INFORME FINAL AUDITORÍA DE GESTION AL PROCESO TIC

OFICINA DE CONTROL INTERNO

AUDITOR (ES):
LÍDER: FRANCISCO JAVIER PINTO
Certificado HSEQ, registro IAC No. GEC68940 e ISO27001:2013 registro ERCA No.1001545

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

BOGOTÁ, junio 2021

SECRETARÍA DISTRITAL DE SALUD

Contenido

1. OBJETIVO GENERAL DE LA AUDITORÍA.

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 al proceso de gestión TIC para los siguientes frentes:

1.1 Se realizará la verificación y evaluación de la gestión desarrollada frente a la implementación de las Políticas de Gobierno digital y Seguridad Digital contempladas en el Modelo Integrado de planeación y gestión – MIPG.
1.2 Respecto al sistema de seguridad de la información se evaluará el ciclo PHVA de manera general, con el fin de determinar el mantenimiento, la mejora continua del mismo y la aplicación de la modelo MSPI y la Norma ISO27001:2013. Insumos informes de auditoría 2020 y recomendaciones FURAG 2019 y 2020.
1.3 Se verificará el cumplimiento de los requerimientos e incidentes solicitados por los clientes internos y externos a través de los diferentes mecanismos establecidos y
1.4 Se realizará la verificación sobre las funciones, responsabilidades y actividades establecidas para la Gestión de TIC mediante la caracterización del proceso.

2. OBJETIVOS ESPECÍFICOS DE LA AUDITORÍA.

2.1 Verificar y evaluar el cumplimiento del proceso, instructivos y lineamientos existentes para las diferentes actividades definidas en el alcance.
2.2 Verificar y evaluar el cumplimiento del marco normativo que lo rige: Resoluciones, Decretos y Normas.
2.3 Determinar el nivel de adherencia frente a los valores institucionales
2.4 Verificar la gestión y los componentes de control, actividades de control, gestión del riesgo, actividades de monitoreo e información y comunicación (Líneas de Defensa).

3. ALCANCE DE LA AUDITORÍA.

- Responsabilidades y actividades TIC,
- Requerimientos e incidentes,
- Políticas de Gobierno Digital y Seguridad Digital
- Sistema de Seguridad de la información

Periodo a evaluar: abril 2020 a abril 2021

4. CRITERIOS DE AUDITORÍA.

Proceso:

- SDS-TIC-CAR-001 – GESTION TIC

Procedimientos:

- SDS-TIC-PR-002 - GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC
- SDS-TIC-PR-001 - GESTIÓN DE SOLUCIONES DE SOFTWARE
- SDS-TIC-PR-005 - SEGURIDAD INFORMÁTICA

Otros: Gestión de Riesgos y Mapa de Riesgo Institucional

5. MARCO LEGAL.

- CONPES 3995 Política Nacional de Confianza y Seguridad Digital
- CONPES 3854 del 2016 Política Nacional de Seguridad Digital
- Decreto 1008 de 2018 Política de Gobierno Digital, habilitadores transversales SI
- Decreto 1499 de 2017 - MIPG y las Políticas de Gobierno Digital y Seguridad Digital
- Norma IEC ISO 27001:2013
- Decreto 507 del 2013
- Resolución 160 del 11 de febrero de 2021
- Resolución 1486 del 11 de agosto de 2020

6. METODOLOGÍA UTILIZADA.

La presente auditoría se desarrolló mediante mesas de trabajo presencial y virtual con los diferentes referentes designados, verificando y constatando el cumplimiento de recomendaciones y requisitos normativos acorde a las listas de verificación elaboradas. Se realizo toma de toma de muestras aleatorias y análisis de información referente al proceso, procedimientos, registros documentales, riesgos, herramientas, entre otros, Las mesas de trabajo fueron agendadas acorde al plan de trabajo establecido.

7. ANÁLISIS DE INFORMACIÓN.

7.1 GOBIERNO DIGITAL

MARCO CONCEPTUAL

Política de Gobierno Digital
Liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, que tiene como objetivo: “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital de acuerdo con el Decreto 1008 de 2018. El Gobierno Digital, busca aumentar la cooperación entre ciudadanos y entidades públicas para el desarrollo de productos y servicios de valor. Por otra parte, cabe anotar que el Manual define los lineamientos, estándares y acciones a ejecutar por parte de las entidades obligadas a cumplir con la Política de Gobierno Digital.

Principales elementos de la Política

Para la implementación de la política se han definido dos componentes principales:
TIC para el Estado: Tiene por objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las TICs. Así mismo, busca fortalecer las competencias T.I. de los servidores públicos, como parte fundamental de la capacidad institucional.

TIC para la Sociedad: tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, políticas y normas, y la identificación de soluciones a problemáticas de interés común.

Estos componentes son habilitados por tres elementos fundamentales que permiten el desarrollo y el logro de los propósitos de la política, denominados habilitadores transversales identificados como:

1. **Arquitectura de TI**: Busca fortalecer las capacidades de gestión de T.I. de las entidades públicas, a través de la definición de lineamientos, estándares y mejores prácticas contenidos en el Marco de Referencia de Arquitectura Empresarial del Estado.
2. **Seguridad y Privacidad:** Busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información.
3. **Servicios Ciudadanos Digitales:** Busca facilitar y brindar un adecuado acceso a los servicios de la administración pública haciendo uso de medios digitales, para lograr la autenticación electrónica, interoperabilidad y carpeta ciudadana, esto será posible a través de la implementación del Modelo de Servicios Ciudadanos Digitales.

Dichos habilitadores cuentan con una serie de lineamientos que se desarrollan a través de estándares, y marcos de referencias, que deben implementarse con la finalidad de alcanzar los propósitos de la implementación de la política de Gobierno Digital.

Conforme a estos conceptos se sintetizan y presentan en la siguiente imagen:

Fuente: https://estrategia.gobiernoenlinea.gov.co/623/articles-79107_recurso_1.pdf

Medición del desempeño de Política de Gobierno Digital

Resultado general para la SDS:

Cumplimiento de la política en la actualidad es del 97%

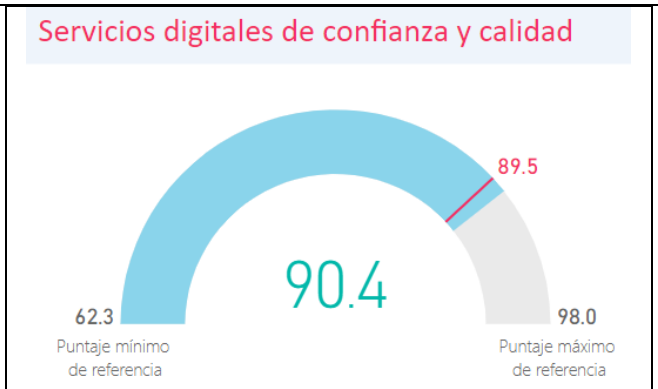
Resultado por Habilitadores:

Cumplimiento del primer habilitador: 96,7%

Cumplimiento del segundo habilitador: 98%

Cumplimiento del tercer habilitador: 68%

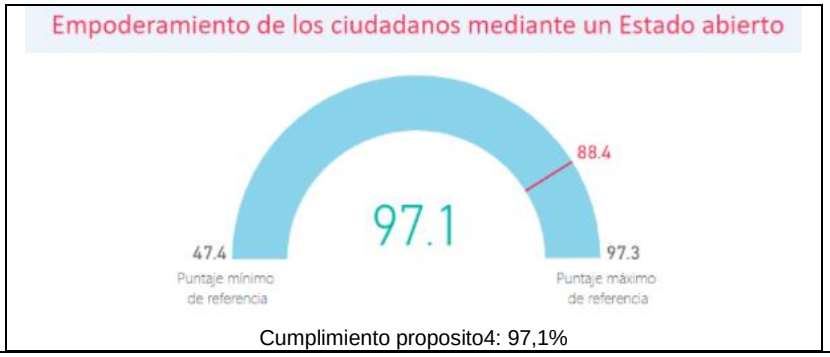
Calificación frente a los 5 Propósitos:



Cumplimiento proposito1: 90,4%

Cumplimiento proposito2: 74%

Cumplimiento proposito3: 83,3%



Cumplimiento proposito4: 97,1%

Cumplimiento proposito5: 71,6%

Fuente de consulta:
https://app.powerbi.com/view?r=eyJrIjoiMTZiZDU5MTQtMjNjNi00OTczLTg0ZjktMzRkNTkyYzg3ODdkIiwidCI6IjU1MDNhYWMyLTdhMTUtNDZhZi1iNTIwLTJhNjc1YWQxZGYxNiIsImMiOjR9

Resultado de la medición, podemos observar que la política de Gobierno Digital en la entidad requiere implementar otros elementos o componentes faltantes para lograr su cumplimiento al 100%.

Análisis de información frente este objetivo

Se llevaron a cabo 4 mesas de trabajo soportado mediante las listas de verificación definidas y los registros de actas de participación de los referentes designados, dando respuesta a todas las preguntas formuladas. El insumo para la elaboración de las preguntas fue tomado del informe Furag que permite identificar las brechas o elementos faltantes en la implementación de la política. Los resultados se presentan de manera sintetizada en este informe y el detalle a cada punto o pregunta se encontrará en los papales de trabajo, archivo denominado: Checklist - Gobierno Digital V1 - MayoFinal.docx.

Nota: Los hallazgos identificados en este componente resultado de la evaluación realizada, se consideran debilidades y derivan en acciones para abordar el riesgo, las cuales serán justificadas en capítulo 10 de este documento.

Preguntas Formuladas:	**25**
Recomendaciones Validadas	25
Recomendaciones Cumplidas:	15
Recomendaciones incumplidas:	10
Acciones para Abordar riesgos	4
No Conformidades	0
Porcentaje de cumplimiento respecto a la evaluación	60%

Primer Hallazgo	
Respecto a las preguntas 1 a la 7 de la lista de chequeo que definen lo siguiente: ¿Se cuenta con los documentos de: diseño detallado, plan de contingencias, informes de las pruebas piloto realizadas, informes de activación de políticas de seguridad, pruebas de funcionalidad y actas de cumplimiento a satisfacción de los elementos intervenidos respecto a la implementación del protocolo IPV6?:	**Información obtenida:** Actualmente el tema de IPV6 se encuentra en etapa de planeación y avanzo en lo que respecta a los estudios previos. Hasta el momento el contrato no se ha suscrito. Insumos obtenidos resultado de la evaluación: estudios previos, estudio de mercado, la ficha técnica, los inventarios, análisis preliminar, análisis del sector y planes en versiones preliminares. La subdirección de contratación por su parte elaborará los RFPs y procederá con la publicación mediante concurso de méritos. Se informa que la ficha técnica fue desarrollada con base al lineamiento del MinTIC. La ficha contiene el dimensionamiento de la migración, duración, forma de implementación, se define como se realizarán las ventanas y la indisponibilidad aceptable. “Reglas a seguir”. La dirección TIC presento el proceso a la subdirección de contratación en la semana del 17 al 21 de mayo 2021. Respecto al año 2020, se elaboraron los documentos preliminares como son: El diagnostico, el plan de diagnóstico y actualización de los inventarios. Se estima que el proceso se contrate en el mes de Julio del 2021 y se tiene contemplado 7 meses para la implementación del cronograma. Se informa que el documento de diseño detallado, el plan de diagnóstico, plan de migración y el plan de direccionamiento le corresponde entregar al contratista adjudicado. Proceso radicado en la subdirección de contratación, mediante el id nro.: 2021IE12440 del 7 de mayo. Fases acordadas; Planeación, implementación y pruebas.
Situación encontrada	Los diferentes documentos expuestos que son la base de las recomendaciones sugeridas por el FURAG y que son el resultado de la implementación de protocolo IPV6, a la fecha siguen sin ser elaborados, lo que conlleva a un cumplimiento parcial de la política de Gobierno Digital en lo que respecta a lo definido por la resolución 2710 del 2017 y la modificación de la misma en la resolución 1126 de 2021. En el capítulo 10 de este documento, se encontrará documenta la acción para abordar el riesgo.

Segundo Hallazgo

Respecto a la pregunta: ¿Se han ejecutado al 100% los proyectos y la operación de TI?

Caso1 analizado:

Información obtenida:

Se procede con la revisión del cumplimiento de los proyectos con respecto a la primera actividad del proceso definida así: "Gestionar los recursos financieros y humanos asignados a la gestión de TI de la SDS e implementar la estrategia de tecnologías de la información y comunicaciones". Para ello se informa que se tienen definidos 2 proyectos, 7785 y 7788 que a continuación vamos analizar.

Proyecto TIC 7785: IMPLEMENTACIÓN DE LA ARQUITECTURA EMPRESARIAL AÑO 2020	
Programado:	$7.726.527.280
Ejecutado (93%)	$7.204.915.049
Proyecto TIC 7788: TRANSFORMACIÓN DIGITAL EN SALUD BOGOTÁ Año 2020	
Programado:	$ 2.451.018.187
Ejecutado (82%)	$2.002.416.913

Respecto a la revisión de los proyectos de inversión acorde a la información suministrada, se desconoce la utilización de los montos sobrantes ya que no encuentra justificación para las actividades id: 7775-01-1.2, 1.5 y 2.7, esto mismo ocurre en el proyecto nro. 7788, por lo que se considera una debilidad por cuanto el control y el detalle que justifica cada actividad no se documenta. Se consulta directamente al director TIC, el cual informa que la operación se cumplió al 100% y los recursos que sobraron fueron liberados, se solicitó el soporte de dichas liberaciones, sin embargo, no fueron entregados.

Documento consultado: SEG DIC 7785 – implementación Arquitectura Empresarial y el intercambio.xlsx

Situación encontrada

Frente al control respecto a los diferentes proyectos de inversión mediante el archivo Excel suministrado, no se evidencia justificación o descripción de la utilización o destino que los montos sobrantes para las actividades identificadas id: 7775-01-1.2, 1.5 y 2.7, esto mismo ocurre en el proyecto nro. 7788, por lo que se considera una debilidad por cuanto el control y el detalle que justifica cada actividad no se tiene, luego es no eficiente. Se consulta al director TIC e informa que la operación se cumplió al 100% y los recursos que sobraron fueron liberados, se solicitó el soporte de dichas liberaciones, sin embargo, no fueron entregados.

En el capítulo 10 de este documento, se encontrará documenta la acción para abordar el riesgo.

Caso2 analizado:

Información obtenida:

Se procede con la revisión al cumplimiento de la tercera actividad del proceso definida así: "Realizar las adquisiciones de bienes servicios de TIC requeridas para satisfacer las necesidades de las partes interesadas". Frente esto, consultamos el documento de seguimiento a las contrataciones de la dirección TIC del año 2020 de cara al Proyecto 7788, e identificamos que se suscribieron 21 contratos por valor de $2002.416.913, que coincide con el valor ejecutado del mismo año. Consultando el documento aportado identificamos que 6 contratos

	continúan su ejecución en el año 2021 y se constituyen pagos a través de reservas presupuestales. Dentro PAA inicial se tenían concebidos 34 iniciativas de adquisición, sin embargo, la ejecución final solo 23 de las iniciativas fueron tramitadas a contratación, mientras que 4 iniciativas no se llevaron a cabo y no se encontró justificación alguna en el tablero de control y otras 7 iniciativas se identificaron que no tiene presupuesto asignado. Documento consultado: Seguimiento contratación TIC 2020 cierre.xlsx Proyecto 7785: Mediante el documento de seguimiento a las contrataciones de la dirección TIC, se tienen 68 contratos x valor de: $7204.915.049, que coincide con lo ejecutado. Realizando los filtros en el tablero, identificamos lo siguiente: 17 iniciativas sin presupuesto, 2 tiene presupuesto, pero no se tramito contrato e identificamos 49 iniciativas que tienen contrato suscrito. Respecto a la contratación del año 2021, se tiene contemplado suscribir 17 contratos de los cuales 2 están en contratación que son las iniciativas para (arquitectura empresarial e IPV6) y el resto está en proceso precontractual (en estudios previos, fichas, otros). Para el seguimiento de los proyectos del año 2021 mediante consulta se obtienen 102 ítems de cara al proyecto 7785 de los cuales 24 ya se suscribieron y 84 no tienen avance. Dicha información no permite tener certeza si la operación está al 100%.
Situación encontrada	De acuerdo con la información suministrada que responde a los informes de seguimiento y contratos en curso y finalizados, la dirección TIC no cuenta con un control o informe solido que permita determinar si los proyectos y la operación se han ejecutado al 100%. Es importante señalar que se conoce el estado de los elementos por separado o individual, pero no se tiene el todo, Por lo anterior, no se logra determinar con exactitud si la operación fue realizada al 100%. El riesgo corresponde a la información inexacta para la toma de decisiones lo cual constituye una debilidad del proceso. En el capítulo 10 de este documento, se encontrará documenta la acción para abordar el riesgo.

Tercer Hallazgo	
Respecto a la pregunta: ¿Se cumple con todos los criterios de accesibilidad web, de nivel A y AA definidos en la NTC5854, para todos los otros procedimientos de la entidad disponibles en línea y parcialmente en línea?	**Información obtenida:** Respecto a la accesibilidad para las personas con discapacidad visual, se consulta el portal WEB: saludcapital.gov.co, el cual nos permite validar criterio de accesibilidad como son: cambiar el tamaño del texto y la luminosidad del sitio, entre otros. En el mismo portal podemos encontrar el banner denominado: Agilinea, y es aquí donde se identifican implementados 11 trámites en línea y 2 tramites parcialmente en línea. Se procede a consultar cada uno de los 11 tramites en línea y se evidencia que las características de accesibilidad se pierden al momento de ingresar al siguiente vinculo o URL, se evidencia que la funcionalidad no es completa al momento de saltar al siguiente vinculo por lo que se comprueba que la accesibilidad para las personas con discapacidad visual esta implementada de manera parcial. Se toma pantallazos de las consultas realizadas. Archivo consultado: Criterio de accesibilidad WEB para personas con discapacidad visual.docx
Situación encontrada	Se evidencia que las características de accesibilidad para los 11 trámites en línea se pierde, todo ocurre al momento de ingresar al trámite correspondiente, el vínculo o la URL al que salta, pierde las características. Se considera una debilidad toda vez que la accesibilidad para las personas con discapacidad visual para los trámites en línea esta implementada de manera parcial, lo que puede derivar en reclamaciones e inconformidad con el servicio prestado. Se toma pantallazos de las consultas realizadas. En el capítulo 10 de este documento, se encontrará documenta la acción para abordar el riesgo.

Cuarto Hallazgo	
Respecto a la pregunta: ¿Se han analizado y explotado los datos capturados por medio de dispositivos de internet de las cosas (IoT) en la entidad?	**Información obtenida:** Se informa que respecto al análisis y explotación datos no se ha avanzado, se han hecho acercamientos con la dirección administrativa, pero a la fecha no se tienen más avances. Se informa que no se han podido concretar las fechas de reuniones por las circunstancias actuales. Se consulta el avance por componentes y se evidencia lo siguiente: 1. identificación y priorización de la infraestructura y servicios de IoT que requiere o se necesita para adelantar iniciativas de ciudad o territorio inteligente: Se realizó la identificación de cámaras de CCTV, control de acceso, monitores de UPS y cuartos fríos y digiturnos. 2. Estructuración de la arquitectura de la infraestructura de IoT a desplegar en la ciudad o territorio: Se creó la red VLAN que segmentan el tráfico de dispositivos IoT. 3. Instalación y despliegue de sensores y redes de IoT: Se cuenta con Sistemas de CCTV instalados, control de acceso, monitores de UPS, cuartos fríos y cámara sensor de temperatura. Activo consultado: IP EQUIPOS DE SEGURIDAD Y CONTROL.xlsx
Situación encontrada	Los dispositivos IoT identificados que hacen parte del inventario, en lo que respecta al análisis y explotación de los datos capturados por estos dispositivos a la fecha no se ha realizado, lo que conlleva a un incumplimiento con la implementación de la política de Gobierno digital, decreto 1008 del 2018 y afectara el desempeño de la entidad frente a otras. En el capítulo 10 de este documento, se encontrará documenta la acción para abordar el riesgo.

7.2 SEGURIDAD DIGITAL

MARCO CONCEPTUAL

Política de Seguridad Digital

El propósito de esta política es contrarrestar el incremento de las amenazas informáticas que afecten significativamente, y afrontar retos en aspectos de seguridad cibernética.

La política busca que las entidades puedan abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales, para ello el Gobierno Nacional expidió el documento CONPES 3701 “Lineamientos de política para ciberseguridad y ciberdefensa” creando un ambiente y unas condiciones para brindar protección en el ciberespacio. El principal logro alcanzado de la presente política, consistió en el fortalecimiento de la institucionalidad por medio de la creación de nuevas instancias tales como el Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional, el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia, el Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia, el Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL), se delegó para la protección de datos a la Superintendencia de Industria y Comercio, la Subdirección técnica de seguridad y privacidad de tecnologías de información del MinTIC, el Comité de ciberdefensa de las Fuerzas Militares, y las Unidades cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana.

POLÍTICA NACIONAL DE SEGURIDAD DIGITAL - CONPES 3854 de 2016

Posteriormente se expide este documento que permite al Gobierno, las organizaciones públicas y privadas, la fuerza pública, la academia y los ciudadanos en general, cuenten con un entorno digital confiable y seguro. Define la visión estratégica que pretende que los colombianos hagan uso responsable del entorno digital y fortalezcan sus capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

Objetivo general: La política consiste en que los ciudadanos, las entidades del Gobierno y los empresarios conozcan e identifiquen los riesgos a los que están expuestos en el entorno digital y aprendan cómo protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos. Así mismo se busca educar y fomentar una cultura a nivel país que permita generar recomendaciones tales como: Utilizar contraseñas de alta seguridad y cambiarlas periódicamente, no dejar el correo abierto en sitios públicos, no entregar las claves a nadie, tener cuidado con el correo spam, tener cuidado con el correo phishing, entre otros cuidados.

POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL - CONPES 3995 del 2020

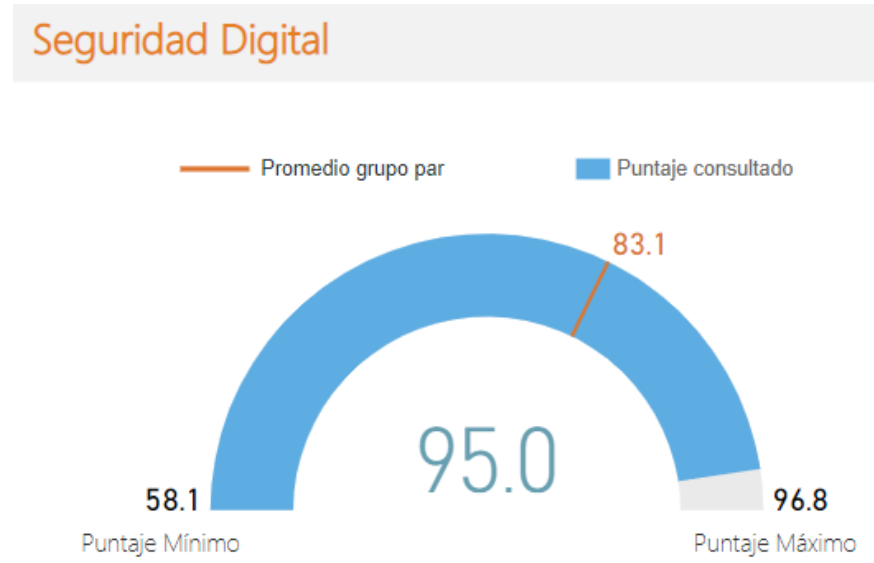
Documento que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital. Para alcanzar este objetivo, en primer lugar, se fortalecerán las capacidades en seguridad digital de los ciudadanos, del sector público y

del sector privado del país; en segundo lugar, se actualizará el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

La política contempla todos los sectores del país y requerirá de la participación de las diferentes entidades e instancias tales como la Consejería Presidencial para Asuntos Económicos y Transformación Digital, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional y el Departamento Nacional de Planeación, entre otras. El logro de las condiciones descritas se dará en el período comprendido entre 2020 y 2022, con una inversión total aproximada de 8.342 millones de pesos.

Medición del desempeño de Política de Seguridad Digital

Resultado general para la SDS:



Cumplimiento de la política en la actualidad es del 95%

Fuente de consulta:
https://app.powerbi.com/view?r=eyJrIjoiMTZiZDU5MTQtMjNjNi00OTczLTg0ZjktMzRkNTkyYzg3ODdkIiwidCI6IjU1MDNhYWMyLTdhMTUtNDZhZi1iNTIwLTJhNjc1YWQxZGYxNiIsImMiOjR9

Resultado de la medición, podemos observar que la política de Seguridad Digital en la entidad requiere implementar otros elementos o componentes faltantes para lograr su cumplimiento al 100%.

Análisis de información frente este objetivo

Se llevaron a cabo 5 mesas de trabajo soportado mediante las listas de verificación definidas y los registros de actas de participación de los referentes designados, dando respuesta a todas las preguntas formuladas. Los insumos para la elaboración de las preguntas corresponden a: 1. el informe Furag respecto a la brecha o elementos faltantes para la implementación de la política, 2. el informe final resultado de auditoria al SGSI del año 2020 y 3. Se toma la norma certificable ISO 27001:2013 y se eligen los requisitos generales respecto al ciclo de vida PHVA, se enfatiza en los requisitos que permiten determinar el mantenimiento y mejora del sistema en la entidad. Los resultados se presentan de manera sintetizada en este capítulo y el detalle a cada punto o pregunta se encontrará en los papales de trabajo, archivos denominados: Checklist Parte1- Seguridad Digital V1 -JunFinal.docx y Checklist Parte2- Seguridad Digital V1 -JunFinal.xlsx
Nota: Los hallazgos identificados en este componente resultado de la evaluación realizada, se consideran debilidades y derivan en acciones para abordar el riesgo, las cuales serán justificadas en capítulo 10 de este documento.

Preguntas Formuladas:	**32**
Recomendaciones validadas	15
Requisitos de Norma validados	17
Recomendaciones Cumplidas:	13
Requisitos de Norma incumplidos:	5
Acciones para Abordar riesgos	4
No Conformidades	1
Porcentaje de cumplimiento respecto a la evaluación	78%

Primer Hallazgo	
Respecto a la pregunta: ¿Se reconoce como instancia de la política de seguridad digital la Coordinación Nacional de Seguridad Digital (Presidencia de la República)? ¿En qué documento propio de la entidad se especifica dicha directriz?	**Información obtenida:** Se informa que el comité técnico de la seguridad de la información liderado por la dirección TIC, hasta el momento no han tenido ningún acercamiento con la coordinación Nacional de Seguridad Digital de la Presidencia de la República, se desconoce su rol y las funciones que ejerce para el fortalecimiento de la seguridad nacional y territorial, así mismo en ninguno de los documentos que tiene que ver con la seguridad de la información en la entidad está siendo mencionado.
Situación encontrada	Respecto a la normativa y específicamente en lo que se refiere en materia a la seguridad digital y gobernanza en Colombia, se informa que existe la coordinación nacional de seguridad digital que dispuso el documento CONPES 3854 aprobado en 2016. Esta figura se encuentra en cabeza de la Consejería de Asuntos Económicos y Transformación Digital de la Presidencia de la República. La consejería actúa como ente asesor para la presidencia de la República y entidades del Gobierno nacional en temas de Seguridad Digital. Por lo anterior se debe solicitar a esta coordinación el apoyo y retroalimentación continua de los temas

	allí se definan. Esta instancia no se está teniendo en cuenta para el ejercicio respectivo. En el capítulo 10 de este documento, se encontrará documenta la acción para abordar el riesgo.

Segundo Hallazgo

Respecto a la pregunta: ¿Se han fortalecido las capacidades en Seguridad digital del talento humano de la entidad, a través de su participación en las convocatorias de encuentros de Gestores de Incidentes Cibernéticos convocados por el CSIRT Gobierno?	**Información obtenida:** Los referentes de TIC, informan que hasta el momento no han sido convocados y tampoco se ha participado de los encuentros generados o programados. Los escenarios en los en los que la SDS ha sido convocada es por el CSIRT y se ha mantenido contacto constante frente posibles amenazas e incidentes de seguridad de Digital que surjan. Por su parte la Alta Consejería para las TIC ha dado a conocer el tema de gestión de incidentes y el protocolo a seguir. Como evidencia se comparte la guía de gestión de incidentes del 21 de mayo del 2021.
Situación encontrada	Respecto a la normativa en materia de seguridad digital, existe la Unidad de Investigación Criminal de la Defensa de la Policía Nacional – DIJIN, este organismo ha convocado a diferentes encuentros de gestores de incidentes informáticos CSIRT con la participación de la Interpol y el Ministerio de las TIC generando diferentes recomendaciones. Hasta el momento la SDS no ha participado de estos encuentros ya que se desconocía. Por lo anterior, se debe solicitar la vinculación, notificación y lograr participar de los diferentes encuentros que programe este organismo, así mismo solicitar retroalimentación continua de los temas allí se impartan, permitiendo el fortalecimiento de las capacidades en seguridad digital en la SDS. En el capítulo 10 de este documento, se encontrará documenta la acción para abordar el riesgo.

Tercer Hallazgo

Respecto al numeral 5.3 Roles organizacionales, responsabilidades y autoridades, literal b) informar a la alta dirección sobre el desempeño del SGSI. ¿Cómo se está reportando el desempeño y cada cuanto se hace? **Respecto al numeral 9.1 Seguimiento, medición, análisis y evaluación** **¿Cómo la organización evalúa el desempeño de la seguridad de la información y la efectividad del SGSI? ¿Conserva información documentada como evidencia de los resultados del monitoreo y de la medición?**	**Información obtenida:** Se informa que el escenario estratégico e idóneo definido para presentar los resultados del desempeño del SGSI es el comité institucional de gestión y desempeño, en el último comité realizado, se presentó el avance de la política de la seguridad de la información. Como segunda instancia se tienen establecidas las mesas técnicas de gobierno y seguridad digital en el cual participa el director TIC. Se soporta mediante las actas de las reuniones y se constata con el acta del Comité institucional de gestión y desempeño realizado el 7 de septiembre y en el mes de noviembre año 2020. De otra parte, en las mesas técnicas realizadas, se cuenta con 3 actas: 6 de mayo, 4 de septiembre y 13 de noviembre del 2020 y del año 2021: se tienen 2 mesas técnicas, una del 22 de enero y la otra del 19 de abril 2021, en dichas mesas se presentaron los logros y retos. Respecto al seguimiento y avance de MIPG, el reporte se hace trimestral y quien presenta los resultados es el referente del departamento de planeación institucional y calidad. Para el 4 Cuarto trimestre del 2020 se presentaron los resultados de la política de seguridad digital, donde se reporta un cumplimiento del 100%. Documento denominado: informe de seguimiento trimestral MIPG cuanto trimestre 2020 seguridad digital.xlsx, Así mismo se consulta los resultados del primer trimestre del 2021, con un avance del 5% en todas las actividades definidas. Respecto a los 5 indicadores definidos en el año 2020 que hizo parte del plan de mejora de la auditoría realizada en ese momento,

Respecto al numeral 9.3 Revisión por la dirección, ¿La alta dirección ha revisado el SGSI a intervalos planificados, para asegurar su conveniencia, suficiencia y efectividad continua?	evidenciamos que los resultados de los mismos no han sido obtenidos y divulgados en las diferentes instancias: comité institucional y mesas técnicas. Por lo anterior, el reporte respecto al desempeño del sistema ha sido parcial.
Situación encontrada	Respecto a los 5 indicadores consultados mediante sus hojas de vida y que fueron definidos en el año 2020, evidenciamos que los resultados de los mismos no han sido obtenidos, divulgados o presentados en las diferentes instancias como son: el comité institucional o las mesas técnicas. Por lo anterior, el reporte respecto al desempeño del sistema ha sido parcial. Se deriva una acción para abordar riesgo, toda vez que el desempeño del SGSI se debe fortalecer mediante los resultados de los 5 indicados definidos. A la fecha no han sido puestos en práctica. En el capítulo 10 de este documento, se encontrará documentada la acción para abordar el riesgo.

Cuarto Hallazgo

Respecto al numeral 8.1 Planificación y Control operacional, ¿La organización está planificando, implementando y controlando los procesos necesarios para cumplir con los requisitos de seguridad de la información? ¿Se han implementado los planes para lograr los objetivos de SI?	**Información obtenida:** Se procede a consultar el plan de seguridad de información y el plan de gestión de Riesgos del año 2020 y 2021. Respecto al plan del año 2020, se definieron 6 objetivos de los cuales 3 se cumplieron y los otros 3 presentan un avance parcial. A continuación se detallan. **Objetivo1**: define el "Análisis de Vulnerabilidades", se informa que por parte del proveedor ETB, se cuenta con los informes mensuales que reportan el estado de la seguridad de la red de enero 2020 hasta marzo 2021. Mediante el monitoreo con las herramientas de fortigate para análisis de dispositivos perimetrales. El contrato finalizo en el mes de marzo 2021 por lo anterior, la operación actual la viene realizando profesionales de la dirección TIC. Sin embargo, frente al objetivo puntual del análisis de vulnerabilidades que venía realizando el proveedor con diferentes herramientas que involucraba identificación de IPs, detección de Sistemas operativos, puertos TCP/UDP abiertos, versiones de aplicaciones, vulnerabilidades WEB entre otras, no se siguió realizando desde hace un año, por lo anterior se deriva una acción para abordar riesgo toda vez que pueden existir huecos de seguridad o debilidades que no han sido identificadas, lo que pudiera conllevar un posible ataque y explotación de vulnerabilidades. Se considera una oportunidad de mejora, con el fin de reforzar el análisis de vulnerabilidades en lo que respecta a puertos abiertos TCP/UDP, versiones de sistemas operativos, aplicaciones, vulnerabilidades web entre otros y con ello aplicar las remediaciones adecuadas. Se informa que en el mes de febrero 2021, se probó el demo DARKTRACE que permitió generar un informe. Hasta el momento ninguna de las recomendaciones del informe se ha implementado por lo que el riesgo persiste en algunos elementos de la infraestructura. **Objetivo 3**: Plan de continuidad, se informa que hasta el momento la entidad no cuenta con un plan de continuidad de negocio o PCN, lo que se tiene es un plan de contingencia a nivel de tecnología, se consulta el documento denominado: esquema inicial de continuidad de negocio, el cual está en construcción. Se informa que en el mes de abril 2021, se tenía contemplado realizar las entrevistas, sin embargo por efectos de la pandemia no se pudo realizar, la definición del comité de crisis y quienes la componen no se tiene, así como tampoco se ha definido el RTP y RPO.

	Objetivo4: el componente BIA está en construcción y a la fecha no se tiene más avances dado que no se han realizado las diferentes entrevistas.
Situación encontrada	**Objetivo 1:** análisis de vulnerabilidades más recomendada que venía realizando el proveedor con diferentes herramientas que involucraba: identificación de IPs, detección de Sistemas operativos, puertos TCP/UDP abiertos, versiones de aplicaciones, vulnerabilidades WEB entre otras, desde hace un año no se viene realizando, por lo se deriva un riesgo, toda vez que pueden existir huecos de seguridad o debilidades que no han sido identificadas, lo que pudiera conllevar un posible ataque y explotación de vulnerabilidades. **Objetivo 3**: Plan de continuidad, se informa que hasta el momento la entidad no cuenta con un plan de continuidad de negocio o BCP, se cuenta con algunos elementos del plan como son: el plan de contingencia a nivel de tecnología y el esquema inicial de continuidad de negocio, el cual está en construcción. En el mes de abril 2021, se tenía contemplado la realización de entrevistas, sin embargo por efectos de la pandemia no se pudo realizar. No existe el comité de crisis y tampoco se ha definido el RTP y RPO. **Objetivo4**: Componente BIA está en construcción y a la fecha no se tiene más avances dado que no se han realizado las diferentes entrevistas. **Objetivos 3 y 4** del plan de Seguridad de información año 2020 no se cumplió y están incorporados en el plan año 2021, que a la fecha sigue sin avance. Se presentaron los siguientes documentos: borrador plan de continuidad de la operación SDS.pdf, BCP presentación 3.ppt y esquema inicial continuidad de negocio.pdf En el capítulo 10 de este documento, se encontrará documentada la acción para abordar el riesgo.

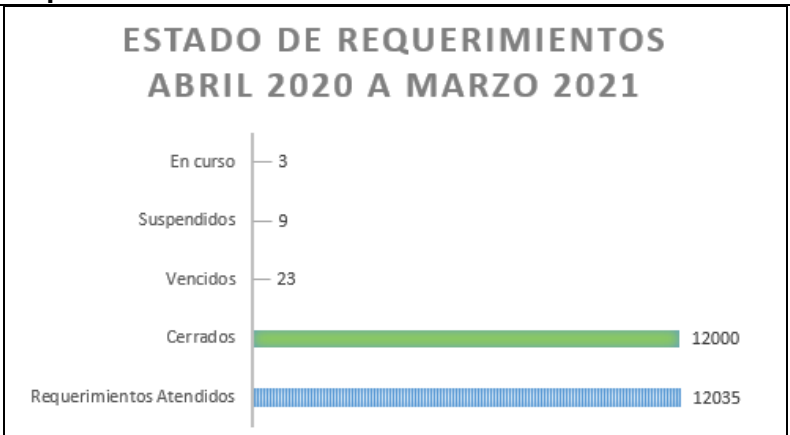
Quinto Hallazgo	
Respecto al numeral 8.3 Tratamiento de riesgo de la seguridad de la información **¿La entidad cuenta con resultados del tratamiento del riesgo de la seguridad de la información?**	**Información obtenida:** Respecto al plan de tratamiento de los 5 riesgos transversales de seguridad de la información identificados, se informa que por efectos el distanciamiento que produjo la pandemia por COVID19, el tema no se pudo realizar. Este requisito también fue evaluado en la auditoría realizada en el año 2020 y genero la acción número 10,6 que a la fecha se sigue cumplirse, Se informa que una vez se diligencie la matriz de riesgos por parte de los referentes en cada dependencia, lo cual es un compromiso para el próximo 11 de julio del 2021, se podrá hacer el respectivo análisis y en octubre se espera tener el informe final consolidado. Se considera una “No Conformidad”, toda vez que se incumple con el requisito 8.3 y se evidencia una reincidencia del hallazgo. Una vez el plan de tratamiento se defina e implemente, se demostrara su eficacia.
Situación encontrada	Planes de tratamiento sin actualizar, se informa que por efectos el distanciamiento que produjo la pandemia por COVID19, el tema no se pudo realizar. Existe el compromiso por parte de los referentes para el próximo 11 de julio del 2021 y con ello se podrá hacer el respectivo análisis. Este requisito también fue evaluado en la auditoría realizada en el año 2020 y conllevo acción de mejora número 10,6 que a la fecha se sigue cumplirse. Se determina una reincidencia con el requisito por tanto se sustenta en una no conformidad. En el capítulo 10 de este documento, se encontrará documentada la acción para abordar el riesgo.

7.3 MANEJO DE REQUERIMIENTO E INCIDENTES

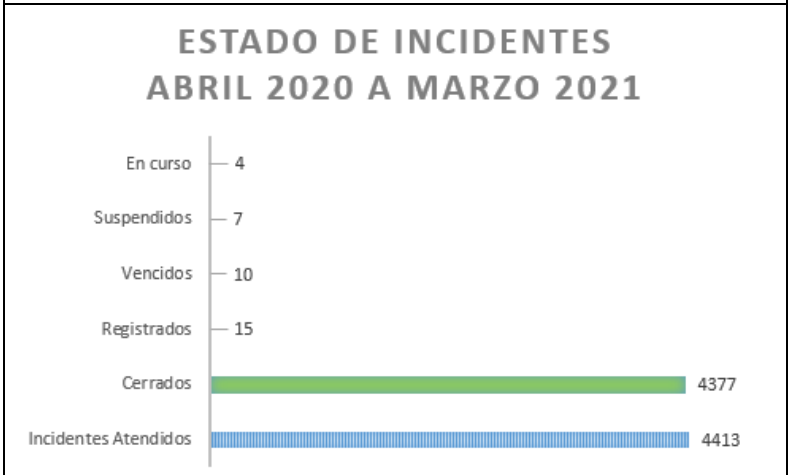
MARCO CONCEPTUAL

Que es un incidente:
Es toda interrupción o reducción de la calidad no planificada del servicio, degradación de la calidad, o la falta de un componente en un servicio. Pueden derivarse de fallos o consultas reportadas por los usuarios, la mesa de servicios o por alguna herramienta de monitorización de eventos. La Gestión de Incidencias corresponde a un proceso ITIL enmarcado en la fase de Operación del Servicio, el principal objetivo en restaurar cuanto antes la operativa normal del servicio minimizando el impacto negativo en las operaciones del negocio. Las actividades más relevantes del proceso son: Registro, clasificación, análisis, resolución y cierre. Actualmente la SDS gestiona sus incidentes mediante la herramienta Aranda software.
Que es un requerimiento:
Se refiere a todas las solicitudes que generan los usuarios, corresponde a una solicitud de soporte IT, sin que haya algún evento que esté interrumpiendo el servicio o reducción en la calidad de dicho servicio. Es un cambio estándar que implica un riesgo bajo, relativamente común, y habitualmente sigue un procedimiento o una instrucción de trabajo. Ejemplos de requerimientos: Creación de una cuenta de usuario a la red o al correo, Desbloqueo de cuenta por vencimiento, cambio de contraseñas, habilitación de un punto de red, configuración de impresoras, instalación de software, entre otros. Las actividades más relevantes de ese proceso son: Registro, clasificación, resolución de la solicitud y cierre. La Gestión de requerimientos corresponde a un proceso ITIL enmarcado en la fase de Operación del Servicio.
Que es Aranda Software:
Es una solución que permite gestionar y resolver (incidentes y requerimientos) asociados a los servicios y la infraestructura tecnológica de la entidad, ofreciendo una mesa de servicio con un único punto de contacto para generar, administrar, responder y monitorear todos los casos teniendo en cuenta las mejores prácticas de ITIL.
Que es un SLA o ANS
SLA o acuerdo de nivel de servicio, es un contrato o documento de servicios IT donde se recogen los objetivos del mismo, las características de los servicios contratados, las responsabilidades, tanto del proveedor como del cliente y, finalmente, las acciones a realizar en caso de incumplimiento (compensaciones o sanciones)

Medición de Requerimientos e Incidentes



Se determina una eficacia del 99,7%



Se determina una eficacia del 99,1%

Resultado de la medición, comparando los requerimientos e incidentes recibidos vs los cerrados o solucionados se obtiene un eficacia del 99,4%

Análisis de información frente este objetivo

Se llevaron a cabo 2 mesas de trabajo soportado mediante las listas de verificación definidas y los registros de actas de participación de los referentes designados, dando respuesta a todas las preguntas formuladas. Los resultados se presentaran de manera sintetizada en este capítulo y el detalle a cada punto o pregunta se encontrará en los papales de trabajo, archivo denominado: Checklist - Requerimientos e Incidentes V1 – JunFinal.docx

Nota: Los hallazgos identificados en este componente resultado de la evaluación realizada, se consideran debilidades y derivan en acciones para abordar el riesgo, las cuales serán justificadas en capítulo 10 de este documento.

Preguntas Formuladas:	**14**
Aspectos Cumplidos	9
Aspectos No cumplidos	5
No Conformidades	0
Acciones para abordar riesgo	2
Porcentaje de cumplimiento respecto a la evaluación	56%

Primer Hallazgo	
Respecto a la pregunta: ¿Constatar de manera general cuantos de los requerimientos e incidentes respecto al alcance siguen en estado Abierto, en progreso, en curso o activos en ARANDA?	**Información obtenida:** Se informan que los requerimientos en estado "Abierto" son equivalentes en ARANDA al estado "REGISTRADO", que mediante consulta a la base suministrada, no se encontraron casos. Esto demuestra que está siendo eficiente este paso dentro del procedimiento, toda vez que las solicitudes que son asignadas al especialista, se procede a realizar el cambio del estado a "EN CURSO" De otra parte el estado: "En progreso", es aplicable a los casos o requerimientos que se encuentran en estados "vencidos", "suspendidos" y "en curso", que para efectos del ejercicio da un total de 35 casos distribuidos de la siguiente forma. 23 requerimientos se encuentran en estado vencido, 9 suspendidos y 3 en curso. Se procede a consultar los requerimientos en estado "SUSPENDIDO", que corresponde a los casos en donde el técnico no cuenta con la disponibilidad para atender el requerimiento, o el técnico se no logro encontrar al funcionario ya que el mismo se ausento, o se encuentra en teletrabajo, en estos casos el tiquete de requerimiento se suspende, debido al procedimiento definido, el técnico realiza 3 visitas en 3 días distinto, no existe una cuarta visita por lo tanto el requerimiento pasa a estado CERRADO y se justifica. Se toma el id: 37109 caso al azar de ejemplo y se verifica mediante el historial que el requerimiento lleva más de 3 meses abierto y sigue sin atención. Se toma captura del historial del caso, fecha de registro el 10 de marzo. Los 9 requerimientos en estado suspendidos presentan el mismo comportamiento. Se informa que el rol de dispacher o coordinador realiza la reasignación de requerimientos o tiquetes a los diferentes especialistas, así mismo se informa que el dispacher realiza control semanal de tiquetes, sin embargo, explica que por efectos de la finalización del contrato con ETB, esta actividad se dejó de realizar. Se consulta un segundo caso, id: 37684 requerimiento en estado: "en curso" que a la fecha sigue abierto y sin avances documentados por el especialista, después de 2 meses el requerimiento sigue sin ser atendido. Se consulta un tercer caso, id: 36955 requerimientos en estado "Vencido", el caso fue registrado en el mes de marzo y a la fecha sigue sin atención y solución. Se concluye que a partir de los diferentes casos consultados que se encuentran en un estado diferente a CERRADO, la gestión de los mismos no está siendo

	eficiente, toda vez que los requerimientos e incidentes no están siendo atendidos por los especialistas asignados... Así mismos se evidencia que los ANS superaron el tiempo definido sin tomar una acción al respecto. La situación expuesta afecta la eficiencia de la mesa de servicios, es por eso que se genera una acción para abordar riesgo toda vez que existen requerimientos que a la fecha siguen sin ser atendidos y solucionados, lo cual deriva en reclamaciones e insatisfacción por parte de los usuarios finales. La acción apunta a reforzar el control que venía realizando el coordinador y reunirse con los especialistas para determinar acciones a seguir.
Situación encontrada	A la fecha 35 requerimientos se encuentran sin ser solucionados y se distribuyen de la siguiente forma: casos vencidos: 23, suspendidos: 9 y en curso: 3. A nivel de incidentes, se cuenta con un total de 36 incidentes sin ser solucionados y están distribuidos de la siguiente forma: Casos registrados: 15, Casos vencidos: 10, suspendidos: 7 y en curso: 4. Se informa que el dispacher o coordinador no está realizando la gestión correspondiente de los casos, explica que por efectos de la finalización del contrato con ETB, esta actividad se dejó de realizar. La situación que afecta la eficiencia de la mesa de servicios. Nota: Estos casos sin solución, tiene más de 2 meses de haber sido registrados en la herramienta y observamos como patrón similar y es que el especialista asignado a estos casos es la misma persona. En el capítulo 10 de este documento, se encontrará documenta la acción para abordar el riesgo.

Segundo Hallazgo

Respecto a la pregunta: ¿Cuál es el tiempo comprometido de atención, SLA establecidos y acordados versus el tiempo promedio de atención de los requerimientos e incidentes obtenido de ARANDA?	**Información obtenida:** Se identifica que varios de los requerimientos e incidentes consultados tomaron más de 2 meses en ser solucionados, no se evidencian notificaciones o alertas respecto al incumplimiento del SLA. Mediante consulta a la base de requerimientos, se toma el TOP 10 de los casos o requerimientos con mayor tiempo de atención, lo cual nos permite demostrar que los SLA definidos para la atención de requerimientos no se está aplicando. Se determina que un requerimiento puede ser atendido en 5 minutos o puede tomar más de 2 o 6 meses y no pasa nada. A continuación, se presenta el TOP10 de requerimientos con mayor tiempo de atención, con lo cual superan los SLAs definidos en la herramienta.

Requerimientos		Incidentes	
No. Caso	**Tiempo Promedio Atención**	**No. Caso**	**Tiempo Promedio Atención**
28646	207,94	15474	101,20
36191	121,95	18145	92,70
35504	118,07	18103	85,11
37037	101,01	18109	84,93
37058	85,15	18102	82,11
37081	78,02	18122	80,90
37429	75,08	18218	80,11
37741	62,97	15575	79,99

	37090 | 62,89 | 14250 | 78,91
Situación encontrada	Existen requerimientos e incidentes que están siendo atendidos y solucionados por fuera de los SLA definidos, casos que son solucionados entre los 2 a 6 meses y no ocurre nada frente al procedimiento y la herramienta. Esta situación genera puede conllevar a insatisfacción y deriva en reclamaciones por parte de los usuarios finales o solicitantes. Se propone reforzar el componente de SLA mediante la herramienta ARANDA, de tal forma que genere las notificaciones correspondientes del vencimiento o próximos a vencer y con ello se controlar los tiempos de respuesta. En el capítulo 10 de este documento, se encontrará documenta la acción para abordar el riesgo.

7.4 RESPONSABILIDADES TIC

MARCO CONCEPTUAL

Objetivo del proceso TIC
Gestionar las necesidades en infraestructura tecnológica, soluciones de software, incidentes y requerimientos, seguridad de la información, a través de la implementación de la Política de Gobierno Digital, la administración de los recursos TIC e implementación del Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETIC, con el fin de contribuir a la eficacia y eficiencia de los procesos de la entidad que soportan la continuidad del negocio en materia de tecnologías de la información y comunicaciones
Alcance del proceso TIC
Inicia con la identificación de necesidades y/o requerimientos de Tecnologías de la Información, la definición de la planeación estratégica de TI, y las Comunicaciones - TIC y la formulación de políticas que definen las condiciones de operación a desarrollar; continúa con el desarrollo y mantenimiento de los sistemas de información y la implementación de la infraestructura que soporta la operación, acorde con la Política de Gobierno Digital y Arquitectura empresarial de la Entidad y finaliza con la gestión, uso, apropiación y publicación de la información.
Actividades objeto de verificación para el alcance de la auditoria
1) Realizar la definición de requisitos de software, para desarrollo interno, externo o adquisición de aplicaciones. (Planear) 2) Desarrollar las soluciones de software, o gestionar la adquisición o contratación de desarrollo externo de las soluciones requeridas, y adecuar los ambientes y plataformas necesarios para su operación y control (Hacer). 3) Probar y validar la adecuación y eficacia de las soluciones de software, mejoras y actualizaciones entregadas a la SDS o sus clientes externos, de acuerdo con los requerimientos definidos, evaluando la satisfacción del cliente con la entrega de las soluciones de software desarrolladas y/o adquiridas, el uso y apropiación de las mismas (Verificar). 4) Gestionar los cambios necesarios de las soluciones de software de la SDS de acuerdo con los requerimientos establecidos e incrementar la satisfacción de los usuarios, así como el uso y apropiación de las soluciones en la SDS. (Actuar)

Análisis de información frente este objetivo

Se llevaron a cabo 2 mesas de trabajo soportado mediante lista de verificación definida y registros de actas de participación de los referentes designados, dando respuesta a todas las preguntas formuladas. Los resultados se presentarán de manera sintetizada en este capítulo y el detalle a cada punto o pregunta se encontrará en los papales de trabajo, archivo denominado: Checklist - Responsabilidades V1 -JunFinal.docx
Nota: Los hallazgos identificados en este componente resultado de la evaluación realizada, se consideran debilidades y derivan en acciones para abordar el riesgo, las cuales serán justificadas en capítulo 10 de este documento.

Preguntas Formuladas:	**3**
Aspectos evaluados	3
Aspectos a reforzar	3
No Conformidades	0
Acciones para abordar riesgo	1

Hallazgo	
Respecto a la pregunta: **Si bien es cierto la dirección TIC tiene el gobierno de las tecnologías de la información y comunicación en la entidad y que mediante el proceso definido establece la responsabilidad de realizar los desarrollos de las soluciones de software, ¿Porque varias de las dependencias de la entidad deben disponer de un recurso humano propio que les permita atender sus necesidades de nuevos desarrollos, ajustes o mejoras de sus aplicaciones?**	**Información obtenida:** Respecto a la pregunta, los referentes convocados informan que la dirección TIC no cuenta con el suficiente personal para desarrollar software a demanda, es por eso, que diferentes dependencias atienden sus propias necesidades de desarrollos con recursos propios. Por su parte la dirección TIC da la línea, orientación y realiza las pruebas que haya lugar para garantizar que el producto entregado por las dependencias contenga las características deseadas; en caso de no tenerlas, se generan las observaciones necesarias y se solicitan realizar los ajustes pertinentes. Respecto al código fuente, debe ser entregado a la dirección TIC para su custodia, en caso de que exista una urgencia, con el aval del funcional, la dirección TIC procede hacer las modificaciones si lo requieren, esto aplica en caso fortuito. Se informa que en la actualidad las diferentes dependencias disponen de los recursos propios para garantizar los desarrollos de los requerimientos que se consideran urgentes y que deben realizarse en función del lineamiento de TIC, las dependencias por su parte entregan los desarrollos a TIC y nunca se hace el paso a pruebas sin el visto bueno de TIC. Se informa que así vienen funcionado por varios años, resultado del acuerdo establecido, sin embargo, no existe un soporte que respalde este acuerdo. Así mismo, se informa que existe un lineamiento definido por parte de TIC, el cual debe conocer el desarrollador y ponerlo en práctica, se aclara que el referente TIC se reúne con el funcional y se le explica el tema, sin embargo, se solicita evidencia al respecto y tampoco se entrega. Se informa que los ejercicios de socialización han sido de forma verbal, pero a la fecha no existen registros al respecto. Aplicaciones que han requerido desarrollos propios a la fecha son: SIVIGILA en sus diferentes componentes, el cual se encuentra bajo el control de la dirección de salud pública y otra aplicación es el controlador de derechos que se encuentra bajo la responsabilidad de Aseguramiento. Se informa que

	en este momento se tienen 2 contratistas desarrolladores contratados por la dirección TIC y que están trabajando para la subsecretaria de participación social y servicio a la ciudadanía, las supervisiones se realizan de manera compartida en conjunto con la dirección TIC y haciendo seguimiento del avance del contrato. Se solicita el soporte de las contextualizaciones realizadas y el protocolo a seguir, sin embargo, no se cuenta con dicha información, solo se cuenta con las actas de inicio de los contratos de la supervisión compartida con la dirección la IVC y salud pública. **Respuesta del director frente al tema:** Aduce que es una práctica que se tiene y que no está de acuerdo con la misma; lo que ocurría, es que las dependencias contrataban al personal humano para solucionar sus necesidades que con el tiempo estas necesidades de desarrollo se convirtieron en sistemas de información vitales para las dependencias. A la fecha la dirección TIC da soporte a la entidad frente a las tecnologías de la información y comunicaciones y no cuenta con el personal suficiente para informarle a las dependencias que no contraten y que TIC se encarga de eso. Para superar esta situación, la dirección TIC estableció las siguientes acciones: 1. Desde el año 2020 se definió el plan de desarrollo, el cual contempla proyectos que requerirían desarrollos de iniciativas o necesidades para lo cual incorporará la fábrica de software en el año 2021, mediante esta alternativa, se busca que la Dirección TIC gobierne y lidere todas las necesidades de desarrollo de software de la entidad por lo que las aplicaciones desarrolladas tendrán restricciones de acceso, ya que la fábrica absorberá las funciones que las dependencias tienen hoy en día. Los responsables de las dependencias no podrán hacer ningún tipo modificación sobre el software ya que esta será la responsabilidad de TIC. Respecto a la fábrica de software, se informa que está deberá ser contratada, es por ello que se realizó un estudio de mercado. Este proceso será abierto mediante contrato interadministrativo, pero existe el riesgo que el proceso de licitación se caiga. 2. Los ingenieros que son contratados por las diferentes dependencias tendrán supervisión compartida, es decir entre la dirección TIC y la Dependencia usuaria. Se informa que actualmente los ingenieros contratistas de la dirección de Salud Pública, están bajo la supervisión compartida, es por eso que los nuevos ingenieros vienen presentando los informes mensuales al director TIC, los cuales deben llevar el aval o visto bueno para el respectivo pago. La segunda iniciativa está en curso y se está trabajando con la dirección de aseguramiento. De esta manera es que se está dando cumplimiento a gobierno de TIC. Nota: Esta acción dependerá de los recursos con los que cuentan las diferentes dependencias, por lo que el riesgo en términos de no atender las necesidades de desarrollo de las dependencias, se seguirá materializando, ya que la actividad la realizan contratistas que dependen de otras dependencias sin embargo la supervisión es compartida con la dirección TIC.

Situación encontrada

Algunos requerimientos o necesidades de nuevos desarrollos, ajustes, o mejoras de software, son realizadas por personal contratista de otras dependencias que deben ser contratados con recurso propios para atender estas necesidades. De acuerdo a lo anterior, se determina que la dirección TIC no ejerce en su totalidad la responsabilidad de Gobierno TIC en la entidad, toda vez que las actividades definidas en la caracterización y que se relacionan con el componente de software son realizadas bajo el liderazgo de otras dependencias. A continuación, relaciono las actividades y su estado.

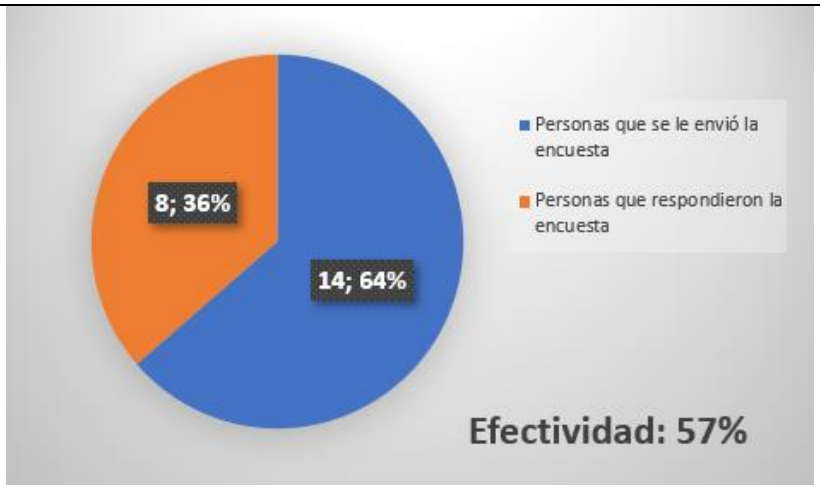
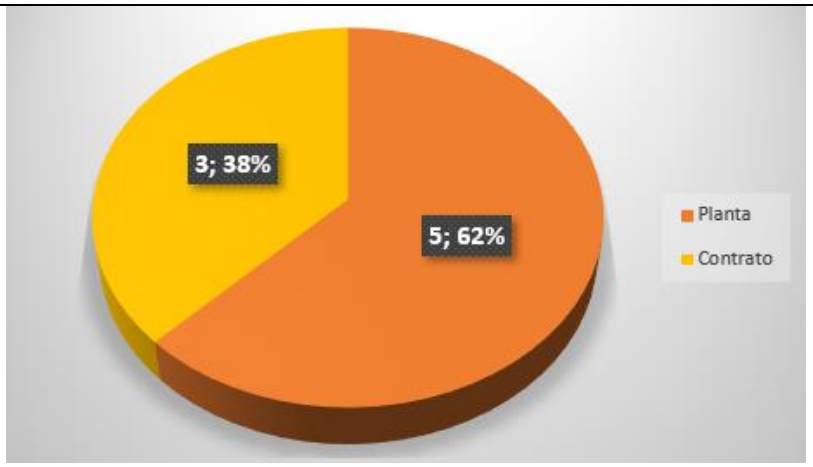
Actividad	Verificación
1. Realizar la definición de requisitos de software, para desarrollo interno, externo o adquisición de aplicaciones	Cumplimiento parcial
2. Desarrollar las soluciones de software	Cumplimiento parcial
3. Probar y validar la adecuación y eficacia de las soluciones de software, mejoras y actualizaciones entregadas a la SDS	Total
4. Gestionar los cambios necesarios de las soluciones de software de la SDS de acuerdo con los requerimientos establecidos, están siendo realizadas por otras dependencias.	Cumplimiento parcial

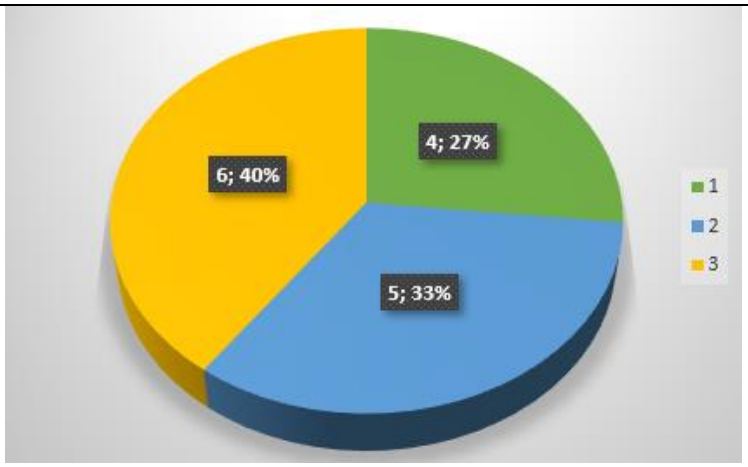
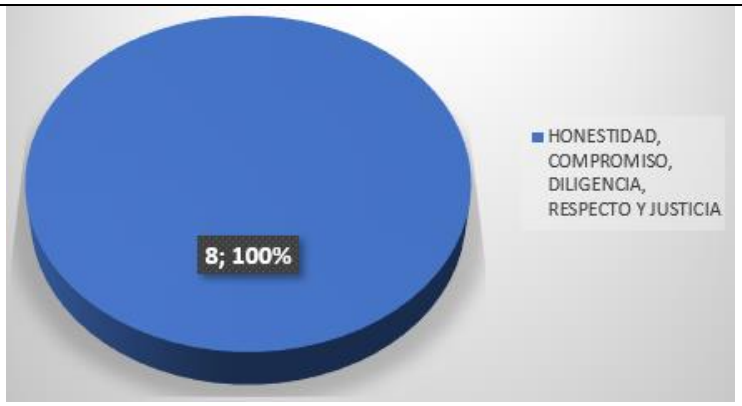
De acuerdo con la información obtenida, los desarrollos de software de forma compartida, pero con mayor responsabilidad de otras dependencias, se viene trabajado por años, resultado del acuerdo establecido, sin embargo, no existe un soporte que respalde este acuerdo. Así mismo, se informa que existe un lineamiento definido por parte de TIC, el cual debe conocer el desarrollador y ponerlo en práctica, se aclara que el referente TIC se reúne con el funcional y se le explica el tema, sin embargo, se solicita evidencia al respecto y tampoco se entrega. Se informa que los ejercicios de socialización han sido de forma verbal, pero a la fecha no existen registros al respecto.

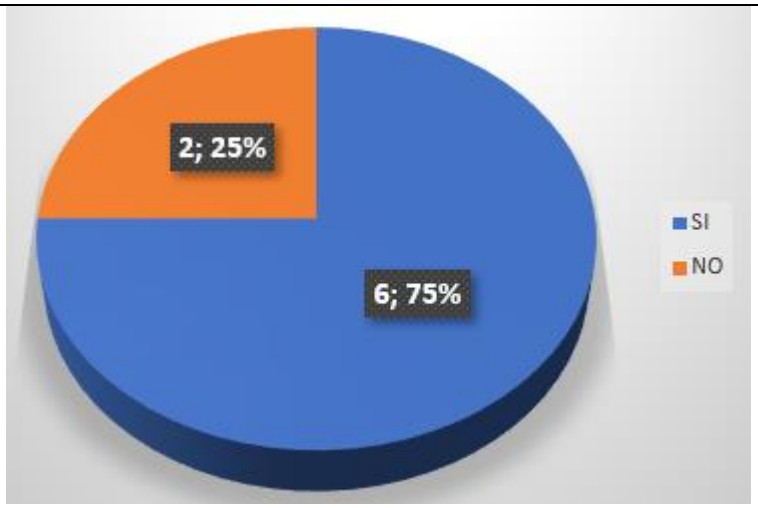
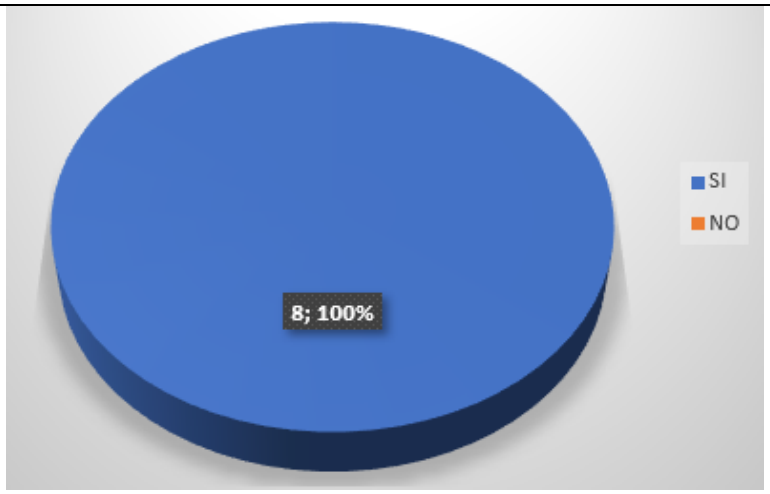
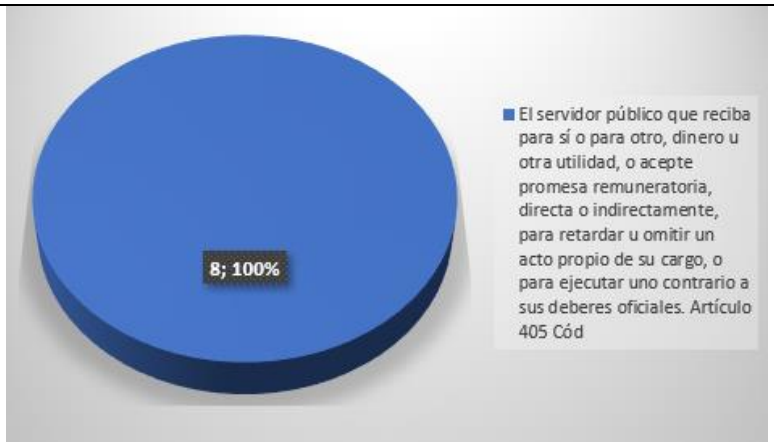
De acuerdo a anterior, se deriva una acción para abordar riesgo, toda vez que el proceso de la contratación de la fábrica de software como solución definitiva no ha sido radicado y una vez esté en proceso precontractual se pudiera caer. Se desconocen los términos técnicos definidos que permitirán elaborar el RFP por parte de la subdirección de contratación, así mismo, no se cuenta con el número de radicado generado que permita constatar el registro y el recibido por parte de esta dependencia. El riesgo en el que se incurre es la perdida de gobernabilidad por parte de la dirección TIC, cumpliendo parcialmente la actividad definida en su proceso, ya que las diferentes dependencias seguirán contratando el personal necesario para atender sus necesidades de software toda vez que la dirección TIC no cuenta con el recurso humano para ello. La acción de mejora apunta a radicar el proceso contractual de cara a la fábrica de software, garantizar que se adjudique, dar inicio a la operación y medir su eficacia. En el capítulo 10 de este documento, se encontrará documenta la acción para abordar el riesgo.

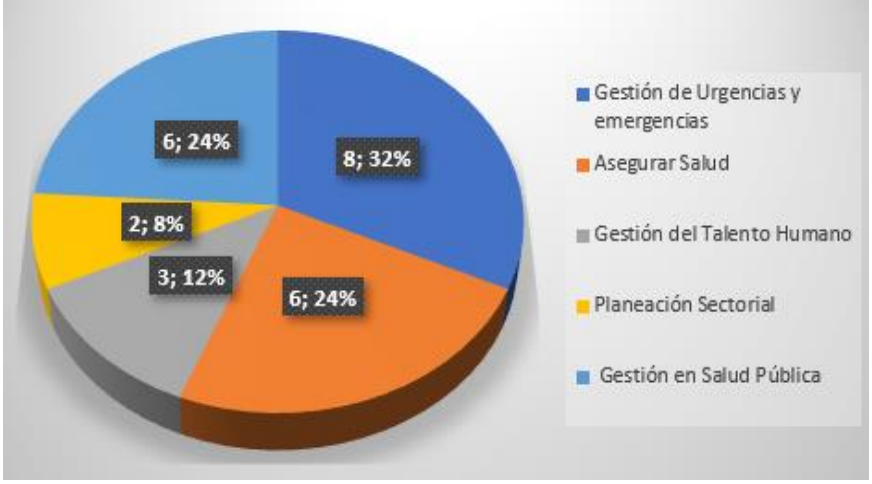
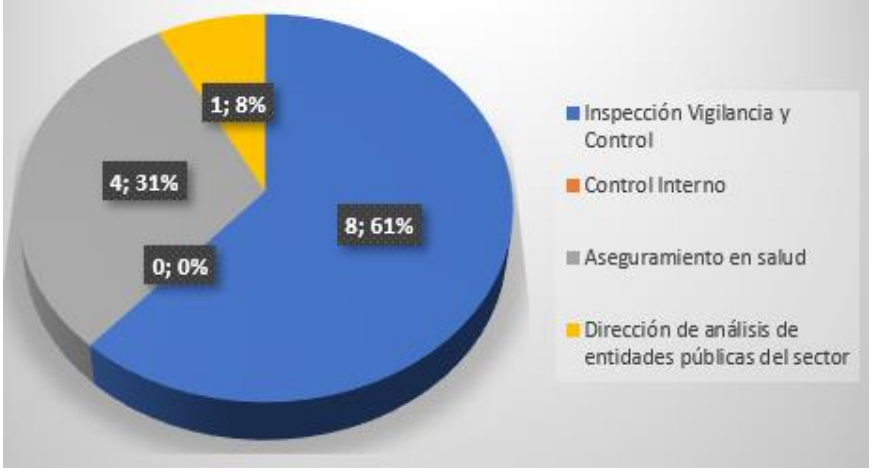
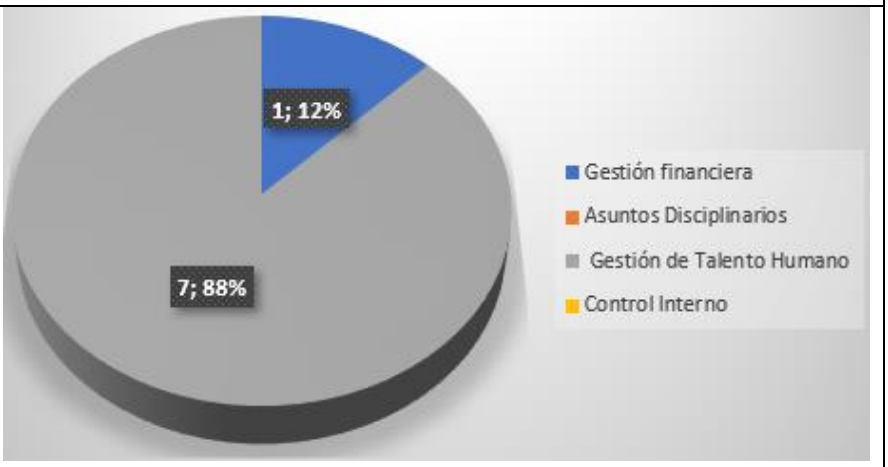
7.5 NIVEL DE ADHERENCIA FRENTE A LOS VALORES INSTITUCIONALES

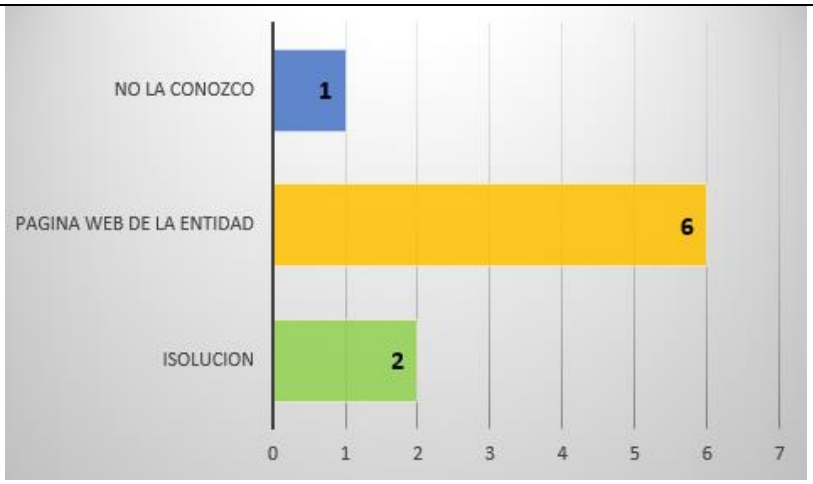
Mediante encuesta elaborada, se desea conocer el nivel de adherencia frente a los valores institucionales, dicha encuesta fue remitida a los participantes de la auditoria y se obtiene los siguientes resultados:

Pregunta	Resultado Obtenido
Envió de encuesta	
¿Tipo de Vinculación?	

Pregunta	Resultado Obtenido
¿Cuántos son los valores definidos para la entidad?	
¿Cuáles son los valores definidos para la entidad?	
¿Por cuál medio ha escuchado hablar de los valores de la entidad?	CORREO ELECTRONICO 4 INTRANET 7 PANTALLAS DIGITALES 2 ROMPETRAFICOS 0 ACTIVACION DE CAMPAÑA 0 VALLAS 1

Pregunta	Resultado Obtenido
¿Los valores han sido socializados al interior de su dependencia?	
¿Conoce el código de integridad de la entidad?	
Seleccione la definición de cohecho propio	

Pregunta	Resultado Obtenido
¿Según el lineamiento de la política institucional anti sobornó, que procesos en la SDS son los más susceptibles para tener riesgos de soborno o de cohecho?	
¿De acuerdo al observatorio de transparencia y Anticorrupción los procesos más susceptibles de riesgos de cohecho o soborno son?	
¿El Riesgo de soborno o cohecho, tanto en la provisión de cargos provisionales y de libre nombramiento y remoción, así como en contratos de prestación de servicios de manera irregular por favoritismos o retribuciones, que conllevan una prestación ineficiente del servicio público son competencia de que área?	

Pregunta	Resultado Obtenido
¿En dónde se encuentra almacenada la política anti sobornó de la SDS	
Conclucion General: Frente a las respuestas obtenidas por parte de los particpantes, se logra determinar que existe conocimiento frente a los valores institucionales. Es necesario seguir realizando campañas de sensibilización y adherencia que permitan reforzar estos conceptos a todo el personal.	

7.6 ANALISIS POR LINEA DEFENSA

Tiene por objetivo verificar la gestión y los componentes de control: ambiente de control, actividades de control, gestión del riesgo, actividades de monitoreo e información y comunicación con relación al proceso TIC.

NIVEL	RESPONSABLES	FUNCIONES	RESULTADO DE LA EVALUACION
NIVEL ESTRATÉGICO	Alta Dirección de la entidad y el Comité de Coordinación de Control Interno.	• Definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantiza el cumplimiento de los planes de la entidad. • Analizar los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos (objetivos, metas, indicadores).	Se tiene definido el marco de buenas prácticas para la gestión de riesgos de la entidad, mediante la metodología del DAFP propuesta para las entidades del distrito y alineada con la Norma técnica ISO31000, la cual es liderada por la Dirección de Planeación institucional y calidad. En la actualidad, la dirección tiene definido un plan de mejoramiento establecido para fortalecer la implementación de la metodología en toda la entidad y existe evidencia que demuestra el análisis y valoración cualitativa para las 5 amenazas transversales de seguridad de la información evaluados en este informe.
Estado: CUMPLE			

NIVEL	RESPONSABLES	FUNCIONES	RESULTADO DE LA EVALUACION
1° LÍNEA DE DEFENSA (AUTOCONTROL)	Gerentes, líderes de proceso y sus equipos. (Servidores públicos en todos los niveles de la organización).	• Gestionar los riesgos	Contemplo la identificación del riesgo, valoración, definición e implementación del plan de tratamiento y con ello el monitoreo, sin embargo, mediante la verificación realizada, no fue posible determinar si los controles implementados han sido eficaces y el seguimiento a cada riesgo tampoco se tiene.
		• Implementar acciones correctivas	Se consultan varios registros de acciones registradas en el aplicativo isolucion, producto de la auditoria del SGSI año 2020. Varias acciones correctivas fueron implementadas y fue comprobada su eficacia.
		• Ejecutar procedimientos de riesgo y control	Los referentes consultados, informa que el monitoreo de los controles no es una tarea constante y se realiza una vez al año, sin embargo, no se presentó evidencia al respecto.
		• Identificar, evaluar, controlar y mitigar los riesgos de la gestión operacional	Mediante la verificación realizada a las fuentes de información suministradas de cara a la gestión de riesgos, se identifican 5 registros de riesgos transversales, así como la valoración cualitativa de los mismos, sin embargo, se informa que el plan de tratamiento no ha sido actualizado y dependerá de las matrices que deberán ser enviadas por los referentes de cada dependencia el día 11 de Julio del 2021. Respecto a evaluación realizada, no fue posible determinar: 1. Si los controles definidos han sido eficaces y suficientes.

			2. Si el seguimiento a cada riesgo se está realizando, esto con el fin determinar si el riesgo se mitigo o redujo.
Estado: NO CUMPLE			

NIVEL	RESPONSABLES	FUNCIONES	RESULTADO DE LA EVALUACION
2° SEGUNDA LÍNEA DE DEFENSA (AUTOEVALUACION)	Media y Alta Gerencia: Planeación o quien haga sus veces Coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, comité de contratación, áreas financieras, De TIC, entre otros que generen información para el Aseguramiento de la operación.	• 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 • Consolidar y analizar información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.	Mediante la verificación realizada a las fuentes de información proporcionadas de cara a la gestión de riesgos desarrollada por la dependencia, se evidencian 5 registros de riesgos transversales de SI, sin embargo, no fue posible constatar y evidenciar lo siguiente: 1. que el riesgo residual se calculara, 2. si los controles definidos han sido eficaces y 3. si el seguimiento a cada riesgo se realiza. Por lo anterior, la gestión del riesgo no es la apropiada. Por parte de la media gerencia, no existe evidencia que permita comprobar la implementación de la gestión de riesgo y la supervisión de la misma. Se cuenta con el plan de gestión riesgos de seguridad, el cual será implementado en el segundo semestre del 2021. Cabe resaltar que el plan contempla las actividades de implementación de controles y monitoreo de los riesgos.
Estado: NO CUMPLE			

NIVEL	RESPONSABLES	FUNCIONES	RESULTADO DE LA EVALUACION
3° TERCERA LÍNEA DE DEFENSA (EVALUACION INDEPENDIENTE)	**Oficina de Control Interno**	• Realiza auditoría interna a través de un enfoque basado en el riesgo. • Proporcionará aseguramiento sobre la eficacia de gobierno, gestión de riesgos y control interno a la alta dirección de la entidad	Mediante el presente informe, se presenta los resultados respecto al desarrollo de la auditoria de gestión con énfasis en riesgos, programada en el mes de mayo y junio respectivamente. En dicho ejercicio participaron los diferentes referentes designados por los dueños de proceso. En síntesis, el ejercicio permitió verificar los diferentes controles implementados para del proceso del alcance, lo cual puede ser constatado con cada uno de los papales de trabajo utilizados. Así mismo, se logró verificar la gestión del riesgo en todo su ciclo de vida. Es importante mencionar que se evidenciaron algunas debilidades que fueron expuestas y descritas en el capitulo10 de este documento y que serán tratadas como acciones para abordar riesgos.
Estado: CUMPLE			

8. ASPECTOS POSITIVOS.

- El recurso humano asignado a responder la auditoria, reúne el conocimiento y la experiencia necesaria para dar respuesta a las dudas e inquietudes que se expusieron.

- Es importante resaltar la cordialidad y la atención prestada por los profesionales que participaron de la auditoria, mostrando un alto grado de compromiso frente a la cultura del control.

- El recurso humano conoce las entradas requeridas y las salidas esperadas, determina los recursos físicos y tecnológicos que son necesarios para la operación diaria.

- Existe el compromiso firme de la dirección TIC encaminado a promover la cultura de la seguridad de la información como elemento estratégico en la entidad, apalancando el cumplimiento de la política de seguridad digital.

9. NO CONFORMIDADES.

9.1. Después de revisar la matriz de tratamiento de riesgo suministrada con relación al componente de seguridad de la información, se evidencia que la información del plan de tratamiento sigue sin ser actualizada desde año 2020, así mismo identificamos que el requisito fue evaluado en la auditoría realizada en julio del año 2020 y derivo en la acción de mejora número 10.6, que a la fecha sigue sin cumplirse de acuerdo a la verificación realizada, evidenciado una reincidencia con el mismo requisito evaluado. En consecuencia, existe un incumplimiento al requisito 8.3 de la norma 9001:2015, por lo que hace necesario e indispensable tomar las acciones pertinentes.

10. ACCIONES PARA ABORDAR RIESGOS.

Política de Gobierno Digital

10.1. De acuerdo con la evaluación y verificación realizada, respecto a la implementación de las acciones o recomendaciones producto del FURAG y los seguimientos establecidos en la política de Gobierno Digital, identificamos que a la fecha la dirección TIC no ha implementado las diferentes recomendaciones y que según lo informado dependerán de la adjudicación del contrato por concurso de méritos. Evidenciamos que el proceso se encuentra en etapa precontractual, con el radicado del proceso a la subdirección de contratación, id: 2021IE12440 del 7 de mayo, pero a la fecha los RFPs no han sido elaborados y publicados. En consecuencia se deriva un potencial riesgo toda vez que el contrato no se ha suscrito y la implementación del protocolo en lo que respecta a la resolución 2710 del 2017 y la modificación de la misma en la resolución 1126 de 2021, se ha realizado de manera parcial y de no hacerlo, afectara el desempeño de la entidad frente a otras, para ello se hace necesario garantizar la elaboración de los RFPs, publicación, evaluación de los oferentes, negociación y adjudicación, lo cual debe darse en el segundo semestre del 2021.

10.2. Mediante la información suministrada con miras a determinar si los proyectos y la operación de TI se encuentran al 100%, se identifican 2 cosas: 1. La utilización o destino de los montos sobrantes para las actividades de los proyectos 7785 y 7788 se desconoce, evidenciamos que no están siendo justificadas y documentadas, el director TIC informa que la operación se cumplió al 100% y los recursos sobrantes fueron liberados, sin embargo los soportes solicitados no fueron entregados, 2. Se conoce el estado de los elementos por separado o de manera individual, pero no se tiene el todo, evidenciamos no se cuenta con un informe consolidado y exacto que permita determinar si los proyectos y la operación se ejecutaron al 100%, por lo anterior, se deriva un potencial riesgo toda vez que el control que se tiene no está siendo eficiente, generando información inexacta para la toma de decisiones, para ello se hace necesario reforzar los controles existentes, permitiendo generar el informe consolidado y exacto de los proyectos y la operación de TI de manera periódica.

10.3. Mediante las consultas realizadas a los 11 tramites en línea del componente de agillinea portal web: saludcapital.gov.co, evidenciamos que las características de accesibilidad implementadas para personas con discapacidad visual se pierden, ocurre que al momento de ingresar a cada tramite, el vínculo o la URL que saltar pierde las características implementadas, en consecuencia se deriva un potencial riesgo toda vez que la funcionalidad es parcial, afectado la consulta que realizan las personas con esta discapacidad, por tal razón se determina que el control no es eficaz, generando inconformidad con el servicio prestado, para ello se hace necesario implementar las características de accesibilidad a todos los vínculos que disparan los tramites en línea permitiendo que las personas con esta discapacidad pueden percibir, entender, navegar, interactuar y contribuir con cada sitio web.

10.4. Mediante la información suministrada, se identifican los inventarios de los dispositivos IoT de la entidad, sin embargo, se evidencia que a la fecha el análisis y explotación de los datos capturados por estos dispositivos no se ha realizado, en consecuencia, se deriva un potencial riesgo toda vez que conlleva un incumplimiento con la implementación de la política de Gobierno digital, decreto 1008 del 2018 y afectara el desempeño de la entidad frente a otras, para ello se hace indispensable iniciar las capturas datos de los dispositivos definidos y llevar a cabo el análisis de esta información, que permitan obtener información importante y clave para aplicarlos a las necesidades de la entidad. Esta información permitirá avanzar hacia la transformación digital de la entidad.

Política de Seguridad Digital

10.5. De acuerdo con la información suministrada respecto al resultado y el estado del desempeño del SGSI en el año 2020 y 2021, se evidencia que los 5 indicadores definidos en el marco del plan de mejora, no han sido obtenidos, y los resultados por ende no han sido divulgados o presentados en las diferentes instancias como son el Comité Institucional de Gestión y las mesas técnicas de Gobierno y Seguridad Digital, en consecuencia, se deriva un potencial riesgo toda vez que los reportes de desempeño del sistema han presentado información parcial, y lo dispuesto en los numerales de la norma 5.1, 9.1 y 9.3 se están cumpliendo de forma parcial, por lo anterior se hace necesario obtener y calcular los 5 indicadores de acuerdo a la periodicidad definida y presentar los resultados en las diferentes instancias establecidas.

10.6. Mediante la información suministrada que permitió verificar el estado del plan de seguridad de la información y el plan de gestión de riesgos del año 2020 y 2021, evidenciamos que los objetivos frente a: Análisis de vulnerabilidades, plan de continuidad de Negocio-BCP y Análisis de Impacto del Negocio-BIA, no han sido cumplidos e implementados a la fecha, en consecuencia, se deriva un potencial riesgo toda vez que la infraestructura tecnológica pudiera sufrir una interrupción o incidente de alto impacto que puede afectar la prestación del servicio, evitará perdidas costosas que atenta contra la reputación de la entidad. Se cumple parcialmente los numerales de la norma A12.6.1, A17.1.1, A17.1.2, A17.1.3, y A17.2.1, por lo anterior se hace necesario 1. Desarrollar el análisis de vulnerabilidades con cierta profundidad y

determinar el nivel de exposición, aplicando los correctivos necesarios. 2. Respecto al BCP se debe desarrollar: Planes de respuesta inmediata, Realizar el análisis de Impacto al Negocio (BIA), crear los planes de gestión de crisis y planes de recuperación, probar y evaluar los planes y determinar el desempeño de su ejecución, analizar los escenarios posibles de desastre, priorizar las acciones a tomar y el orden de la recuperación, crear estrategias de continuidad que ayuden a restablecer las operaciones, capacitar y sensibilizar al personal.

Requerimientos

10.7. Mediante las consultas realizadas a la base de datos de ARANDA SOFTWARE en lo que respecta a los componentes de requerimientos e incidentes, evidenciamos que a fecha existen 71 casos entre requerimientos e incidentes que se encuentran sin ser atendidos y solucionados, casos que fueron registrados hace más de 2 meses y que el especialista asignado es la misma persona, se informa que por efectos de la finalización del contrato con ETB, la actividad de seguimiento se dejó de realizar, en consecuencia, se deriva un potencial riesgo toda vez que genera insatisfacción por parte de los usuarios finales, conlleva reclamaciones y afecta la eficiencia de la mesa de servicios, por lo anterior se hace indispensable reactivar el control que venía realizando el coordinador con el fin de depurar las casos sin solución y reunir a los especialistas para determinar acciones de mejoramiento a seguir.

10.8. Mediante las consultas realizadas a la base de datos de ARANDA SOFTWARE en lo que respecta a los componentes de requerimientos e incidentes, evidenciamos que los SLA o acuerdos de nivel de servicios definidos e implementados en la herramienta se están incumpliendo, las consultas realizadas, permiten demostrar que los tiempos de atención y solución están en el rango de 2 a 6 meses, lo cual está por encima de los SLA estándar o base y en la operación o mesa de servicios no ocurre nada, en consecuencia, se deriva un potencial riesgo toda vez que genera insatisfacción por parte de los usuarios finales, por lo anterior se hace indispensable y necesario redefinir o ajustar los SLA y aplicarlos a la herramienta de tal forma que generen las notificaciones correspondientes de los vencimientos y permitirá mejorar los tiempos de respuesta.

Responsabilidades

10.9. Mediante las respuestas obtenidas a las preguntas formuladas a los referentes participantes respecto a la Gobernabilidad que ejerce TIC en la entidad y la responsabilidad de atender al 100% las necesidades de software de las diferentes dependencias, evidenciamos que no existe un soporte que respalde el acuerdo entre las dependencias para realizar desarrollos compartidos, no existe un lineamiento definido por TIC que le permita al nuevo contratista-desarrollador conocer las directrices que debe seguir en términos del producto y características que debe tener este, no existen registros de socialización en donde el referente de TIC le explique al nuevo contratistas como debe funcionar y que espera al final del ejercicio, en consecuencia, se deriva un potencial riesgo toda vez las actividades definidas en el proceso para el componente de software se están realizando de forma parcial, así mismo genera insatisfacción por parte de los usuarios finales y la responsabilidad de

Gobierno TIC no se está ejerciendo en su totalidad, por lo anterior se hace indispensable y necesario elaborar los términos técnicos para la consecución de la fábrica de software, radicar los termino en la subdirección de contratación, garantizar su adjudicación, dar inicio a la operación, medir su eficacia. Debe contemplar la divulgación a todas las dependencias de la nueva forma como va a funcionar la dirección TIC y como serán atendidas todas las necesidades, para ello se debe crear instructivo y formatos.

11. CONCLUSIONES.

11.1. En virtud de lo informado y consultado, ahora sabemos frente a la política de Gobierno Digital a la fecha no se ha implementado las diferentes recomendaciones de cara al protocolo IPV6 y que de acuerdo a lo indicado su implementación dependerán de un tercero o consultor especialista. El proceso se encuentra en etapa precontractual, se radico a la subdirección de contratación, sin embargo, a la fecha los RFPs no han sido elaborados y publicados. Se hace necesario gestionar y agilizar con la subdirección de contratación el proceso.

11.2. Respecto al cumplimiento de los proyectos y la operación de TI, se determina que la utilización o el destino de los montos sobrantes en las actividades de los proyectos 7785 y 7788 se desconoce, por alguna razón no están siendo justificadas y documentadas lo cual genera información inexacta para la toma de decisiones.

11.3. Dentro del análisis realizado, podemos determinar que las características de accesibilidad implementadas para personas con discapacidad visual para los 11 tramites en línea del componente de agilinea portal web: saludcapital.gov.co, se pierden, el vínculo o la URL que saltar no mantiene las características implementadas, afectado la consulta que realizan las personas con esta discapacidad ya que no pueden percibir, entender, navegar, interactuar y contribuir con cada sitio web.

11.4. En virtud de lo consultado, se ha podido establecer que el análisis y explotación de los datos capturados por los dispositivos IoT en la entidad, no se ha realizado, lo cual corresponde a información clave hacia la transformación digital y alineada con la política de Gobierno Digital.

11.5. Los 5 indicadores definidos para el SGSI en el año 2020, no han sido calculados y no han sido presentados en las diferentes instancias que los requieran.

11.6. De acuerdo a lo consultado, podemos determinar que el análisis de vulnerabilidades con cierta profundidad realizado a los elementos críticos de la entidad no se ha realizado desde el año 2020. Todo apunta a que por la finalización del contrato con ETB, se dejó de realizar con el detalle y expertis que requiere.

11.7. El plan de continuidad de Negocio-BCP y el Análisis de Impacto del Negocio-BIA que corresponden a elementos del plan de seguridad de la información año 2020 y que fueron traslados al 2021, siguen sin ser desarrollados e implementados en la entidad. Se cuenta con algunos documentos preliminares, pero hace indispensable avanzar

muy rápidamente para lograr cumplir con este objetivo en el segundo semestre del año 2021.

11.8. Respecto a la gestión de incidentes y requerimientos realizada mediante la mesa de ayuda (SOC-NOC), se constata que se está dejando de atender y resolver varios casos, toda vez que el contrato con ETB finalizo y no se cuenta con el recurso humano de planta suficiente para atender la demanda diaria.

11.9. Se hace necesario gestionar y agilizar con la subdirección contratación el proceso para la consecución de la fábrica de software que permita atender las necesidades de desarrollos que demandan las diferentes dependencias y permitiendo con ello, liderar y cumplir las actividades definidas en la caracterización del proceso.

11.10. La gestión de los riesgos frente a los 5 riesgos se encuentra desactualizada ya que la evaluación del riesgo residual a la fecha no sido actualizada, los controles definidos no han sido medidos, por lo anterior, no se puede determinar si son eficaces y suficientes.

11.11. Se logra determinar mediante encuesta que el conocimiento frente a los valores institucionales se conoce y se aplica. Sin embargo, es necesario seguir realizando campañas de sensibilización y adherencia que permitan reforzar estos conceptos a todo el personal.

11.12. Continuar con el fortalecimiento de la “cultura de autocontrol” respecto del seguimiento a Política de Gobierno Digital, de acuerdo con el cronograma previsto para su implementación.

12. RECOMENDACIONES

Atender las recomendaciones del furag en el marco de la política de seguridad digital, llevando acabo la vinculación, y participación de los diferentes encuentros en materia de incidentes cibernéticos que la Coordinación Nacional de Seguridad Digital convoque, además solicitar retroalimentación continua de los temas que allí se impartan, permitiendo el fortalecimiento de las capacidades en seguridad digital en la SDS y aplicando lo dispuesto en el documento CONPES 3854 del 2016 en materia de seguridad digital y gobernanza en Colombia.

13. PLAN DE MEJORAMIENTO

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 a los riesgos incluyendo en las actividades el ciclo PHVA y de ser necesario realizar mesas de trabajo cuando los acciones para abordar los riesgos involucren otras dependencias.

14. ANEXOS.

Corresponde a los papeles de trabajo utilizados en cada mesa de trabajo y que serán entregados con este informe para el análisis de cada uno las partes interesadas.

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

FRANCISCO JAVIER PINTO
Auditor Líder

APRUEBA JEFE OFICINA DE CONTROL INTERNO

OLGA LUCIA VARGAS COBOS
Jefe Oficina de Control Interno