capacidad de identificar, examinar y ajustar diferentes soluciones en el campo de las tecnologías de la información (TI), eligiendo la que mejor responda a los principios de calidad y eficiencia, para posteriormente ser llevada a la operación de acuerdo a la planificación y los objetivos determinados por la entidad.

La gestión de proyectos de software, consiste en una serie de actividades para la: planificación, programación, ejecución, seguimiento, administración de los recursos y presentación de proyectos de software, controlando y respondiendo de modo eficiente ante cualquier dificultad que surja en el ejercicio. Su principal objetivo es la de encaminar la labor de los desarrolladores de manera productiva, competente y que conduzca proyectos exitosos.
Una parte importante de los proyectos de software en la actualidad, es la gestión bajo metodologías Agiles, que corresponde a un enfoque de mejora continua que está transformando el desarrollo de proyectos de software, su principal objetivo es responder rápidamente a las necesidades del negocio. La principal característica que presentan los proyectos de software agiles, es que suelen seguir un ciclo de vida iterativo e incremental, y se adapta a los cambios y requerimientos en curso, lo que puede resultar en entregas más rápidas y frecuentes. En cambio, la gestión de proyectos tradicional sigue un enfoque lineal, secuencial, en donde cada fase debe completarse en su totalidad antes de pasar a la siguiente fase, lo cual no permite las entregas oportunas o tempranas de los productos y los cambios que se pudieran presentar, impactaran considerablemente el proyecto.

- ISO 27000-1:2013 (Desarrollos Seguros): Es la norma principal de la serie actualmente se actualizado a la versión 2022 y contiene los requisitos del sistema de gestión de seguridad de la información y en su Anexo A, se enumera en forma de resumen los objetivos de control y controles que desarrolla la norma ISO 27002:2022. Se tuvo en cuenta los apartados referentes a desarrollo seguro.

- ISO 25000:2014: Proporciona una guía para el uso de una serie de Normas internacionales denominadas Sistemas y requisitos de calidad del software y evaluación, el objetivo de ISO/IEC 25000:2014, es proporcionar una visión general de los modelos de referencia y definiciones comunes, así como la relación entre los documentos, lo que permite a los usuarios comprender la serie de estándares, de acuerdo con su propósito de uso.

- ISO 19011:2011: Proporciona orientación sobre sistemas de gestión de auditoría, incluidos los principios de auditoría, gestión de un programa de auditoría y realización de auditorías del sistema de gestión, así como orientación sobre la evaluación de la competencia de las personas en el proceso de auditoría.

- ISO 12207:2008: Establece un marco común para los procesos del ciclo de vida del software, con terminología bien definida, que puede ser referenciada por la industria del software. Contiene procesos, actividades y tareas que se aplicarán durante la adquisición de un producto o servicio de software y durante el suministro, desarrollo, operación, mantenimiento y eliminación de productos de software.

- **Metodologías Agiles:** el desarrollo ágil de software refiere a métodos de ingeniería del software basados en el desarrollo iterativo e incremental, estas metodologías son imprescindibles en un mundo en el que nos exponemos a cambios recurrentemente. Siempre hay que tener en cuenta como programadores que lo que es la última tendencia hoy puede que no exista mañana y por esto existe la metodología ágil donde los requisitos y soluciones evolucionan mediante la colaboración de grupos auto organizado y multidisciplinario. Se tuvo encuesta los lineamientos de la metodología de Scrum debido al enfoque y facilidad de administración de los proyectos, las entregas parciales “Sprint” y la relación entre el equipo de trabajo dado el seguimiento diario para lo que referente a los proyectos liderados por la Fábrica de software de la SDS.

- **ITIL:** Un conjunto de publicaciones de mejores prácticas para Gestión de servicios de TI. ITIL proporciona asesoramiento sobre la provisión de servicios de TI de calidad y de los procesos, funciones y demás capacidades necesarias para apoyo. El marco de ITIL está basado en el ciclo de vida del servicio y consiste en cinco etapas (estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio).

- **SPRINT:** Es una iteración o ciclo corto de desarrollo en Scrum, cuya duración máxima es de un mes.

1. OBJETIVO GENERAL DE LA AUDITORÍA (NIA 2210).

Verificar la gestión y los componentes de control (ambiente de control, actividades de control, gestión del riesgo, actividades de monitoreo e información y comunicación), en lo que respecta a la oportunidad en la respuesta en el desarrollo de los proyectos de software, con especial atención a los proyectos que contemplaron interoperabilidad entre los sistemas de información y se verificara el ciclo de vida del desarrollo del Software, así como el grado de satisfacción del usuario final respecto a los productos entregados. Así mismo, se realizará la evaluación y comparación de los requerimientos de software recibidos, atendidos y ejecutados, se identificarán errores presentados o modificaciones que conllevaron cambios o ajustes impactando las variables de alcance, tiempo y costo.

Por último, de manera transversal, se realizará la verificación al cumplimiento de las políticas de Seguridad Digital y Gobierno Digital del MIPG en lo que respecta al procedimiento de desarrollo de software.

2. OBJETIVOS ESPECÍFICOS DE LA AUDITORÍA. (NIA 2210).

- Evaluar el desarrollo de software a la medida en la SDS, Ciclo de Vida SDLC y procedimiento PR-001.
- Evaluar la oportunidad en la respuesta de los requerimientos hasta la entrega del producto.
- Evaluar el grado de satisfacción del usuario final frente al producto entregado.
- Validar el cumplimiento de las políticas de Seguridad Digital y Gobierno Digital en lo que respecta al procedimiento de desarrollo de software.
- Realizar test de seguridad mediante herramienta libre para análisis de vulnerabilidades WEB.

3. ALCANCE DE LA AUDITORÍA. (NIA 2220).

Contempla los siguientes elementos:

- Procedimiento de Gestión de Soluciones de Software – SDS-TIC-PR-001
- Ciclo de vida del desarrollo del Software – SDLC
- Gestión integral de los requerimientos de software mediante las herramientas dispuestas para ello.

Periodo a evaluar: Desde: 1/04/2023 Hasta: 31/03/2024

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

4. CRITERIOS DE AUDITORÍA. (NIA 2210- A3).

4.1 Internos: (políticas, normatividad interna, procedimientos lineamientos)

Para el desarrollo el presente ejercicio, se tuvo en cuenta los siguientes elementos:

Procedimientos, Lineamiento, guías:

- SDS-TIC-PR-001 GESTIÓN DE SOLUCIONES DE SOFTWARE
- SDS-TIC-LN-016 DESARROLLO SEGURO
- SDS-TIC-GUI-008 ESTÁNDARES DE DESARROLLO SOFTWARE EN LA SDS
- Modelo-223 ANÁLISIS Y DISEÑO DE SISTEMAS DE INFORMACIÓN

Instructivos:

- SDS-TIC-INS-002 BACKUP Y CUSTODIA DE MEDIOS MAGNÉTICOS
- SDS-TIC-INS-004 CONTROL DE CAMBIOS
- SDS-TIC-INS-009 IMPLEMENTACIÓN DE DESARROLLO EN AMBIENTE DE PRODUCCIÓN
- SDS-TIC-INS-010 INSTRUCTIVO PARA EL PROCESO DE ANALISIS Y DISEÑO DE SOFTWARE
- SDS-TIC-INS-011 IMPLEMENTACIÓN DE DESARROLLO DE SOFTWARE EN AMBIENTE DE PRUEBAS

Formatos:

- SDS-TIC-FT-005 CONCEPTO TÉCNICO DE PRUEBAS
- SDS-TIC-FT-015 PLAN DE PRUEBAS
- SDS-TIC-FT-016 IMPLANTACIÓN PROYECTOS DE SISTEMAS DE INFORMACION
- SDS-TIC-FT-023 SOLICITUD DE NUEVAS APLICACIONES O MANTENIMIENTO DE SOFTWARE
- SDS-TIC-FT-024 SOLICITUD DE CALIDAD DE SOFTWARE (PRUEBAS) DE APLICATIVOS
- SDS-TIC-FT-050 CRONOGRAMA PARA ANÁLISIS DE VULNERABILIDADES DESARROLLO DE SOFTWARE
- SDS-TIC-FT-057 MATRIZ DE SEGUIMIENTO A USUARIOS INSATISFECHOS

4.2 Externos (leyes y regulaciones que apliquen): Para el desarrollo el presente ejercicio, se tuvo en cuenta los siguientes marcos normativos y mejores prácticas:

ISO27001:2013: evalúa la adquisición, desarrollo y mantenimiento de sistemas
ISO25000:2011: evalúa la calidad del producto de software
ISO12207:2006: define, controla y mejora los procesos del ciclo de vida del software
PMBOOK: Metodología para Gestión de proyectos Tradicionales
SCRUM: Metodología para proyectos agiles

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

5. METODOLOGÍA UTILIZADA. (NIA 2300).

La presente auditoría se desarrolló mediante la realización de mesas de trabajo presencial y virtual con los diferentes referentes designados, verificando la conformidad de los criterios y requisitos de las listas de verificación elaboradas. Es clave mencionar que, de acuerdo al inventario entregado, se realizó la selección de casos o requerimientos de acuerdo a ciertos criterios, esto con el fin de realizar el análisis de la información en cada una de las fases del ciclo de vida y basado en el procedimiento existente, así como: registros documentales, matriz de riesgos, autoevaluaciones, entre otros, Las mesas de trabajo fueron agendadas acorde a la programación establecida.

Adicionalmente el auditor se tuvo en cuenta los siguientes aspectos:

Revisión de la documentación: El auditor solicitó recopilo y revisó la documentación suministrada con respecto al procedimiento en cuestión, guías, registros de actas entre otros documentos.

Consultas con el personal designado: El auditor realizó consultas específicas a los funcionarios designados del proceso y consulto entre otras cosas piezas comunicativas elaboradas, con el fin de conocer el nivel de concientización frente al proceso de desarrollo de software en la entidad.

Listados de verificación para los auditados: El auditor entrega la lista de requisitos de revisión, la cual se diligenció en compañía de los referentes designados y personal que acompaño el ejercicio. Estos listados serán una imagen cualitativa y cuantitativa del nivel de madures del ciclo de desarrollo de software en la entidad basado en las normas ya mencionadas.

6. ANÁLISIS DE INFORMACIÓN Y DE DATOS. (NIA 2320).

La presente auditoria, se llevó a cabo mediante recolección de información de diferentes fuentes, entrevistas, listas de chequeo, matriz de riesgos, encuestas, entre otros documentos, que permitieron conocer el procedimiento y las prácticas utilizadas, los resultados fueron analizados con el fin de determinar posibles hallazgos, evidenciando las causas que las originan y proponiendo alternativas que permitan mitigarlos, dichos resultados serán presentados serán presentados a lo largo del informe.

6.1 Esquema de líneas de defensa

A continuación, el análisis por línea:

TEMAS REVISADOS	ASPECTOS VERIFICADOS
6.1.1. Ambiente de control: Es el conjunto de procesos y estructuras que proveen las bases para llevar a cabo el control interno a través de la organización	Contemplo la revisión del procedimiento operativo, instructivos, guías y demás controles definidos, al fin de brindar un cubrimiento general de cara a la gestión de soluciones de software, dichos elementos permitieron llevar a cabo una revisión integral por parte de la oficina de control interno.
6.1.2. Actividades de Control (incluye la revisión de políticas de operación procedimientos, normatividad interna y externa, Plan Operativo Anual	1. Se verifico y evaluó el cumplimiento bajo los siguientes marcos normativos: ISO27001:2013: para evaluar la adquisición, desarrollo y mantenimiento de sistemas, ISO25000:2011: que permite evaluar la calidad del producto de software, ISO12207:2006: que define, controla y mejora los procesos del ciclo de vida del software, PMBOOK: Metodología para Gestión de proyectos tradicionales SCRUM: para la gestión de proyectos de software agiles y se evaluó las fases del ciclo de vida de Software SDLC: Planificación y administración de requerimientos, diseño, implementación pruebas, despliegue y mantenimiento. 2. A nivel de control se tuvo en cuenta el procedimiento SDS-TIC-PR-001, instructivos y documentación complementaria que hacen parte del repositorio de información documental evaluados para este alcance. 3. Se evaluó mediante encuesta, el nivel de percepción frente a los requerimientos finalizados. Mayor detalle se podrá consultar en el numerales: 6.2, 6.3, 6.4, 6.5, 6.6 y 6.7 del presente documento.

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

6.1.3. Evaluación del Riesgo y controles (incluye análisis de contexto, riesgos relacionados identificación de controles y su operación, posibles riesgos detectados)	En materia de Seguridad Digital, la SDS adopta la implementación de la política del Modelo de Gestión de Riesgos de Seguridad Digital desarrollado por Min Tic, que adopta las siguientes fases: Identificar, gestionar, tratar y mitigar los riesgos de seguridad digital. El proceso TIC, cuenta con matrices de riesgos de proceso, de corrupción y de seguridad de la información, esta última, relacionada con la implementación de la política de seguridad digital, ya que la matriz cuenta con 3 riesgos identificados para el manejo de la confidencialidad, integridad y disponibilidad de la información, dichos riesgos se gestionan periódicamente de acuerdo a lo establecido en el POGD. Con relación a lo anterior, el proceso cuenta con matrices de riesgo, donde se evalúan los riesgos y se establece el riesgo inherente y riesgo residual, así como el plan de tratamiento. Adicionalmente, se cuenta con las matrices de autoevaluación para determinar si el riesgo se ha materializado a partir del seguimiento de los diferentes controles establecidos. En lo que respecta a los riesgos de proceso, se informa que a principios de año 2024, se llevaron a cabo las mesas de trabajo para la revisión de los riesgos asociados con el desarrollo de soluciones de software y se tiene establecido para esta vigencia, la revisión trimestral. Al consultar la matriz de riesgos, el ID: 4, consta de 3 controles, los cuales se encuentran asociados con las primeras fases del procedimiento SDS-TIC-PR-001. El riesgo asociado se describe así: “Posibilidad de afectación económica y reputacional por el desarrollo que no cumpla con las especificaciones técnicas del correcto levantamiento de los requerimientos”. El primer control está basado en el formato SDS-TIC-FT-023 y es aquí donde se definen y establecen los requerimientos y necesidades por parte del solicitante, que pudiera tener ajustes o aclaraciones resultado de las mesas de trabajo particulares, el tercer control tiene que ver con la verificación de los requisitos al final para cada proyecto de software y como resultado de la eficacia de los controles establecidos, se cuentan documentos o formatos codificados SDS-TIC-FT-023, que definen los requerimientos de usuario. En ultimas, lo que no este escrito, no será desarrollado y hará parte de un nuevo requerimiento.
6.1.4. Actividades de monitoreo (incluye las acciones que la primera y segunda línea de defensa ejercen para mitigar la ocurrencia de los riesgos sean este seguimiento al cumplimiento de políticas, actividades, directrices, metas)	Se llevó a cabo la verificación y el resultado fue el siguiente: **Primera Línea (Autocontrol):** • **Implementar acciones correctivas:** Se consultan las acciones registradas en el aplicativo isolucion, producto de las auditorías realizadas y acciones de mejora que, de acuerdo a lo informado, la mayoría han sido implementadas y se comprobó su eficacia. • **Ejecutar procedimientos de riesgo y control:** El gestor de calidad informa, que el monitoreo de los controles es una tarea constante que se realiza cada trimestre, mediante el instrumento de autoevaluación se logra. identificar, evaluar, controlar y mitigar los riesgos de la gestión de soluciones de

	software y mediante la verificación realizada a las fuentes de información suministradas, se identifican registros de riesgos identificados, así como la valoración cualitativa de los mismos. **Segunda Línea (Autoevaluación):** • Aseguran que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente. • Supervisan la implementación de prácticas de gestión de riesgo eficaces por parte de la gerencia. **Resultado**: Mediante la verificación realizada a las fuentes de información proporcionada, se evidencian matrices de registros de riesgos con su plan de tratamiento de riesgos, el cual se viene implementando.
6.1.5. Información y comunicación	• Se verifico el proceso, procedimientos, registros e información compartida, así como los diferentes aplicativos utilizados para la gestión y control de requerimientos. • Se consultaron diferentes piezas comunicativas que reflejan las campañas de sensibilización desarrolladas respecto a conceptos, prácticas y recomendaciones frente a la gestión de soluciones de software. • Se cuenta con el rol de gestor de calidad, que tiene como responsabilidad, multiplicar o replicar los conocimientos adquiridos a los colaboradores de la dirección TIC. • Se cuenta con registros de actas de reuniones de revisión por la dirección, Comité técnico y comité institucional de Gestión y desempeño como mecanismos de comunicación de los diferentes temas a los interesados.

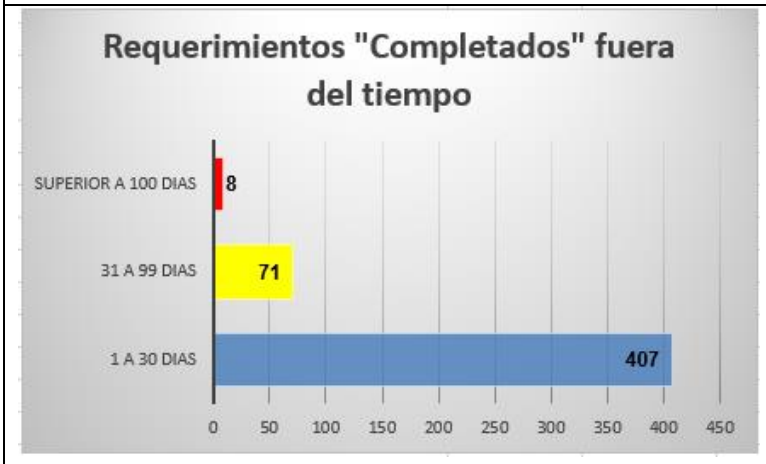
Una vez realizado el análisis de información mediante la base de datos suministrada de gestión requerimientos de software por medio del aplicativo PLANNER, encontramos los siguientes resultados:

6.2 Análisis de requerimientos gestionados para software

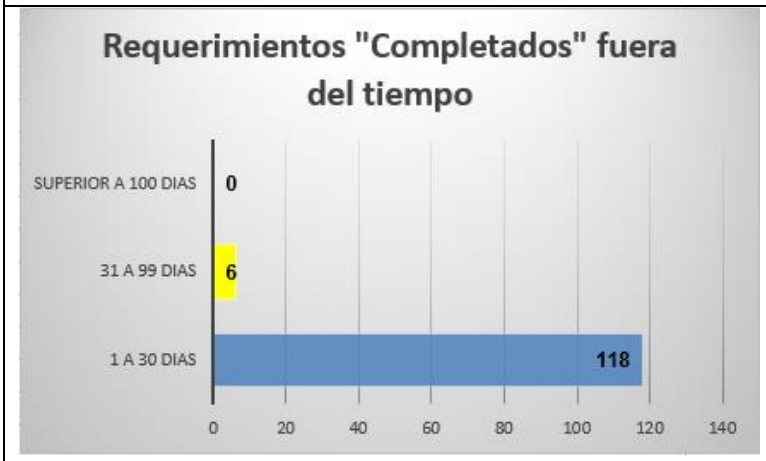
La tabla que a continuación se presenta, identifica el número de requerimientos de software que han sido recibidos mediante el formato-023. Es clave mencionar que los casos analizados, corresponden al intervalo del mes de marzo año 2023 al mes de abril 2024, que corresponden a un total de 2670 requerimientos de los cuales, 2608 es decir el 98% de estos requerimientos, se encuentran en estado: “completados”, mientras que 59 de los requerimientos, es decir el 2,2%, se encuentran con estado: “En Curso” y 3 requerimientos, se encuentran “sin iniciar”.

Estado	Completada	En curso	No iniciado	Total general
⊟2023	1855	19	1	1875
3	136	1		137
4	166			166
5	239			239
6	199			199
7	162	1		163
8	181			181
9	185	1		186
10	164	2		166
11	177	2		179
12	246	12	1	259
⊟2024	753	40	2	795
1	248	7		255
2	259	16	1	276
3	229	2		231
4	17	15	1	33
Total general	**2608**	**59**	**3**	**2670**

6.2.1. Análisis de los requerimientos en estado: “Completados”

	La grafica representa la totalidad de requerimientos en estado “completados” en el periodo de marzo a diciembre del año 2023 y cada porción de la torta representa un segmento del tiempo en la completitud de los mismos, en otras palabras, la completitud o finalización, se dio antes, durante y después de la fecha acordada. El total de requerimientos en el periodo fue de 1855, de los cuales el 26% de estos, corresponden a requerimientos que superaron la fecha comprometida, es decir, finalizaron fuera del tiempo, afectando la fecha comprometida con el cliente. La grafica que se presenta a continuación, representa el tiempo adicional utilizado para la finalización de los proyectos o requerimientos.
	Total, de requerimientos “completados fuera de tiempo” en el intervalo de marzo a diciembre del año 2023 fue de 486, de los cuales el 16% de estos casos, superaron el tiempo de entrega a más de 30 días y resaltamos que 8 casos de estos, la entrega fue superior a 100 días, lo cual constituye una no-conformidad, ya que existe un incumplimiento con respecto al compromiso en diferentes requerimientos.

A continuación, se representa el paralo de un año a otro.

	La grafica representa la totalidad de requerimientos en estado “completados” en el periodo de enero a abril del año 2024 y cada porción de la torta representa un segmento del tiempo en la completitud de los mismos, en otras palabras, la completitud o finalización, se dio antes, durante y después de la fecha acordada. El total de requerimientos en el periodo fue de 753, de los cuales el 16% de estos, corresponden a requerimientos que superaron la fecha comprometida, es decir, finalizaron fuera del tiempo, afectando la fecha comprometida con el cliente. La grafica que se presenta a continuación, representa el tiempo adicional utilizado para la finalización de los proyectos o requerimientos.
	El total de requerimientos “completados fuera de tiempo” en el intervalo de enero a abril del año 2024 fue de 124, de los cuales el 5% de estos casos, superaron el tiempo de entrega a más de 30 días, lo cual constituye una no-conformidad, ya que existe un incumplimiento con respecto al compromiso.

A continuación, como evidencia se relaciona la tabla de los requerimientos que superaron más de 100 días para el conocimiento del lector.

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

id	Nombre de la tarea	Nombre del depósito	Asignado a	Fecha de inicio2	Fecha de vencimiento	Fecha de finalización	Tiempo de Retrazo (días)
1	RIAS - Apoyo en el proceso de seguimiento al proceso del contrato de RIAS	SIRC	Miembro	5/05/2022	07/03/2023	22/09/2023	199
2	SICAI -QA_SICAI_1.9.0 - procesos de investigación que se realizan en las SISS	SICAI	Claudia Patricia, Ruiz	9/08/2023	16/08/2023	06/02/2024	174
3	Licencia RX Veterinarias- 2022IE14359- Habilitar parametro al usuario validador "Programar visita tecnica"	TRA-12 Licencia de equipos RX Veterinaria	Segundo Jesus, Neira Guio	15/03/2022	15/03/2023	10/08/2023	148
4	SISEM - DUESCorreo02062022- Sistema propio de información para realizar las actividades de seguimiento,	SISEM	Javier Enrique, Mejia Reinoso	2/06/2022	31/10/2023	05/03/2024	126
5	SIVIGILA DC - QA_SIVIGILA DC_210.164.0 - Modulo Sistema de vigilancia epidemiológica ambiental - Establecimientos	SIVIGILA DC	Jose Oscar, Ramos Rivera	18/01/2023	01/03/2023	29/06/2023	120
6	Autorregulación - SVSCorreo17042023 Q.A 2.2.0 - Ajustar funcionalidad de los botones	Trámites en línea	Segundo Jesus, Neira Guio;Erick Fabian, Torres Aguirre	17/04/2023	03/05/2023	30/08/2023	119
7	Tramites en linea RX- 2022IE32091- Ajuste Modulo Licenciamiento de Practica Medica Rayos X Categoria I y II	TRA-11 Licencia de equipos RX	Segundo Jesus, Neira Guio	29/12/2022	28/07/2023	23/11/2023	118
8	SIIAS - 2022IE31660 Q.A 1.69.0 - Art. 51	SIIAS	Eduardo, Hernandez Gomez;Javier Alberto, Martinez Leiva;Claudia Patricia, Ruiz Sanchez	29/11/2022	06/12/2023	21/03/2024	106
9	CIP - 2023IE10614 Q.A 4.4.0 - Ajuste aplicativo 4.3.3 en pro de mejorar las salidas de informacion	CIP	Erick Fabian, Torres Aguirre;Diana del Pilar, Correcha Vasquez	26/04/2023	23/05/2023	24/08/2023	93

Fuente: planner

6.2.2. Análisis de los requerimientos en estado: "en Curso":

Al consultar la tabla maestra y realizando el filtro correspondiente en el campo de "fecha de vencimiento" valor año 2023, encontramos 19 requerimientos, que presentan retrasos significativos, ya que existen requerimientos desde el año 2020 hasta el año 2023 que no han sido resueltos.

A continuación, se presenta lo informado:

Req. registrados que ya vencieron y siguen en CURSO	
Año	**# de Casos**
2020	1
2021	3
2022	8
2023	7

A continuación, como evidencia se relaciona la tabla de los requerimientos que se encuentran con atrasos significativos. Adicionalmente, resaltado en color azul, los requerimientos que fueron objeto de una revisión detallan en las mesas de trabajo.

la gestión realizada por el equipo de mantenimiento

Fuente: planner

Tramite 35 es una opa Certificado de discapacidad y registro para la localizacion y localización de personas con discapacidad Migracion	Trámites en línea	Media	Segundo Jesus, Neira Guio	10/07/2023	30/12/2023	173	130
Licencia de equipos de RX veterinario - SIVCcorreo26072023- Complementar opciones con las que cuenta el ciudadano para efectuar	TRA-12 Licencia de equipos RX Veterinaria	Media	Segundo Jesus, Neira Guio	26/07/2023	15/12/2023	142	145
SIIAS - DFcorreo06092023 Q.A 1.68.0- Pasarela Tu Compra	SIIAS	Media	Martha Ligia, Suarez Rojas;Claudia Patricia, Ruiz	06/09/2023	30/12/2023	115	130
Tramites en linea RX- 2023IE21271 Q.A 2.0.0- Puesta a punto del modulo de expedicion de licencias de RX	TRA-11 Licencia de equipos RX	Media	Segundo Jesus, Neira Guio;Jose Oscar, Ramos Rivera	01/09/2023	19/12/2023	109	141
Labvantage - SVSCorreo27062023- Modulo de Redes LabVantage de laboratorio	LABVANTAGE	Media	Segundo Jesus, Neira Guio	24/08/2023	30/11/2023	98	160
LITERALMENTE- QA_LITERALMENTE_1.1.0- Realizar la revisión del sitio, su funcionamiento y	Apoyo	Media	Erick Fabian, Torres Aguirre	19/09/2023	26/09/2023	7	225

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

De acuerdo al análisis de los datos presentados, existen incumplimientos continuos con respecto a la fecha comprometida de entrega con el cliente, ya que existen requerimientos de más de 1 año o 2 años que siguen sin finalizar, afectando los objetivos estratégicos que como entidad se han trazado de cara al plan de desarrollo y en lo que respecta a los procesos misionales, las necesidades no han sido resueltas en los tiempos acordados. De acuerdo a lo anterior, se declara una no-conformidad que deberá ser subsanada por el proceso.

Es clave mencionar que, el caso del requerimiento o proyecto identificado como “SIGEME-Q-2021IE35391”, que se registra en el cuarto lugar de la tabla anteriormente presentada, se evidencia un atraso de más de 3 años, ya que dicho requerimiento se recibió e inicio en el año 2021 y de acuerdo a lo informado en el desarrollo del mismo, se agotaron los recursos u horas hombre para desarrollo por parte de la Fábrica de Software, por tal motivo, el proyecto tuvo que detenerse, hasta tanto no se adjudicara el nuevo contrato con la fábrica de software de ETB, el requerimiento o proyecto ha sido escalado reiteradamente en diferentes instancias, existen registros de actas y acuerdos establecidos con la dirección TIC con sus diferentes representantes, aclarando que la dirección TIC en el periodo comprendido del proyecto, ha tenido diferentes directores y se han acordado y estableciendo cronogramas de trabajo que han sido incumplidos reiteradamente y a la fecha de la presente auditoria aun sigue sin finalizar. Dicha situación se replica en otros casos y por tanto se deberán tomar los correctivos que haya lugar.

Análisis de requerimientos “en curso” que vencieron en el año 2024

Al realizar el filtro mediante el campo de “fecha de vencimiento” año 2024, identificamos 40 requerimientos, que reflejan retrasos, ya que existen requerimientos desde el año 2020 hasta el año 2023 que no han sido culminados o finalizados.

A continuación, se presenta lo informado:

Req. registrados que ya vencieron y siguen en CURSO	
Año	**# de Casos**
2020	1
2021	4
2022	10
2023	16
2024	9

A continuación, como evidencia se relaciona la tabla de los requerimientos que se encuentran con atrasos.

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Nombre de la tarea	Nombre del depósito	Fecha de inicio	Fecha de vencimiento	Duracion del proyecto hasta el Vencimiento	Retrazo en dias
SISETMI - DPScorreo12112020 QA 1.0.6 - Sprint 1 - Aplicativo para realizar seguimiento casos de transmisión materno infantil, sífilis gestacional	SISETMI	12/11/2020	12/04/2024	1247	26
SICAI - correo16032021- procesos de investigación	SICAI	16/03/2021	09/01/2024	1029	120
PAMEC - DCSScorreo22082021- Nuevo aplicativo	PAMEC	22/08/2021	15/02/2024	907	83
SAEVAD - Seguridad al paciente - SCSScorreo22082021- Crear aplicativo	SAEVAD - Seguridad al paciente	22/08/2021	15/02/2024	907	83
Transporte SDS - 2021IE28072- Aplicación nueva	TRANSPORTABILIDAD	07/10/2021	29/01/2024	844	100
SIRC -2022IE3835 Q.A 3.49.0- Actualización aplicativo SIRC según normatividad vigente	SIRC	15/02/2022	15/02/2024	730	83
SIVIGILA DC - 2022IE8795- Diagnostico aplicativo SIVIGILA DC modulo SISVEA	SIVIGILA DC	07/04/2022	28/02/2024	692	70
Trámites en línea - 2022IE7523 Q.A 1.0.0 - Virtualización trámite de inhumación y cremación	TRA-13 Inhumación	31/03/2022	20/02/2024	691	78
Tramites en Linea-2022IE10131-Nuevo tramite ETB modulo Autorizacion renovacion,ampliacion de distribucion de medicamentos	TRA-25 Modulo Autorizacion renovacion,ampliacion de distribucion de medicamentos	03/05/2022	28/02/2024	666	70
SALUDATA - 2022IE1681- Optimizar la operacion de SaluData y la experiencia del usuario	SALUDATA Fabrica	09/05/2022	28/02/2024	660	70
Red Sangre - 2022IE14698- Ajustar módulo de promoción de la donación	Red Sangre Fabrica	09/06/2022	08/03/2024	638	61
SICAB - 2022IE19402- Desarrollo e implementacion del sistema de informacion de cancer en Bogotá	SIAATH	29/07/2022	19/04/2024	630	19
INTRANET - SALUDATA - 2022IE24820- Solucion informatica para el control de acceso a informacion confidencial	SALUDATA Fabrica	14/09/2022	28/02/2024	532	70
Autorización de Títulos - 2022IE21749- Mejora tramite en cuestion de agilidad y oportunidad Tramite 19	TRA-19 Registro de autorizacion de titulos	16/08/2022	29/01/2024	531	100
SIVIGILA DC - DEAGcorreo14102022 Q.A 210.157.3_210.165.0- Desarrollo en SISVEA que permita interoperabilidad con Labvantage	SIVIGILA DC	14/10/2022	30/01/2024	473	99
SEP002_APOYO_CXP_CONSECUTIVO DE PAQUETES EN MÓDULO CXP	CXP	21/01/2023	30/04/2024	465	8
SIIAS - 2022IE35628 Q.A 1.0.0- Interfaz SIIAS - LIMAY	SIIAS	23/01/2023	15/02/2024	388	83
Línea 106 - SDSCORREO10012022- Actualizar el Sistema de información	Línea 106	10/01/2023	17/01/2024	372	112
ABR002_APOYO_SISCO_Formato creación de opciones menú	SISCO	05/05/2023	30/04/2024	361	8
JUN005_APOYO_ADMUSER_Revisión de funcionalidad y ajuste cuentas con caducidad	ADM USER	05/06/2023	30/04/2024	330	8
JUL009_APOYO_PREDIS_CAMBIAR LA FIRMA DEL RESPONSABLES DE PRESUPUESTO-ANULADOS	PREDIS	26/07/2023	30/04/2024	279	8
Ambiente Digital - SGTPCorreo14062023 - Reporte ciudadano	TIPS Digitales	14/06/2023	21/02/2024	252	77
PAI 2.0 - 2023IE17358 - Actualización del servicio web con el sistema información SAP	PAI	17/07/2023	01/03/2024	228	68
Trámites en línea - VSP - dispositivos médicos (visual y ocular)	TRA-05 Visual y Ocular	06/07/2023	15/02/2024	224	83
OCT003_DESARROLLO_CXP_PLANILLA DE CONTRATISTAS NOVEDADES - CUMPLIDOS 2023	CXP	12/10/2023	30/04/2024	201	8

De acuerdo a la tabla y el análisis realizado, existe un porcentaje de requerimientos que han sido objeto de incumplimientos reiterativos respeto a la promesa de valor con cliente,

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

en otras palabras, se incumplió con la fecha comprometida de entrega con el cliente, ya que identificamos requerimientos de más de 1 año que siguen sin finalizar y los profesionales argumentan que esto es debido a que el proceso es tan dinámico, transversal y critico que van surgiendo nuevos requerimientos que deben ser priorizados y por consiguiente afectan e impactan los tiempos ya acordados de requerimientos previos. Por lo anterior, requerimientos que fueron suspendidos o detenidos, no cambian de estado en la herramienta generando desinformación. De acuerdo a lo anterior, se decreta la no-conformidad por incumplimiento a los tiempos comprometidos para múltiples requerimientos.

6.3 Requerimientos o proyectos de software que involucran INTEROPERABILIDAD

¿Qué es Interoperabilidad?

Es la capacidad de los sistemas de información de compartir datos o intercambiar información y conocimiento entre ellos. Permite comunicar diferentes sistemas con datos en diferentes formatos de modo que la información pueda ser compartida, accesible desde distintos entornos y comprendida por cualquiera de ellos. En el caso en la secretaria de Salud, existen proyectos de interoperabilidad en operación y otros en curso de desarrollo. A continuación, por medio del inventario de requerimientos consolidado, se detallan los casos consultados:

1. Requerimiento de nombre: **SICAPITAL ERP- TICCorreo07062022**, que consiste en la Integración de la plataforma de Facturación electrónica y el SI-CAPITAL. **Estado:** En curso, se explica que debido a la contingencia por las fallas en la prestación de los servicios TIC, se perdió la interoperabilidad entre el web service y facturación electrónica. Adicionalmente, se informa además que el proyecto lo retoma un ingeniero de curva administrativa de la dirección TIC, ya que el contrato con la fábrica de software había finalizado y era necesario realizar la conexión entre estos 2 sistemas. A la fecha el requerimiento sigue “activo” y se solicita al responsable del proyecto, el informe o reporte detallado del estado del proyecto de interoperabilidad.

2. **Requerimiento de nombre:** PAI 2.0 para actualización del servicio WEB con el sistema de compensar. **Estado del requerimiento:** En curso y se encuentra pendiente del paso a pruebas, dicho requerimiento inicio en junio del 2023 y tenía fecha comprometida el día 1 de marzo del 2024. Se informa que el paso a pruebas se adoptó la semana pasada y está pendiente la reunión con el coordinador de QA para hacer el despliegue en ese ambiente y se informa además que el aplicativo PAI esta funcionado u operando con normalidad ya que solo se aplicó una actualización.

3. **Requerimiento de nombre:** Integración de SIIAS con el módulo de Limay de terceros, dicha integración se encuentra en curso, en fase de pruebas por el grupo de QA.

Al consultar el inventario consolidado de requerimientos en planner, identificamos 3 requerimientos que corresponden a interoperabilidad entre sistemas así:

- 1er. requerimiento denominado: SIVIGILA DC_210.184.0, finalizo y tuvo un retraso de 7 días en la entrega, lo cual no es de gravedad.
- 2do. requerimiento denominado: PAI2.0 – 2023IE17358, se encuentra “En CURSO” y presenta un atraso de 68 días con respecto a la fecha de vencimiento o compromiso, lo cual puede estar afectando el área usuaria.
- 3er. requerimiento denominado: OPGET – 2023IE3711, dicho requerimiento fue registrado en el mes de junio del año 2023 y la fecha no presenta ningún avance.

Nombre de la tarea	Nombre del depósito	Progreso	Asignado a	Fecha de inicio2	Fecha de vencimiento	Fecha de finalización	Tiempo de Retrazo
SIVIGILA DC - QA_SIVIGILA DC_210.184.0 - resoluciones generadas en formato PDF	SIVIGILA DC	Completada	Erick Fabian, Torres Aguirre	29/09/2023	06/10/2023	02/11/2023	7
PAI 2.0 - 2023IE17358 - Actualización del servicio web con el sistema información SAP	PAI	En curso	Diana del Pilar, Correcha Vasquez	17/07/2023	01/03/2024		68
OPGET - 2023IE3711- FOR023.2 OPGET Mitigacion del riesgo en el cruce de informacion	SIIAS	No iniciado		15/06/2023			

6.4 Gestión de soluciones de Software con la implementación de las políticas de MIPG: Gobierno Digital y Seguridad Digital

Política de Seguridad Digital

En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades. Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

Por su parte, el Comité Institucional de Gestión y Desempeño, debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política. Es por ello que se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área transversal que haga parte de la Alta Dirección. En el orden territorial, MinTIC definirá los lineamientos para que las entidades territoriales definan la figura del enlace de Seguridad Digital territorial para la implementación de la política de Seguridad Digital, así como las instancias respectivas para la articulación con el Coordinador Nacional de Seguridad Digital.

La implementación de la política, se hará mediante la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital, que será desarrollado y socializado por Min TIC y para los entes territoriales y demás partes interesadas, se adelantarán jornadas de sensibilización en temas de Seguridad Digital.

Fuente: Manual Operativo MIPG de la función Publica

El Modelo Gestión de Riesgos de Seguridad Digital, brinda un marco para la identificación de las amenazas y vulnerabilidades a las que está expuesta una entidad desde la perspectiva del entorno cibernético, con el fin de fortalecer el ambiente de control, intensificar la confianza de las múltiples partes interesadas en el medio digital.

En materia de Seguridad Digital, la SDS adopta la implementación de la política del Modelo de Gestión de Riesgos de Seguridad Digital desarrollado por Min Tic, por medio de las siguientes fases:

Identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

El proceso TIC, cuenta con matrices de riesgos de proceso, de corrupción y de seguridad de la información, esta última, relacionada con la implementación de la política de seguridad digital, ya que la matriz cuenta con 3 riesgos identificados para el manejo de la confidencialidad, integridad y disponibilidad de la información, dichos riesgos se gestionan periódicamente de acuerdo a lo establecido en el POGD. Con relación a lo anterior, el proceso cuenta con Matrices de riesgo donde se evalúan los riesgos y se establece el riesgo inherente y riesgo residual, así como el plan de tratamiento. Adicionalmente, se cuenta con las matrices de autoevaluación para determinar si el riesgo se ha materializado a partir del seguimiento de los diferentes controles establecidos.

En lo que respecta a los riesgos de proceso, se informa que a principios de año 2024, se llevaron a cabo las mesas de trabajo para la revisión de los riesgos asociados con el desarrollo de soluciones de software y se tiene establecido para esta vigencia, la revisión trimestral. Al consultar la matriz de riesgos, el ID: 4, consta de 3 controles, los cuales se encuentran asociados con las primeras fases del procedimiento SDS-TIC-PR-001. El riesgo asociado se describe así: “Posibilidad de afectación económica y reputacional por el desarrollo que no cumpla con las especificaciones técnicas del correcto levantamiento de los requerimientos”. El primer control está basado en el formato SDS-TIC-FT-023 y es aquí donde se definen y establecen los requerimientos y necesidades por parte del solicitante, que pudiera tener ajustes o aclaraciones resultado de las mesas de trabajo particulares. El tercer control tiene que ver con la verificación de los requisitos, al final para cada proyecto de software y como resultado de la eficacia de los controles establecidos, se cuentan documentos o formatos codificados SDS-TIC-FT-023, que definen los requerimientos de usuario. En ultimas, lo que no este escrito y no será desarrollado y hará parte de un nuevo requerimiento.

Dicho lo anterior, se valida la conformidad.

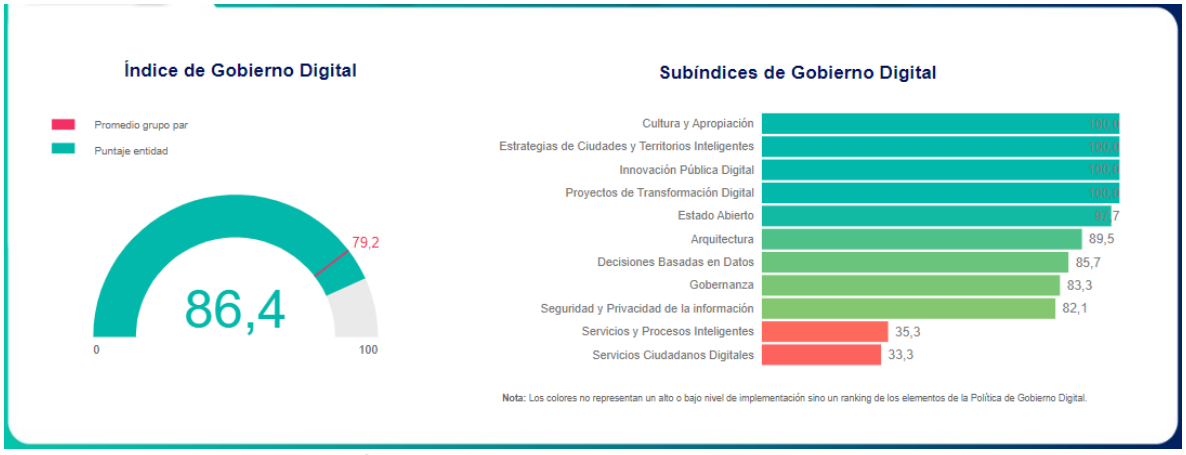
Política Gobierno Digital

La política propende por la transformación digital pública y busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC.

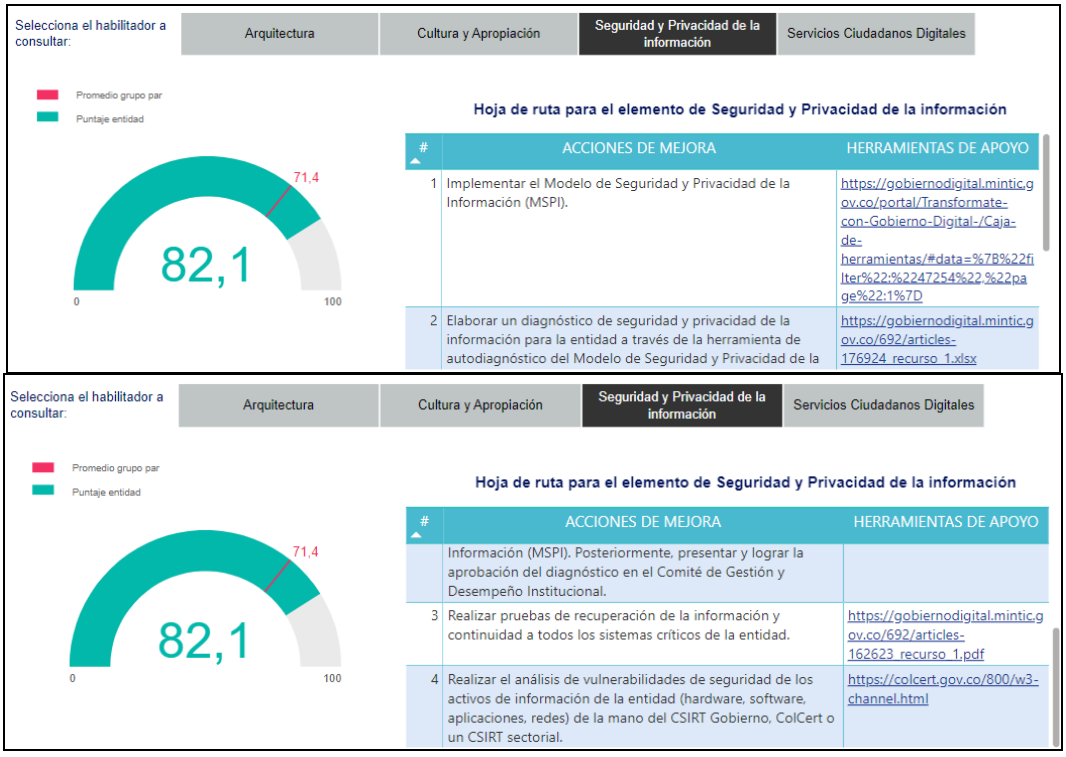
La implementación de la Política de Gobierno Digital esta previstos en el Manual del Gobierno Digital, el cual es un instrumento centralizado, estandarizado y fácil de uso, donde encuentran todo lo que necesitan las entidades públicas para transformarse digitalmente, mediante el siguiente enlace se puede consultar el Manual Interactivo de Gobierno Digital: https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/.

Fuente: Manual Operativo MIPG de la función Publica

En lo que respecta a la implementación de la política por parte de la secretaria de salud y en lo específico a la gestión de soluciones de software, se da conformidad de la siguiente manera:



Como se aprecia en la gráfica, se logra constatar un avance general del 86,4% en la implementación de la política en la secretaria Distrital de Salud y en lo que respecta al subíndice o habilitador de Seguridad y Privacidad de la información, se reporta un avance del 82,1% como se aprecia en las siguientes graficas:



Actualmente la hoja de ruta del habilitador de Seguridad y Privacidad de la información, consta de 4 actividades o acciones de mejora, la acción Nro1, 2 y 4 permiten implementar y realizar diagnóstico del MSPI o modelo de seguridad y privacidad de la información, dicho modelo consta de 14 dominios, agrupados en 114 controles basado en el código de buenas prácticas de la norma ISO27002:2013, en lo que respecta a los controles de dicha norma que tienen relación con el desarrollo de software y su ciclo SDLC, se presentan y resaltan a continuación:

- CONTROL DE ACCESOS enfoca el control de acceso en los aplicativos desarrollados mediante uso de credenciales con políticas de contraseñas seguras.

- CIFRADO: corresponde a contraseñas asignadas y almacenadas en tablas que son cifradas mediante algoritmos, así mismo al momento del transporte de la información entre sistemas, dicha información viaja de forma cifrada.

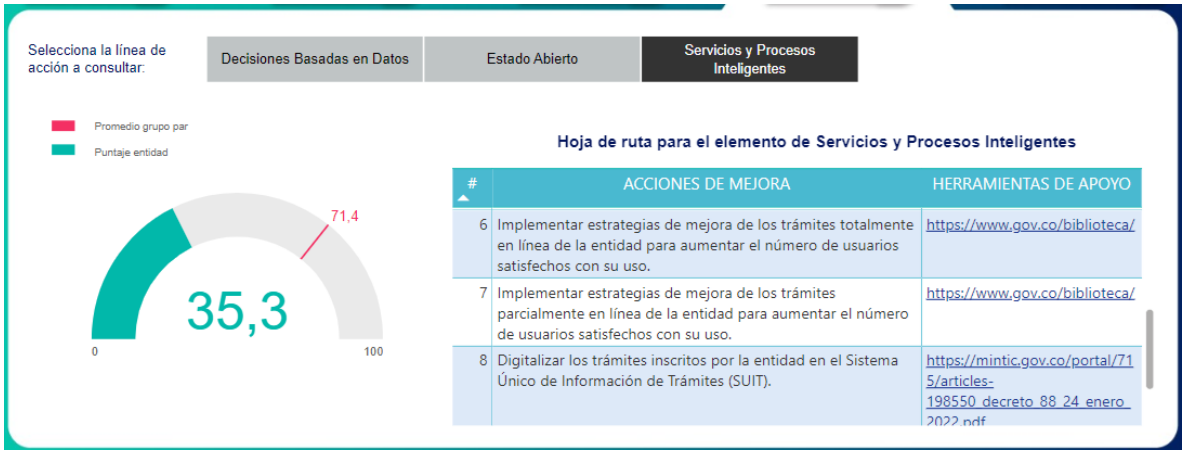
- SEGURIDAD EN LA OPERACION, Son varios los controles a saber:
  -Copias de seguridad de la información: Las copias se realizan para cada sistema de información desarrollado y que ha sido puesto en producción.

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

-Instalación del software en sistemas en producción: una vez el especialista QA del grupo de pruebas, genera el concepto técnico del aplicativo, se procede con el paso a producción avalado.
-Gestión de la vulnerabilidad técnica: mediante lineamiento y programación establecida, se realiza el test o set de pruebas de vulnerabilidades técnicas sobre las aplicaciones WEB desarrolladas mediante herramientas especializadas.

- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
  - Requisitos de seguridad de los sistemas de información.
  - Análisis y especificación de los requisitos de seguridad.
  - Seguridad en los procesos de desarrollo y soporte.
  - Política de desarrollo seguro de software.
  - Procedimientos de control de cambios en los sistemas.
  - Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - Restricciones a los cambios en los paquetes de software.
  - Uso de principios de ingeniería en protección de sistemas.
  - Seguridad en entornos de desarrollo.
  - Externalización del desarrollo de software.
  - Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - Pruebas de aceptación.
  - Datos de prueba.
  - Protección de los datos utilizados en pruebas.

Todos los controles anteriormente mencionados, hacen parte del ciclo de vida de desarrollo de software, actualmente son implementados en cada proyecto de software y se cuenta con los respectivos soportes y evidencias que dan cumplimiento al respecto.



Como se aprecia en la gráfica, se constata un avance general del 35,3% en lo que respecta a la implementación de las acciones de mejora para el componente de “Servicios y Proceso inteligentes”. Dicho componente, consta de 8 actividades, 3 de ellas, son enfocadas en la implementación de los trámites totalmente en línea y parcialmente, en la actualidad existen un total de 19 trámites implementados, de los cuales 16 se encuentran totalmente en línea y 3 parcialmente en línea, dicha información podrá ser consultada en el enlace: https://www.saludcapital.gov.co/Paginas2/Tramitesyservicios.aspx. Dichos trámites han sido desarrollados por el grupo de desarrollo de software de la secretaria de salud basado en el ciclo SDLC.

Dicho lo anterior, se valida dicho aspecto.

6.5 Test de seguridad para análisis de vulnerabilidades WEB

Para efectos del ejercicio, se utilizó la herramienta denominada **OWASP ZAP,** que es un escáner de seguridad web gratuito, utilizado como una herramienta profesional para pruebas de penetración y está diseñada específicamente para probar aplicaciones web. En esencia, esta herramienta permite comprobar si existe algún tipo de fallo, debilidad o vulnerabilidad de seguridad conocido, funciona como un "proxy de intermediario", es decir que encuentra entre el navegador WEB del probador y la aplicación web para que pueda interceptar e inspeccionar los mensajes enviados entre el navegador y la aplicación web.

OWASP ZAP, rastrea las aplicaciones web con su araña o exploit de ataque, a fin de escanear pasivamente cada página web que encuentre y también utilizará el escáner activo para atacar todas las páginas, funcionalidades y parámetros descubiertos. La araña ZAP tradicional utilizado para las pruebas, descubre enlaces examinando el HTML en las respuestas de la aplicación web. A continuación, mediante tablas se presentan los resultados obtenidos de los test ejecutados el día 17 de mayo de 2024, es de anotar que cada uno de los informes detallados resultado del escaneo, será entregado como anexos al presente informe:

URLS de sitios web definidos para los aplicativos seleccionados:

#	Sistema de Información	Enlace o URL del ambiente de producción
1	SICAI	https://sicai.saludcapital.gov.co/WebSicai/
2	SIIAS	https://appa.saludcapital.gov.co/siias/inicio/login.aspx
4	LABVANTAGE	https://appasaludsds.saludcapital.gov.co/lavantage/
5	PAI	https://appb.saludcapital.gov.co/pai/inicio/login.aspx
6	CIP	https://appa.saludcapital.gov.co/cip/Formularios/Autentificacion/Autentificacion.aspx?ReturnUrl=%2fcip%2f
8	Autorregulación	http://autorregulacion.saludcapital.gov.co/
9	Licencias RX - Veterinarias	https://tramitesenlinea.saludcapital.gov.co/
10	SIDCRUE	http://fappd.saludcapital.gov.co/crue/
11	SIRC	http://app.saludcapital.gov.co/sirc2/

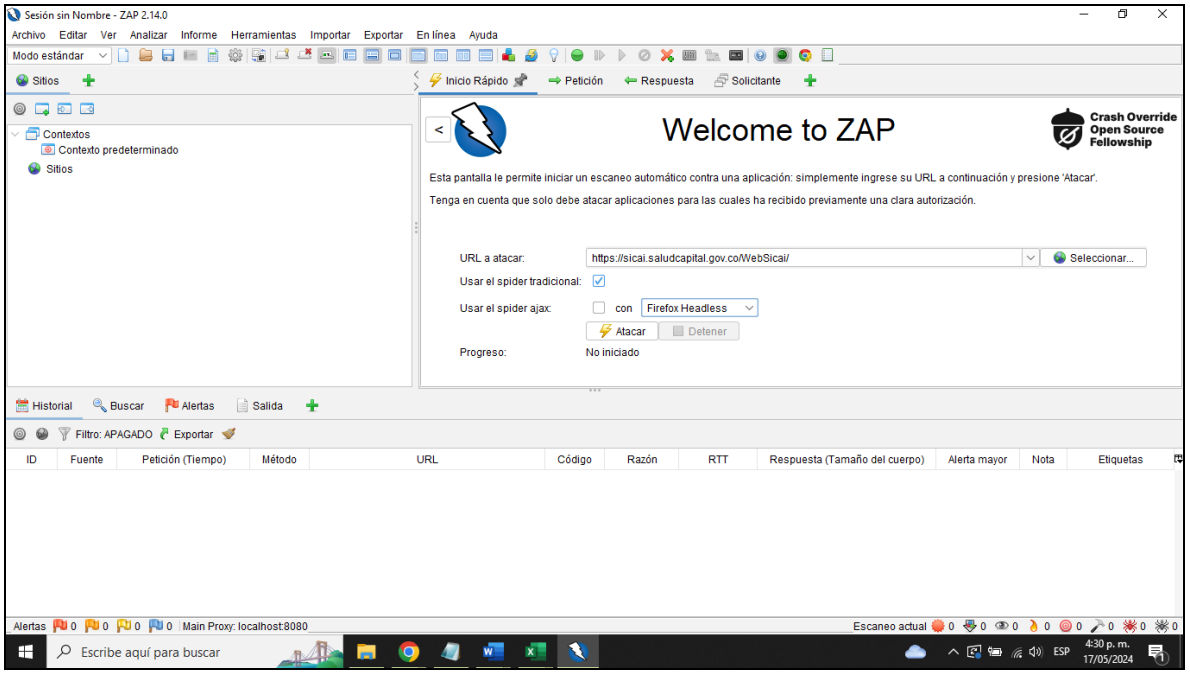
A continuación, Se presenta un recuento de las alertas encontradas durante el testeo, desglosadas en categorías de riesgo. Las alertas de tipo: Alto y Medio, corresponden a

debilidades o vulnerabilidades identificadas en los sitios web y deberán ser objeto de revisión por parte de los responsables a fin de aplicar los correctivos o remediaciones necesaria para evitar o reducir el riesgo de un posible ciberataque.

			Alertas encontradas				
#	Sistema de Información	Enlace o URL del ambiente de producción	Total Hallazgos	Altos	Medio	Bajo	Informativo
1	SICAI	https://sicai.saludcapital.gov.co/WebSicai/	15	0	5	5	5
2	SIIAS	https://appa.saludcapital.gov.co/siias/inicio/login.aspx	19	0	5	7	7
3	LABVANTAGE	https://appasaludsds.saludcapital.gov.co/lavantage/	21	1	6	8	6
4	PAI	https://appb.saludcapital.gov.co/pai/inicio/login.aspx	17	1	4	6	6
5	CIP	https://appa.saludcapital.gov.co/cip/Formularios/Autentificacion/Autentificacion.aspx?ReturnUrl=%2fcip%2f	18	0	5	7	6
6	Licencias RX -Veterinarias	https://tramitesenlinea.saludcapital.gov.co/	15	0	5	6	4
7	SIDCRUE	http://fappd.saludcapital.gov.co/crue/	26	5	6	9	6
8	SIRC	http://app.saludcapital.gov.co/sirc2/	19	2	4	5	8
Total debilidades encontradas			150	9	40	53	48

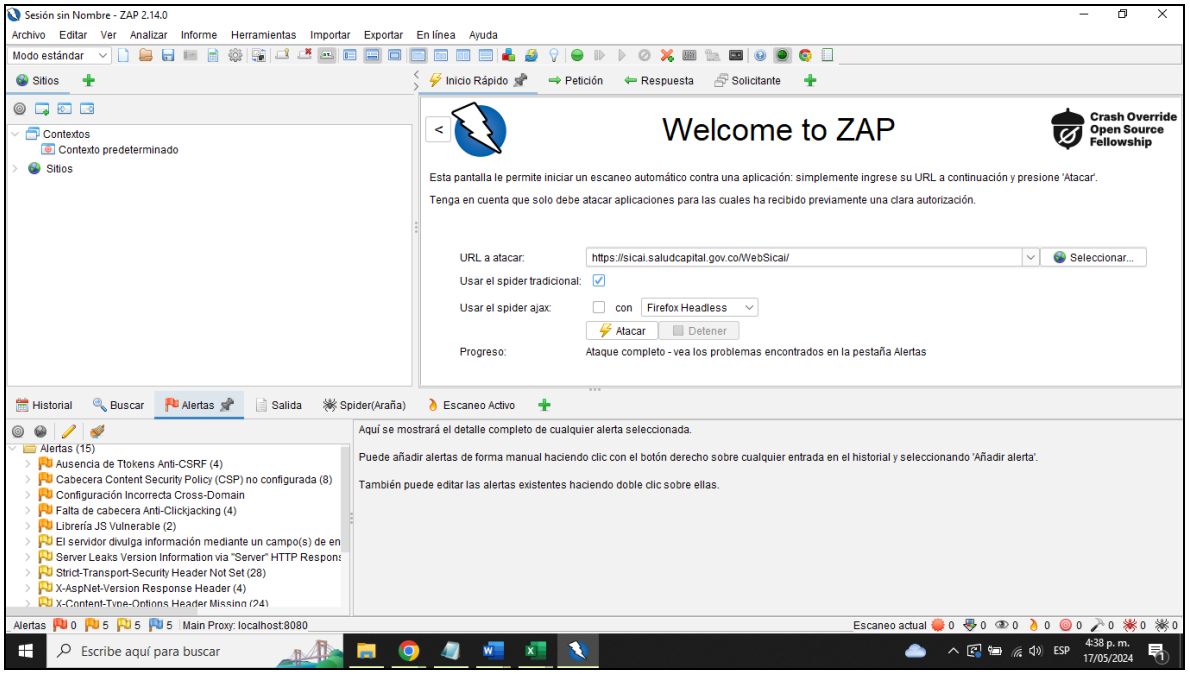
A continuación, se comparten 2 pantallazos de la herramienta al inicio y al final del test con el resultado generado, para efectos de comprobación se eligió el sistema de información: SICAI

Inicio del test:



*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Final del test:



En síntesis, al identificarse ciertas vulnerabilidades sobre los sitios WEB desarrollados que fueron objeto de los escaneos o test, se evidencian y confirman las debilidades del software y, en consecuencia, existe riesgo de pérdida de confidencialidad, integridad y disponibilidad que pudiera materializarse, por lo que será indispensable aplicar los correctivos del caso, lo que obedece a una oportunidad de mejora para el proceso.

6.6 Grado de satisfacción del usuario final frente al producto entregado

Con relación a este objetivo, se seleccionó una muestra de 10 proyectos de desarrollo de software es estado "cumplidos", y se solicitó se allegaran los registros de envió de encuesta de satisfacción y las respuestas a estas por parte del usuario final. A continuación, mediante tabla, se presentan los resultados encontrados.

#	Sistema de Información	Envió de Encuesta	Satisfacción Funcional
1	SICAI	SI	SI
2	SIIAS	SI	SI
3	LABVANTAGE	SI	SI
4	PAI	SI	SI
5	CIP	SI	SI
6	Autorregulación	SI	SI
7	Licencias RX -Veterinarias	SI	SI
8	SIDCRUE	SI	SI
9	SIRC	SI	SI

Nota: Respecto a la muestra seleccionada, se constata el grado de satisfacción, el cual fue satisfactorio, sin embargo, es importante precisar que existen proyectos de software que se encuentran “EN CURSO”, que vencieron con respecto a la fecha de entrega o fecha comprometida que, al momento de la evaluación, se constata que siguen sin cumplir, han superado varios meses o años y se podría afirmar que, debido a los atrasos e incumplimientos el usuario final podría estar insatisfecho. Proyectos como:

1. Reconocimiento de personería jurídica de fundaciones, corporaciones y/o asociaciones de utilidad común y/o sin ánimo de lucro.
2. Reforma de estatutos de fundaciones, corporaciones y/o asociaciones de utilidad común y/o sin ánimo de lucro.
3. SIGEME-Q
4. Entre otros, presentan incumplimientos.

Dicho lo anterior, el riesgo de incumplimiento se materializo y hace parte de la no-conformidad ya decreta en los puntos anteriores. En consecuencia, es indispensable por parte del proceso aplicar los correctivos del caso.

6.7 Evaluación integral mediante lista de chequeo

El ejercicio que se llevó a cabo mediante lista de chequeo o verificación previamente definidas y contemplo la evaluación de requisitos o criterios clasificados en 2 grupos, el primer grupo, se compone de 47 criterios en base a las buenas prácticas y normatividad aplicable y el segundo grupo que se compone de 16 criterios, evaluando el procedimiento SDS-TIC-PR-001 en base al ciclo de vida SDLC. A continuación, mediante tabla consolidada, se presentan cada una de las preguntas formuladas y los resultados generados. Nota: El detalle de la evaluación para cada uno de los criterios o requisitos se encontrará en los papeleres de trabajo generados, los cuales serán suministrados al final del ejercicio como evidencia digital.

Convenciones: C: Cumple, NC: No conformidad y AR: Acción para abordar riesgo u Oportunidad de mejora

Grupo 1:

Criterio a Verificar	Preg	C	NC	AR
¿Documenta constantemente los procedimientos que ejecuta su área, y los da a conocer los mismos?	1	X		
¿Cuenta con un procedimiento de control de cambios, es decir, si se requiere un cambio de un aplicativo puesto en producción cuales son los pasos para aplicar dicho ajuste?	2	X		X
¿Tiene registros para verificar y determinar que los recursos a nivel de servidores están asignados correctamente y que estos no requieren mayor capacidad?	3	X		
¿Se cuenta con ambientes de desarrollo, prueba y producción, cuáles son los servidores?	4	X		
¿Realiza copia de respaldo de datos? ¿Cada Cuánto?	5	X		
¿Se ha probado que los Backus realizados funcionen correctamente?	6	X		
¿Existe una Política definida para el desarrollo seguro que contemple las reglas para los desarrollos dentro y fuera de la entidad?	7	X		
Se establece y protege los entornos de desarrollo seguro de manera apropiada para el desarrollo del sistema y que cubra todo el ciclo de vida.	8	X		
Se realiza supervisión y monitoreo de las actividades de desarrollo de sistemas tercerizado.	9	X		
¿Realiza pruebas de seguridad en los aplicativos?	10	X		X
¿Realiza pruebas de aceptación de la aplicación?	11	X		
¿Cómo controla y protege los datos que usa para las pruebas?	12	X		

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

¿En caso de una caída general, tiene algún plan o contingencia para que las aplicaciones sigan funcionando?	13	X		X
¿Se revisa el cumplimiento técnico de las aplicaciones y cumpla con normas de seguridad?	14	X		
¿Cómo proceden cuando hallan o identifican vulnerabilidades?	15	X		
Para el desarrollo de software, se realiza protección de datos confidenciales, ocultando dichos datos mediante el uso de técnicas como el enmascaramiento de datos, seudonimización o anonimización.	16	X		
Se cuenta con medidas de prevención para fuga de datos de los sistemas de información desarrollados.	17	X		
Principios de codificación segura deben aplicarse al desarrollar software. El software se escribe de forma segura, reduciendo posibles vulnerabilidades que surgen de fallas de diseño y los errores de programación.	18	X		X
Control de acceso al código fuente de los programas, ¿se restringe el acceso al código fuente de los programas?	19	X		
¿Contamos con evidencias documentadas del levantamiento de información? ¿Dónde están ubicados?	20	X		
¿Dónde están ubicados los manuales de usuario y documentación general de los aplicativos?	21	X		
¿Los aplicativos contienen pruebas unitarias? De que tipo: ¿Carga, stress?	22	X		
¿Dónde mantiene su versionamiento de código?	23	X		
¿Tiene documentado un estándar de desarrollo?	24	X		
¿Ha considerado integrar varios de los sistemas que desarrolla?	25	X		
¿Dónde se puede observar la solicitud de cambios realizados a un sistema por parte del usuario funcional?	26	X		
¿Se deja evidencias del análisis que se realiza para validar la coherencia de este cambio?	27	X		
¿Dónde se encuentra alojada la documentación de soporte de las aplicaciones?	28	X		
¿Cómo realiza la liberación de versión, donde documenta dicho procedimiento?	29	X		
¿El mismo desarrollador que construye el aplicativo lo prueba?	30	X		
¿Se realizan pruebas a nivel de campos del formulario?	31	X		
¿Cómo valida la entrada de datos al sistema?	32	X		
¿Define Modelo Entidad Relación (MER)?	33	X		
¿Cómo evita la redundancia de datos en su BD?	34	X		
¿Cómo realiza la selección del motor de BD?	35	X		

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

¿Cómo realiza la creación de usuarios?	36	X		
¿Cómo ejecuta el mantenimiento de los servidores de aplicación?	37	X		
¿Cada cuánto se realiza mantenimiento preventivo a servidor de aplicación y motor de BD?	38	X		
¿Cuenta con alguna retroalimentación de parte del cliente para validar su conformidad frente al producto entregado?	39	X		
¿Los sistemas implementados son fácilmente escalables?	40	X		
¿Los sistemas son de fácil adaptación a las nuevas especificaciones y requisitos del software	41	X		
¿Los sistemas elaborados son portables, es decir tiene la capacidad de ser transferidos de un entorno a otro?	42	X		
¿Se tiene un responsable por cada proyecto?	43	X		
¿Quién determina que se debe iniciar a desarrollar?	44	X		
¿Tiene algún procedimiento para estimación de tiempos para los desarrollos?	45	X		
¿Cada cuánto realiza liberaciones de funcionalidades?	46	X		
¿Dónde se almacena el control de seguimiento de cada proyecto?	47	X		
Resultado consolidado en grupo 1		**47**	**0**	**4**

Grupo 2:

Aspectos Evaluados	Preg	C	NC	AR
Validar recepción de solicitudes de software para el desarrollo interno, externo o adquisición de aplicaciones. Se cuenta con inventarió de requerimientos gestionados mediante Formato FT-023 u otros mecanismos.	1	X		X
Consultar requerimientos que fueron devueltos ya que no cumplieron con toda la información requerida. ¿Como notifican?	2	X		
Consultar registros de reuniones de alcance técnico o evaluación de los diferentes requerimientos recibidos.	3	X		
Consultar conceptos de viabilidad de software aceptados y rechazados y notificaciones generadas	4	X		
Validar los requerimientos Versión finales con aceptación (Firmas) de las partes interesadas para dar inicio a fase de diseños.	5	X		
Validar desarrollo de soluciones de software inhouse (nuevo, ajustes o actualizaciones) y su estado. Consultar proyectos de software que conllevo la interoperabilidad entre otros sistemas de información.	6		X	

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Consultar registros de ATPs o pruebas realizadas, garantizando la eficacia de las soluciones de software, mejoras y actualizaciones entregadas a la SDS. Validar conceptos técnicos de pruebas emitidas	7	X		
Validar la elaboración o actualización de documentación producto de la nueva solución o mejoras.	8	X		
Validar registros de satisfacción de los usuarios con la entrega de las soluciones de software desarrolladas y/o adquiridas, el uso y apropiación de las mismas	9	X		
Validar registros de capacitaciones efectuadas con los referentes para presentar la nueva solución	10	X		
Validar soluciones en ambiente de producción y la entrega a los lideres funcionales (registros de aceptación)	11	X		
Validar resultados de la medición de percepción y las acciones de mejoramiento desarrolladas	12	X		
se identificarán errores presentados o modificaciones que conllevaron cambios o ajustes impactando en alcance, tiempo y costo	13	X		
Validar las revisiones por la dirección realizadas respecto al tema	14	X		
Cómo es el manejo de los riesgos propios del procedimiento.	15	X		
Gestión de las comunicaciones del procedimiento	16	X		
Resultado consolidado en grupo 2		**15**	**1**	**1**

En síntesis:

	RESULTADOS	**#**	**%**
Evaluación General	PUNTOS O CRITERIOS EVALUADOS	63	100%
	CUMPLIMIENTO	62	98%
	NO CONFORMIDAD	1	2%
	OPORTUNIDADES DE MEJORA	5	8%

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

7. ASPECTOS POSITIVOS (NIA 2410 A2).

Se resaltar la cordialidad y la atención prestada por los participantes de la auditoria, mostrando un alto grado de compromiso frente a la cultura del control, los colaboradores de la dirección TIC, identifican, entienden y gestionan el procedimiento evaluado.

8. NO CONFORMIDADES. (NIA 2431).

8.1 Si bien es cierto, se cuenta con el inventario de requerimientos de software del año 2023 y 2024 gestionado mediante el aplicativo PLANNER, el cual fue unificado para el ejercicio de acuerdo a los diferentes frentes de trabajo, evidenciamos que existen incumplimientos reiterativos respecto a la entrega oportuna o fecha comprometida con el cliente, ya que identificamos requerimientos de más de 6 meses, 1 año, 2 años, que se encuentran “en curso”, sin finalizar, afectando los metas y objetivos de diferentes procesos, por consiguiente las necesidades del usuario final no han sido resueltas o satisfechas en los tiempos establecidos o pactados, en consecuencia, existe un incumplimiento al procedimiento SDS-TIC-PR-001, instructivo SDS-TIC-INS-010, modelo 223, ley 87 de 1993 que asegura la oportunidad, confiabilidad de la información y de sus registros, y los numerales: 8.1 literal a), b), 8.3.2 literal a) y 9.1.2 de la norma 9001:2015, por lo que hace necesario e indispensable tomar las acciones correctivas del caso.

9. ACCIONES PARA ABORDAR RIESGOS. (NIA 2410-A1).

9.1. Pese a que, se cuenta con inventarios de requerimientos de software mediante el aplicativo PLANNER para los diferentes frentes, evidenciamos que existen registros que no están siendo actualizados adecuadamente, ya que por ejemplo en el campo progreso de la base, informa estado “iniciado” y los requerimientos ya se encuentra “finalizado” y en otros casos consultados, informa que el requerimiento se encuentra “en curso” cuando no ha iniciado, lo cual demuestra que el manejo de la información y el control de la misma no es del todo eficiente, por consiguiente, existe una debilidad que debe ser subsanada y se hace necesario fortalecer este aspecto, implementando las mejoras que haya lugar.

9.2. Pese a que existe la gestión de requerimientos de software mediante el aplicativo PLANNER, evidenciamos que dicha gestión se encuentra desagregada en varios frentes de trabajo como son: fábrica de software, frente ERP y requerimientos múltiples no ERP, y por lo tanto, fue necesaria la unificación o centralización de la información al momento de la auditoria ya que desde el momento que se solicitó la información o inventario por parte del auditor, demoro varios días para ser procesada y suministrada, lo cual demuestra que el manejo de la información y el control de la misma no es del todo eficiente, por consiguiente, existe una debilidad que debe ser subsanada y se hace necesario fortalecer este aspecto, implementando las mejoras que haya lugar.

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

9.3. Si bien es cierto, el proceso de gestión de soluciones de software entrega productos al final del ciclo de vida SDLC, evidenciamos que no cuenta con mediciones de la eficacia y eficiencia del procedimiento en sí, mediciones de impacto tales como: tiempos de oportunidad en la entrega, grado de satisfacción del usuarios final, numero de requerimientos atendidos o recibidos en el periodo en comparación con los requerimientos cumplidos o finalizados, no se tienen definidos o establecidos, en consecuencia, existe una debilidad frente al procedimiento y la buena práctica y en tal sentido se hace necesario implementar las mejoras que haya lugar.

9.4. Si bien es cierto, el ciclo de vida de desarrollo de software SDLC establece como buena práctica el desarrollo de código seguro, a partir de las entrevistas que hicimos algunos de los desarrolladores, afirman utilizar las metodologías, sin embargo al realizar los test o pruebas de análisis de vulnerabilidades técnicas mediante el aplicativo OWASP ZAP sobre 8 sitios WEB desarrollados y que se encuentran en producción, se evidencian múltiples debilidades del software, ya que el resultado o informes arrojan amenazas latentes de severidad tipo alto y medio que pudiera materializarse afectando la confidencialidad, integridad y disponibilidad de la información, en consecuencia, existe una debilidad frente al procedimiento y la política de desarrollo seguro y en tal sentido, será indispensable aplicar los correctivos del caso.

10. CONCLUSIONES. (NIA 2410-A1).

- La auditoría se desarrolló bajo en el estricto seguimiento y cumplimiento del plan definido, cabe señalar que resultado del ejercicio, se identificaron 6 oportunidades de mejora y una no-conformidad, que son sustentadas y formuladas en el presente documento.

- Se identificó un total de 1855 requerimientos “completados” en el intervalo de marzo a diciembre del año 2023, de los cuales el 26% de estos, corresponden a requerimientos que superaron la fecha comprometida, es decir, finalizaron fuera del tiempo y por consiguiente afectaron la entrega oportuna y comprometida con el cliente.

- Se identificó un total de 753 requerimientos “completados” en el intervalo de enero a abril del año 2024, de los cuales el 16% de estos, corresponden a requerimientos que superaron la fecha comprometida, es decir, finalizaron fuera de tiempo y por consiguiente afectaron la entrega oportuna y comprometida con el cliente.
- Se identificó que un 5% de los requerimientos “completados fuera de tiempo” es decir, 124 casos en el intervalo de enero a abril del año 2023, superaron el tiempo

de entrega a más de 30 días, existen casos que superaron más de 100 días, lo cual representa una debilidad importante, ya existe un incumplimiento importante que reinciden y deriva en una no-conformidad.

- Se identifica 19 requerimientos en estado “EN CURSO” del año 2020 hasta el año 2023 que vencieron frente a la fecha comprometida de entrega y a la fecha de la presente auditoria siguen sin finalizar, lo cual representa una no-conformidad, ya que existe un incumplimiento que afecta el indicador de oportunidad y satisfacción o percepción del cliente.

- La secretaria de Salud mediante la dirección TIC, ha venido adelantando proyectos de interoperabilidad entre sistemas de información, que se encuentran en operación y al consultar el inventario de requerimientos de software año 2023 y 2024 mediante el aplicativo PLANNER, evidenciamos 3 requerimientos que se encuentran en curso o en desarrollo.

- Evidenciamos la implementación de la Política de Gobierno Digital y Seguridad Digital en lo concerniente a los aspectos del ciclo de vida de desarrollo de software.

- Al realizar el test o prueba de análisis de vulnerabilidades técnicas, sobre 8 sitios WEB desarrollados, se evidencian y confirman debilidades del software y, en consecuencia, existe una amenaza latente que pudiera materializarse por pérdida de confidencialidad, integridad y disponibilidad, por lo que será indispensable para los custodios o responsables de los activos de información, aplicar los correctivos del caso.

.

- Respecto a la gestión de riesgos en la fase de medición y seguimiento, se sugiere reforzar, realizando el ejercicio por lo menos 3 veces al año ya que la severidad de los riesgos podría variar de acuerdo a la dinámica entidad y podrían definirse nuevos procesos, nuevos servicios, nueva infraestructura y todo ello deriva en nuevos riesgos que no están siendo tratados y evaluados.

- Existen 3 bases de datos mediante el aplicativo PLANNER que contiene la totalidad de los requerimientos de software gestionados por los frentes de desarrollo, dichos grupos funcionan como silos y es por eso que la información se encuentra desagregada, lo que se busca como oportunidad de mejora, es la unificación y estandarización de la información.

- La OCI concluye, que el proceso de Gestión de soluciones de software, cumple con el procedimiento establecido SDS-TIC-PR-001, existiendo varios aspectos susceptibles de mejora que deben ser ajustados de acuerdo con los hallazgos presentados en el presente informe.

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

- Dada la relevancia de la gestión de soluciones de software, como uno de los servicios destacados o insignia de la dirección TIC, es recomendable definir indicadores, a fin de medir la eficacia y eficiencia del servicio ofrecido, toda vez que las mediciones tales como: tiempos de oportunidad en la entrega, grado de satisfacción del usuario final, numero de requerimientos atendidos en el periodo en comparación de los requerimientos cumplidos, no se miden. lo cual se considera un aspecto susceptible de mejora que permita medir la eficacia y eficiencia del proceso.

- **Recomendación 1:** Pese a que la gestión de cambios o mejoras sobre software que se vienen adelantado e implementando por parte del equipo de desarrollo de la SDS, dichos cambios que afectan la prestación de los servicios y que generan una indisponibilidad en el paso o puesta a producción, no se rigen del todo al lineamiento interno estándar SDS-TIC-LN-007, en tal sentido, se hace necesario armonizar cualquier tipo de cambio (estándar o de emergencia) bajo el lineamiento existente.

- **Recomendación 2:** Aun cuando, el proceso de gestión de soluciones de software entrega productos al final del ciclo de vida SDLC, evidenciamos incumplimientos reiterativos en los tiempos comprometidos con el usuario final, esto obedece a que el recurso humano es limitado bajo un número de horas contratadas, de igual forma, proyectos de software que se encontraban en fase de desarrollo, han tenido que detenerse o pausarse debido a la demanda y priorización de nuevos requerimientos, de otra parte, el personal contratista, finaliza contrato y la formalización del nuevo contrato no es inmediata, puede tomar varios días o incluso meses, en consecuencia afecta la continuidad de los proyectos de software y los tiempos comprometidos y en tal sentido, la situación debe ser puesta en consideración, a fin de toman los correctivos del caso, evitando que dicha situación se siga presentando.

11. PLAN DE MEJORAMIENTO (NIA 2500).

Como resultado de la auditoría, el proceso auditado deberá cumplir con el lineamiento establecido por la dirección de planeación institucional y calidad para la elaboración del plan de mejoramiento que haya lugar, con el fin de realizar el tratamiento adecuado incluyendo en las actividades el ciclo PHVA y de ser necesario realizar mesas de trabajo cuando los acciones involucren otras dependencias. Nota: Sera responsabilidad de los referentes elaborar el plan de mejoramiento adecuado que responda a las oportunidades de mejora identificadas

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

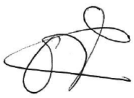
12. ANEXOS.

Corresponde a los papeles de trabajo utilizados en cada una de mesas de trabajo realizadas y así mismo, se compartirán los 8 informes de análisis de vulnerabilidades técnicas aplicadas sobre sitios WEB.

NOMBRE (S) Y APELLIDO (S) Y FIRMA (S) DE AUDITOR (ES).

Francisco Javier Pinto González

APRUEBA JEFE OFICINA DE CONTROL INTERNO.



Firmado digitalmente por OLGA LUCIA VARGAS COBOS

Olga Lucia Vargas Cobos

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)