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, abril 2022

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 respecta a los siguientes elementos:

1.1 Sistema de seguridad de la información, se evaluará el ciclo PHVA, con el fin de determinar planificación. Implementación, mantenimiento y la mejora respecto a la aplicación de la Norma ISO27001:2013 y complementarias.

1.2 Procedimiento de atención de la mesa de Servicios acorde a lo diferentes canales y mecanismos de recepción y se verificara la adquisición de bienes y servicios de TI, la ejecución y el seguimiento de dichos contratos acorde al (PETIC2020-2024 y PAA).

2. OBJETIVOS ESPECÍFICOS DE LA AUDITORÍA.

2.1 Elaborar el plan de auditoría y los instrumentos de auditoria para la recolección de información, evidencias y pruebas que se llevarán a cabo.
2.2 Establecer la situación actual en cuanto a la seguridad de la información acorde a la norma ISO27001:2013
2.3 Elaborar y entregar a los líderes del SGSI el informe final de auditoria con recomendaciones y observaciones que permitan a la entidad implementar las oportunidades de mejora que haya lugar.
2.4 Verificar y evaluar el cumplimiento de las mejores prácticas para la gestión del Servicio en lo concerniente a la operación del servicio. Así mismo, se verificara la adquisición de bienes y servicios de TI acorde al PETIC2020-2024 y el seguimiento de dichos contratos. Contempla la revisión de la contratación por prestación de servicios del recurso humano que apoyo a las diferentes actividades de la operación de TI.

3. ALCANCE DE LA AUDITORÍA.

- Sistema de Seguridad de la información o MSPI y revisión con base al ciclo de vida PHVA.
- Procedimiento de mesa de servicios para la atención de requerimientos e incidentes.
- Adquisición de bienes y servicios de TI acorde al PETIC2020-2024 y PAA

Periodo a evaluar: enero 2021 a febrero 2022

4. CRITERIOS DE AUDITORÍA.

- Marco normativo ISO27001:2013 y complementarias como son:
  - Norma IEC ISO 31000:2018 y 27005 para Gestión de Riesgos
  - Norma IEC ISO 22301:2012 Continuidad de Negocio.
  - Framework NIST 801-53 – Ciberseguridad ISO 27032

- PETIC2020-2024 y PAA 2021.
- Caracterización SDS-TIC-CAR-001 – GESTION TIC

Procedimientos:

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

Otros: Gestión de Riesgos y Mapa de Riesgo Institucional

Nota: Dicho ejercicio fue basado listas de chequeo elaboradas para este propósito

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
- Ley 1581 del 2012 protección y tratamiento de datos personales

6. METODOLOGÍA UTILIZADA.

Con el fin de evaluar en primera instancia la protección y seguridad de la información conforme a los requerimientos de la Norma ISO27001:2013, el auditor tuvo en cuenta la siguiente metodología:

Revisión de la documentación de seguridad de la información

El auditor solicitó y revisó la documentación remitida y existente en la entidad respecto a la gestión de la seguridad de la información, verificando los documentos de políticas de seguridad de la información, procesos, procedimientos, guías, registros de actas entre otros documentos.

Consultas con el personal designado

El auditor realizó consultas específicas al personal designado por la entidad, con el fin de conocer el nivel de concientización frente a la seguridad de la información en la operación diaria.

Lista de verificación para los Auditados

El auditor entrega la lista de requisitos de revisión, la cual fue diligenciada en compañía de los referentes designados y personal que acompaño el ejercicio. Estos listados serán una imagen cualitativa y cuantitativa del estado de la seguridad respecto a la norma ISO 27001:2013 y su ANEXO-A. Cabe señalar que el alcance de la verificación contemplo la selección de 40 requisitos de la norma certificable y 39 controles del anexo. Las mesas de trabajo fueron agendadas acorde al plan de trabajo establecido.

7. ANÁLISIS DE INFORMACIÓN

El análisis de la información es el arte de descubrir y analizar ciertos patrones, comportamientos, desviaciones e inconsistencias que pudieran estar presentándose en la operación y originan debilidades. ES por eso necesario desarrollar un plan de mejoramiento con el fin de fortalecer todos estos aspectos identificados. El insumo de la información para el correspondiente análisis, es producto de las respuestas obtenidas a cada uno de los criterios evaluados mediante de las diferentes mesas de trabajo realizadas. 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 o listas de verificación mediante el archivo denominado: Listadechequeo-GestiónTICparte1VF27abr2022.xlsx.

El análisis realizado fue focalizado en 2 componentes principalmente:

1. Componente de Seguridad de la información y
2. Componente Plan Estratégico de Tecnologías de la Información – PETIC y Gestión de incidentes/Requerimientos.

A continuación, se presenta los resultados del análisis realizado por cada uno de los componentes mencionados.

7.1 Componente de Seguridad de la información

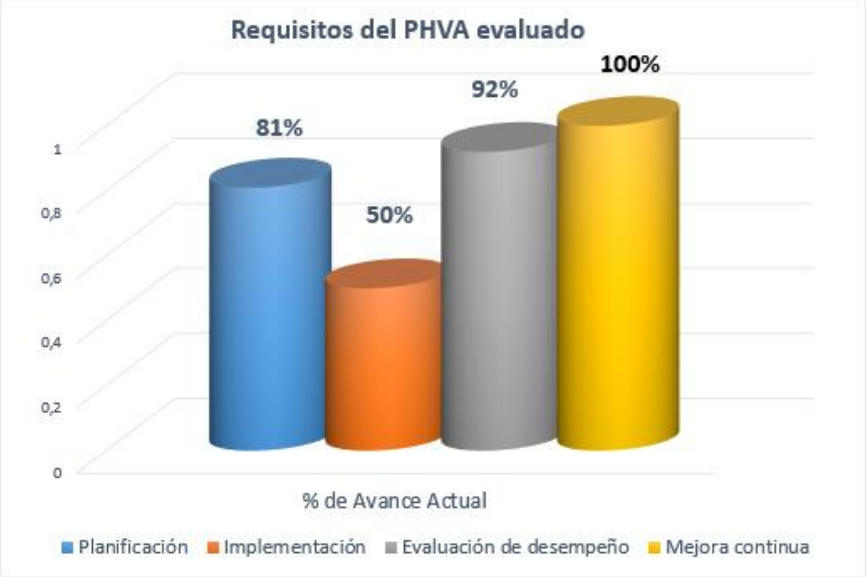
Mediante gráficas y tablas se presentan los resultados obtenidos en base a la buena práctica o norma internacional ISO-IEC 27001:2013 e ISO-IEC 27002:2013.

7.1.1 Resultados en base a la norma NTC ISO-IEC 27001

La Norma NTC ISO-IEC 27001, contempla diversos requisitos en cumplimiento de los 7 dominios que conforman el ciclo PHVA. Con el objetivo de limitar o focalizar el ejercicio, el auditor selecciono 40 requisitos de los diferentes dominios, requisitos que se consideran dinámicos que cambian constantemente y que son importantes validar desde la óptica de la auditoria.
Nota: La correspondiente evaluación, no mide el nivel de madurez o implementación de la norma, toda vez que todos los requisitos que define la norma no fueron considerados en el alcance inicial.

El porcentaje de cumplimiento respecto a los 40 requisitos seleccionados fue el siguiente:

Figura 1. Ciclo PHVA



Fuente: Lista de chequeo

Tabla 1. Análisis por Dominio

Ciclo PHVA	Dominios de la Norma	Requisitos Evaluados	Cumplen	Acciones de Mejora
P	4 contexto de la Organización	1	1	0
	5 liderazgo	10	8	2
	6 planificación	3	1	2
	7 apoyo	8	8	0
H	8 operación	4	2	2
V	9 evaluación de desempeño	13	12	1
A	10 mejora	1	1	0
Total general		**40**	**33**	**7**

Fuente: Lista de chequeo

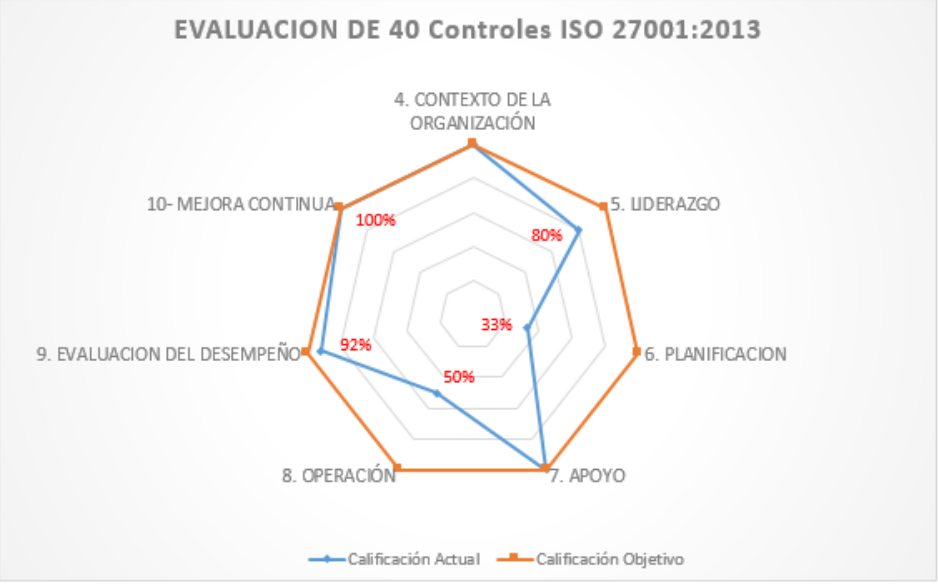
De los resultados de la figura 1 y tabla 1 podemos concluir que, en las etapas de Planificación y Operación, los requisitos evaluados presentan ciertas debilidades y originan oportunidades de mejora las cuales serán justificadas en el capítulo 9 y 10 del presente documento. Para conocimiento del lector, cada uno de los requisitos catalogados como “Acción de Mejora”, no significa que se esté incumpliendo, simplemente desde la óptica del autor y la buena práctica requieren mejorarse. A modo de conclusiones se aclaran cada uno de estos aspectos detectados.

Figura 2. Resumen de evaluación de requisitos

Fuente: Lista de chequeo

De los 40 requisitos evaluados, 33 de ellos es decir 83% cumplen a satisfacción.

Figura 3. Representación del avance por Dominio



Fuente: Lista de chequeo

7.1.2 Resultados en base a la norma NTC ISO-IEC 27002

La Norma NTC ISO-IEC 27002, contempla 114 controles agrupados en 14 dominios. Con el objetivo de limitar o focalizar el ejercicio, el auditor seleccionó 39 controles de los diferentes dominios que son importantes validar desde la óptica de auditorías previas.
Nota: La correspondiente evaluación, no mide el nivel de madurez o implementación del código de buenas prácticas, toda vez que todos los controles no fueron considerados dentro del alcance inicial para este ejercicio.

El porcentaje de cumplimiento respecto a los 39 controles seleccionados fue el siguiente:

Figura 4. Análisis por los 14 Dominios

Fuente: Lista de chequeo

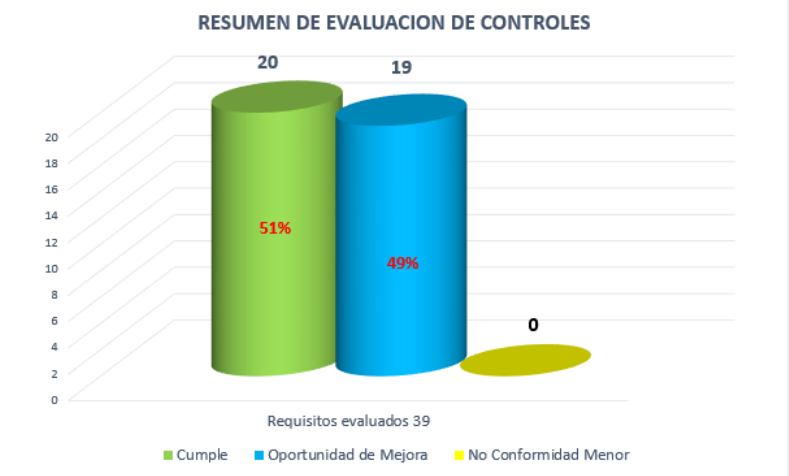
Tabla 3. % de Avance por los 14 Dominios ANEXO A

ID	Evaluación de Efectividad de controles				
	DOMINIO	# de Controles Evaluados	Cumple	Acciones de Mejora	No-Conformidades
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	2	0	2	0
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	3	2	1	0
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	1	1	0	0
A.8	GESTIÓN DE ACTIVOS	3	2	1	0
A.9	CONTROL DE ACCESO	2	1	1	0
A.10	CRIPTOGRAFÍA	2	1	1	0
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	2	0	2	0
A.12	SEGURIDAD DE LAS OPERACIONES	7	4	3	0
A.13	SEGURIDAD DE LAS COMUNICACIONES	2	2	0	0
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	2	1	1	0
A.15	RELACIONES CON LOS PROVEEDORES	4	2	2	0
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	5	2	3	0
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	3	1	2	0
A.18	CUMPLIMIENTO	1	1	0	0
Totales		**39**	**20**	**19**	**0**

Fuente: Lista de chequeo

De los resultados de la figura 4 y tabla 3 podemos concluir que los dominios 5, 11, 12,15 y 16 evaluados presentan ciertas debilidades y originan oportunidades de mejora las cuales serán justificadas en el capítulo 10 del presente documento. Para conocimiento del lector, cada uno de los controles catalogados como “Acciones de Mejora”, no significa que se esté incumpliendo, simplemente desde la óptica del autor y la buena práctica requieren mejorarse. A modo de conclusiones se aclaran cada uno de estos aspectos detectados.

Figura 5. Resultado de evaluación de 39 controles ANEXO A



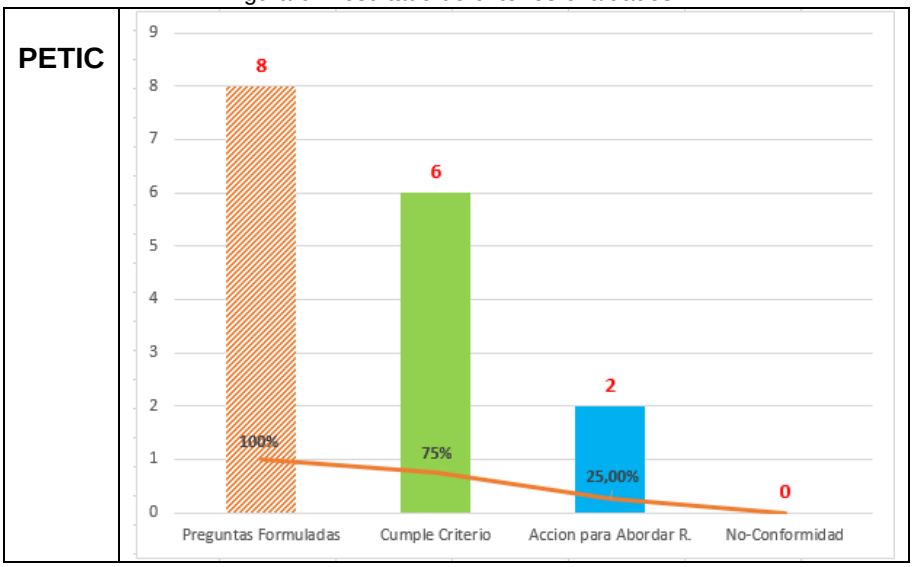
Fuente: Lista de chequeo

De los 39 requisitos evaluados, 20 de ellos es decir 51% cumplen a satisfacción.

7.2 Componente PETIC y Gestión de incidentes/Requerimientos

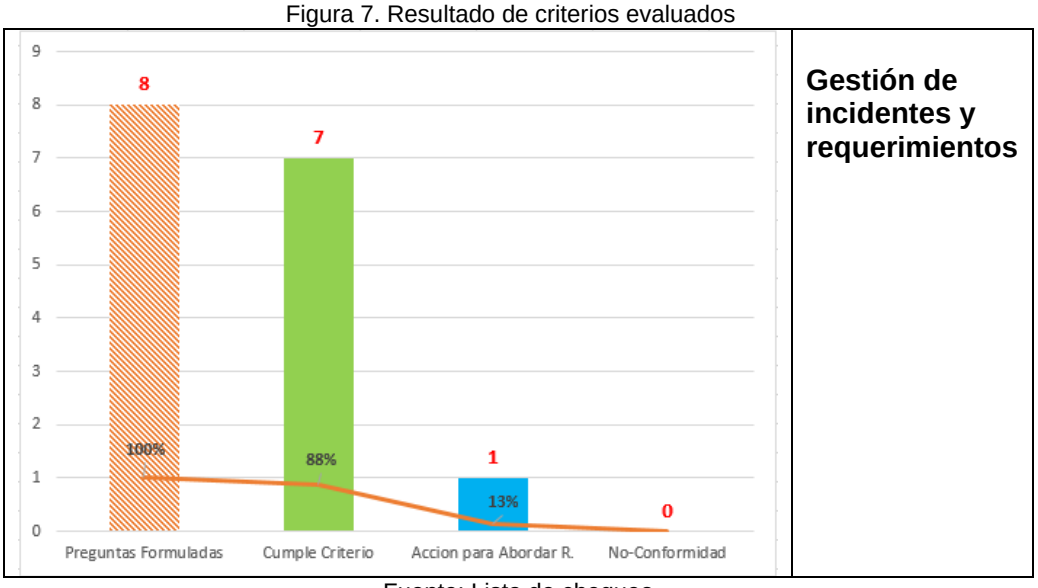
Mediante graficas se presentan los resultados obtenidos en base a la evaluación realizada.

Figura 6. Resultado de criterios evaluados



Fuente: Lista de chequeo

Figura 7. Resultado de criterios evaluados

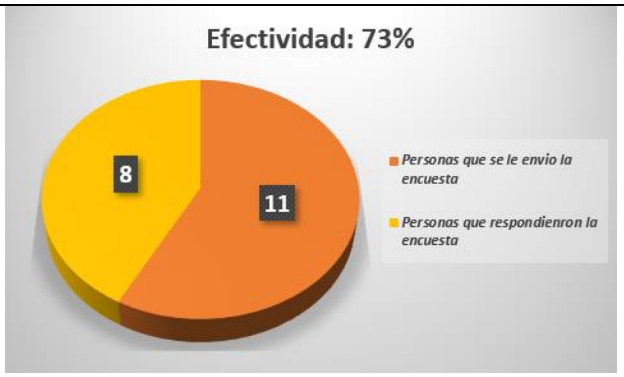
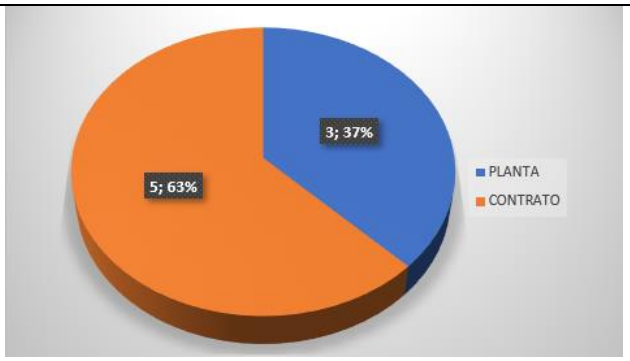
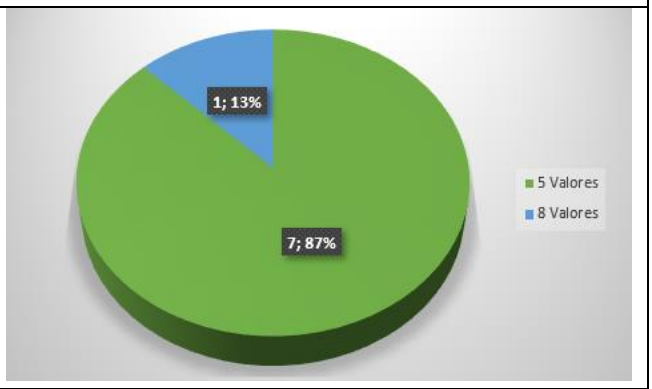


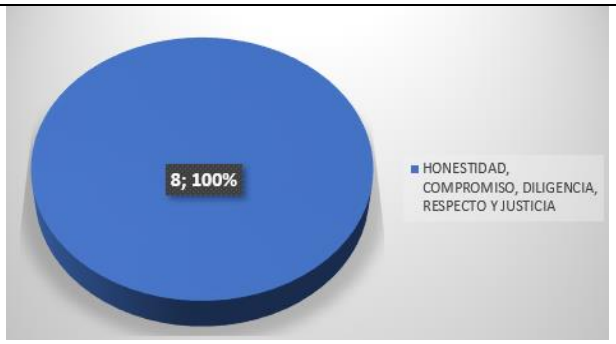
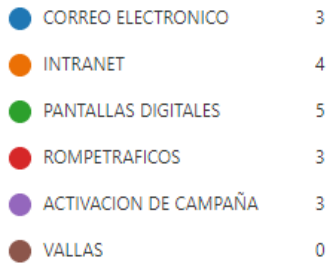
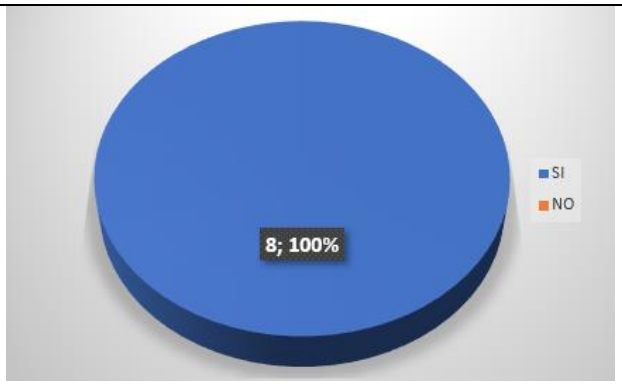
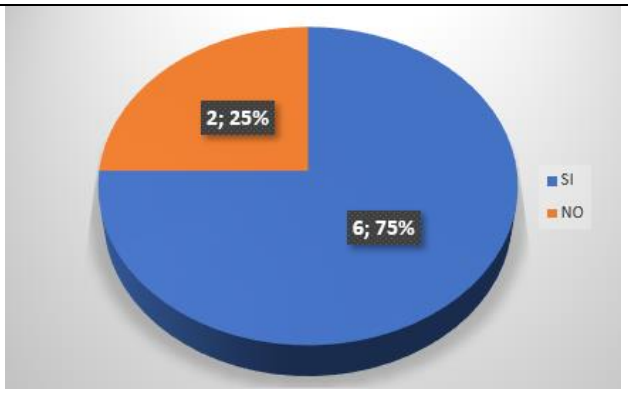
Fuente: Lista de chequeo

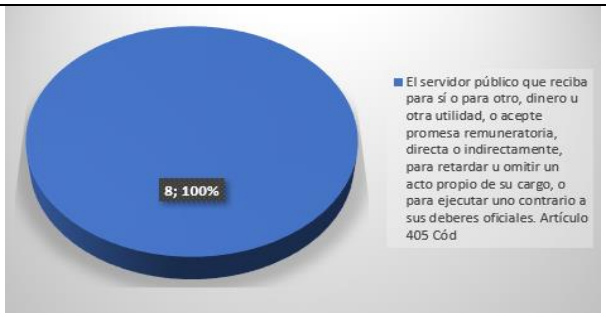
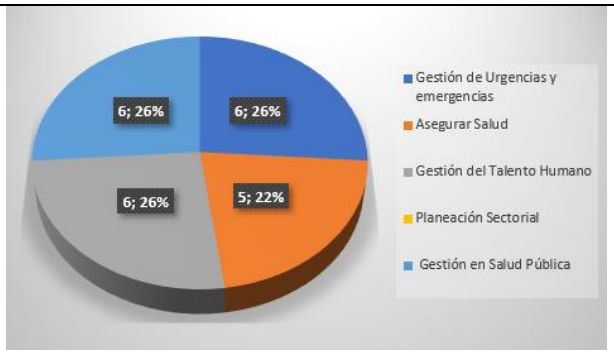
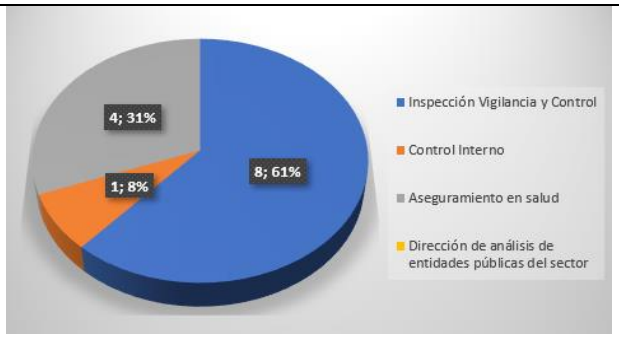
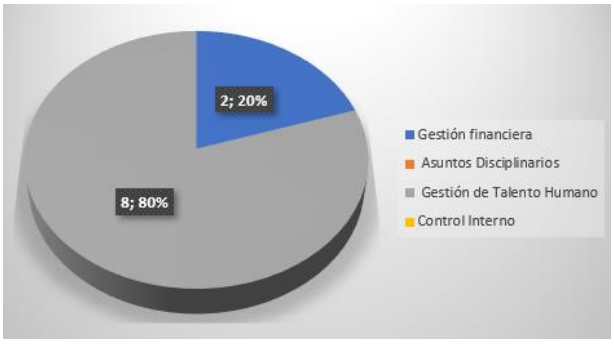
De los resultados de la figura 6 y 7 podemos concluir que los 16 criterios evaluados, el 19% presentan cierta debilidad y por consiguiente originan oportunidades de mejora que serán justificadas en el capítulo 9 del presente documento.

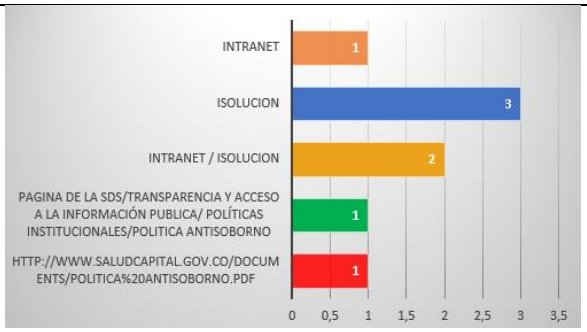
7.3 NIVEL DE ADHERENCIA FRENTE A LOS VALORES INSTITUCIONALES

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

Pregunta	Resultado Obtenido
Envío de encuesta	
¿Tipo de Vinculación?	
¿Cuántos son os valores definidos para la entidad?	

Pregunta	Resultado Obtenido
¿Cuáles son los valores definidos para la entidad?	
¿Por cuál medio ha escuchado hablar de los valores de la entidad?	
¿Los valores han sido socializados al interior de su dependencia?	
¿Conoce el código de integridad de la entidad?	

Pregunta	Resultado Obtenido
Seleccione la definición de cohecho propio	
¿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	
Conclusion General: Frente a las respuestas obtenidas por parte de los particpantes, se logra evidenciar el conocimiento frente a los valores institucionales. Es necesario seguir realizando campañas de sensibilización y adherencia que permitan reforzar estos conceptos a todo el personal.	

7.4 ANALISIS POR LINEA DEFENSA

Fase que 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 en relación al proceso de gestión TIC en los subcomponentes ya descritos.

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 ISO31000, la cual es liderada por la Dirección de Planeación institucional y calidad. En la actualidad dicha dirección tiene definido un plan de mejoramiento establecido para fortalecer la implementación de la metodología en toda la entidad. Así mismo, existe evidencia que demuestra el análisis y valoración cualitativa de las amenazas identificadas de las iniciativas y procedimientos evaluados en el presente 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	La gestión implica la identificación del riesgo, valoración, definición e implementación del plan de tratamiento y a partir del correspondiente monitoreo y seguimiento, 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	Esta viene siendo la tercera auditoria que se ha realizado respecto al tema, por lo anterior, existe evidencia de acción tomadas para eliminar la causa raíz de las situaciones indeseadas encontradas.
		• Ejecutar procedimientos de riesgo y control	El gestor de calidad, manifiesta que la actividad de monitoreo de 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 de cara a la gestión de riesgos, se identifican varias fuentes con registros de riesgos tanto de corrupción como de servicio, que tienen relación con los componentes en cuestión, De igual forma se evidencia la evaluación cualitativa y el riesgo residual mediante la matriz, sin embargo, no fue es posible determinar si los controles definidos han sido suficientes y eficaces y a partir del seguimiento determinar si cada riesgo se mitigo. Lo cual se considera una debilidad importante.
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 de cara a la gestión de riesgos utilizada por la dependencia, se evidencian registros de riesgos y controles definidos tienen relación con los subcomponentes, sin embargo, el riesgo inherente y residual no cambian, la severidad del riesgo tampoco cambia y no fue es posible determinar si los controles definidos han sido eficaces y el seguimiento a cada riesgo tampoco se realiza. Por lo anterior, existe una debilidad respecto al manejo del riesgo. 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.
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 comparten los resultados respecto al desarrollo de la auditoria de gestión con énfasis en riesgos programada en el mes de marzo y abril respectivamente y participaron los diferentes referentes designados. En síntesis, el ejercicio permitió verificar los diferentes criterios y controles implementados para los procedimientos 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 encontraron algunas debilidades que se serán expuestas y descritas en el capitulo9 y 10 del presente documento y que deberán ser tratadas como acciones para abordar riesgos y no-conformidades.
Estado: CUMPLE			

8. ASPECTOS POSITIVOS.

- Existe el compromiso firme de la Dirección TIC encaminado a promover la cultura de la seguridad y protección de la información como elemento estratégico de la entidad, sin embargo, en el corto plazo no es un objetivo certificar a la entidad en dicho propósito.

- Se cuenta con el recurso humano idóneo y comprometido con las diferentes actividades que permitirán implementar, mantener y mejorar el sistema de gestión de seguridad de la información.

- La gestión de incidentes y la mesa de ayuda (SOC-NOC) cumple con los requisitos funcionales de negocio.

9. NO CONFORMIDADES.

No identificadas para el ejercicio realizado.

10. ACCIONES PARA ABORDAR RIESGOS.

10.1. Al consultar el documento de la "política general" definido y suministrado por el especialista de seguridad, evidenciamos que desde su creación en el año 2019 a la fecha, no se han registrado cambios o modificaciones, de igual forma el documento no está bajo el formato institucional y tampoco cuenta con controles de versiones, en consecuencia, se deriva un potencial riesgo toda vez que existe una debilidad en cuanto al cumplimiento en su totalidad de los controles numerales A.5.1.1 y A.5.1.2 de la norma ISO27002:2013; por tal motivo se hace necesario: 1. Mediante el escenario de mesa técnica de gobierno y seguridad digital, realizar la revisión de la consistencia, solidez de la política actual, 2. Actualizar, formalizar, aprobar y publicar la nueva versión del documento bajo el formato institucional, 3. Socializar la nueva política general aprobada a todos los funcionarios de la entidad.

10.2. Si bien es cierto, existe un documento que define la estructura de roles y responsabilidades atribuibles a la Seguridad de la información, evidenciamos que no existe la figura del Oficial de Seguridad de la Información en la entidad y las responsabilidades están repartidas en el director TIC y los diferentes especialistas de SI. Así mismo roles claves como son: especialistas de SI, Gestor de incidentes, Oficial de protección de datos, especialistas del SOC, Mesa Técnica, y las interrelaciones con otras dependencias como son: Asuntos disciplinarios, Oficina Jurídica y Oficina de Comunicaciones, Bienes-Servicios y asuntos disciplinarios que juegan un papel fundamental dentro del sistema no están definidos en esta estructura. Por lo anterior, se deriva un potencial riesgo toda vez que existe una debilidad en cuanto al cumplimiento en su totalidad del control numeral A.6.1.1 de la norma ISO27002:2013 ya que todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas. Por tal motivo, se hace necesario: 1. Definir los roles especificados y las responsabilidades dentro del esquema de la entidad, 2. Formalizar mediante el escenario de mesa técnica de gobierno y seguridad digital el nuevo esquema jerárgico y presentar la estructurar de roles y responsabilidades que deberá ser comunicada o socializada a toda la entidad.

10.3. Si bien es cierto, las matrices o inventarios de activos de información consolidados en el año 2021 se encuentran publicadas en la página WEB de la entidad, evidenciamos que no todas las matrices fueron remitidas por todos los procesos, la situación obedece a que el requerimiento tenia fecha limite al 11 de junio del 2021 acorde al PAAC 2021 y posteriormente se remitió un memorando recordado el compromiso, sin embargo han trascurrido 10 meses y sigue sin ser remitida la información. De otra parte se identifica que los inventarios existentes no cuentan con elementos de TIPO: servidores, firewall, switches, routes, entre otros, ya que los referentes del proceso aducen que estos elementos no procesan información. Lo cierto es que dichos elementos son esenciales para garantizar la disponibilidad y continuidad de los servicios ofrecidos. en consecuencia, se deriva un potencial

riesgo toda vez que existe una debilidad en cuanto al cumplimiento en su totalidad del control numeral A.8.1.1 de la norma ISO27002:2013 ya que los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos. Por tal motivo, se hace necesario: 1. Solicitar los inventarios faltante y la actualización de los existentes, 2. Incorporar en las diferentes matrices los activos de información tipo hardware, 3. Mantener una fuente de inventarios de activos de información consolidada y única independiente desde donde se accede y consulte y 4. Realizar la gestión de riesgos en base a los nuevos inventarios de ACTIVOS.

10.4. Al consultar la política específica sobre el uso de controles criptográficos, define en el numeral 5 que las áreas deben cifrar o aplicar claves a los documentos (PDF, Excel, Word, csv,) que contengan datos personales o datos sensibles. Sin embargo, se evidencia que en la práctica no se está llevando a cabo esta actividad ya que varios de los documentos consultados, no cuentan con ningún tipo de cifrado. En consecuencia, se deriva un potencial riesgo toda vez que existe una debilidad en cuanto al cumplimiento en su totalidad del control numeral A.10.1.1 de la norma ISO27002:2013 y por tal motivo se hace necesario: 1.Seleccionar la herramienta para aplicar contraseñas mediante algoritmo seguro. 2. Cifrar y descifrar documentos y 3 Generar TIP informativo para los especialistas o referentes apliquen este mecanismo.

10.5. Al consultar la base de cambios o RFC registrados en ARANDA software, se evidencia que solo existen 21 casos registrados desde el año 2021 y corte a febrero 2022, adicionalmente encontramos que varios de las solicitudes de cambio formulados mediante el formato SDS-TIC-FT-025, no fueron registrados en la herramienta por lo anterior, no se está llevando una gestión eficiente de los casos incumpliendo con el instructivo definido, Otro aspecto identificado es que el comité de cambios de Cambios se realiza semanalmente o cuando existen ventanas de urgencia, sin embargo, solo existen actas del mes de febrero del 2022. en consecuencia, se deriva un potencial riesgo toda vez que existe una debilidad en cuanto al cumplimiento en su totalidad del control numeral A.12.1.2 de la norma ISO27002:2013, por tal motivo se hace necesario: 1. Registrar todas las ventanas de mantenimiento o RFC y adjuntar los formatos en el módulo de cambios del aplicativo Aranda y 2. Gestionar todas las solicitudes para conocer el estado del proceso.

10.6. Si bien es cierto, existe un informe de análisis de vulnerabilidades técnicas realizado en el mes enero del 2022, se evidencia que el análisis solo fue aplicado a 4 direcciones IPs y no contemplo el escaneo de versiones de los sistemas operativos, de aplicaciones, escaneo de puertos TCP y UDP, escaneo de vulnerabilidades WEB entre otro y el plan de remediación no ha sido implementado. En consecuencia, se deriva un potencial riesgo toda vez que existe una debilidad en cuanto al cumplimiento en su totalidad del control numeral A.12.6.1 de la norma ISO27002:2013, por tal motivo se hace necesario: 1.Llevar a cabo la implementación del plan definido para el análisis y remediación del año 2022. Nota: El análisis de vulnerabilidades técnico se deberá aplicar a los elementos críticos de la entidad con las herramientas adecuadas y 2. Realizar seguimiento a los

resultados obtenidos.

10.7. Al consultar el documento de Políticas específicas de seguridad de SI en el numeral: 6.22, se define la política de SI con relación con los proveedores y establece en uno de sus literales la divulgación de las políticas y procedimientos de seguridad de la SDS a los proveedores, sin embargo se evidencia que al solicitar los soportes o registros de las divulgaciones realizadas de las políticas de seguridad de los nuevos contratos de TIC estos no fueron suministrados. En consecuencia, se deriva un potencial riesgo toda vez que existe una debilidad en cuanto al cumplimiento en su totalidad de los control numerales A.15.1.1 y A.15.1.2 de la norma ISO27002:2013, por tal motivo se hace necesario:1. Acordar con los proveedores de los nuevos contratos, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos de información de la entidad, estos riesgos tienen que ver con las actividades de: acceder, procesar, almacenar, comunicar información de la entidad y 2. Realizar la divulgación de las políticas de seguridad a los proveedores y contar con registro de la actividad.

10.8. En la operación una de las responsabilidades del grupo de especialistas del SOC es realizar el monitoreo, reconocimiento y análisis de los eventos de seguridad mediante las diferentes herramientas de seguridad y con ello determinar si algunos de los eventos recibidos debido a su criticidad y sus características se define como incidentes. A partir de esto se evidencia que los especialistas del SOC no están realizando el registro de incidentes en el software de ARANDA ya que al consultar la base general con corte a Febrero 2022, no existen registros de incidente provenientes del canal de especialistas del SOC. En consecuencia, se deriva un potencial riesgo toda vez que existe una debilidad en cuanto al cumplimiento en su totalidad del control numeral A.16.1.4 de la norma ISO27002:2013, por tal motivo se hace necesario: 1. evaluar eventos y decidir su clasificación como incidentes de seguridad de la información y 2. Registrar los incidentes de seguridad en la herramienta de ARANDA para tener control total de los diferentes casos presentados.

10.9. Al consultar la matriz de declaración de aplicabilidad - SOA, se evidencia que se encuentra desactualizada ya que varios de los controles se encuentran en blanco o no están diligenciados, además y las exclusiones en caso haberlas no están identificadas. Por lo anterior, se deriva un potencial riesgo toda vez que existe una debilidad en cuanto al cumplimiento en su totalidad del requisito numeral 6.1.3 literal d) de la norma ISO27001:2013, por tal motivo se hace necesario: 1. Actualizar y publicar la matriz.

10.10. Al consultar el plan de seguridad del año 2021, se evidencia que varias de las actividades programadas no se realizaron y se reprogramaron para el año 2022 y se informa que fue debido a que no se tuvo contrato con el proveedor etb por el tiempo de 10 meses, dichas actividades para la atención del centro de cómputo y soporte de la mesa de ayuda - línea 55 se realizaron mediante contingencia con apoyo del personal de planta de la Dirección TIC. Sin embargo, los servicios se vieron impactados ya que la atención de los múltiples requerimientos e incidentes

tuvieron altos tiempos de respuesta y la línea de contacto telefónica no se respondía ningún tipo de llamada. En consecuencia, se deriva un potencial riesgo toda vez que existe una debilidad en cuanto al cumplimiento en su totalidad del requisito numeral 5.1 literal e) de la norma ISO27001:2013, por tal motivo se hace necesario: 1. Gestionar con anticipación la etapa precontractual y contractual de dicha necesidad con la Subdirección de contratación. 2. Empatar la finalización del contrato con la declaración del acta de inicio del nuevo contrato. Garantizando que la operación no se vea afectado por no contar con el recurso humano especializado.

10.11. Al consultar el tablero de control de los proyectos de inversión – PAA 2021, se identifican 35 iniciativas o compras de TIC que tienen relación con los proyectos del PETIC, sin embargo, se evidencia que el seguimiento que en la actualidad se realiza desde la dirección TIC, es orientado a proyectos de inversión PAA y no a proyectos de TI, además cada iniciativa del PETIC es gestionada de manera independiente por cada líder y no existe una articulación que permitirá conocer el todo. Adicionalmente no existe un PMO-TIC que permitirá centralizar y gestionar los diferentes proyectos TIC. En consecuencia, se deriva un potencial riesgo toda vez que existe una debilidad en cuanto al seguimiento y medición a la ejecución del PETIC, por tal motivo se hace necesario: 1. Conformar la PMO-TIC que permita la centralización, consolidación y seguimiento de proyectos e iniciativas 2. Dar a conocer a todas las partes interesadas el propósito de esta oficina y 3. Gestionar de manera unificada el PETIC, con el fin de conocer su avance de manera consolidada.

10.12. Si bien es cierto, al consultar el documento de políticas específicas definido en el numeral 6.7.3, se definen las reglas para el manejo de la seguridad de la información para el proceso de desarrollo de software, evidenciamos que dicha política no define una regla y tampoco se aplica una metodología de desarrollo seguro de software acorde al ciclo de vida SDLC en la actualidad, Por lo anterior, existe una debilidad en los códigos fuentes generados, los cuales son vulnerables a un posible ataque informático. Se deriva un potencial riesgo toda vez que existe un cumplimiento parcial del control A.14.2.1 de la norma ISO27002:2013, por tal motivo se hace necesario: 1. Ajustar y aprobar la política incorporando la metodología a seguir, 2. Implementar la metodología en la operación y 3. Hacer seguimiento de los requerimientos que cumplieron con la metodología.

10.13. Al realizar las entrevistas con los especialistas encargados y con el fin de conocer el grado de implementación, revisión y evaluación de la continuidad de la seguridad de la información en la entidad, evidenciamos que los planes DRP y el análisis BIA se encuentra en etapa de elaboración, a la fecha no se ha realizado ningún tipo prueba de los DR y además en lo que respecta al BCP de seguridad no se tienen definidos métricas de RTO, RPO y SDE. En consecuencia, existe una debilidad en cuanto al cumplimiento en su totalidad de los controles A.17.1.2 y A.17.1.3, ya que la entidad debe: establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa y adicionalmente se debe hacer verificación, revisión y evaluación de la continuidad de la seguridad de la información, por tal motivo se hace necesario: 1. Llevar a cabo la implementación del plan o cronograma de continuidad trazado para el año 2022, 2. Definir,

implementar y mantener procesos, procedimientos y controles orientados a la continuidad de los servicios, 3. Realizar el seguimiento del avance en la implementación del plan trazado y 4. Dar a conocer a las partes interesadas los diferentes entregables resultado del plan.

11. CONCLUSIONES.

- El gobierno de seguridad de la información de la SDS esta delegada a la dirección TIC, pero al ser un tema transversal que aplica a todos los procesos podría ser un tema liderado por un proceso estratégico.

- En el esquema de roles y responsabilidades, no existe la figura del Oficial de Seguridad de la Información y las responsabilidades están repartidas en el director TIC y los diferentes especialistas de SI.

- Las diferentes dependencias como son: Jurídica, Talento Humano, Comunicaciones, Bienes-Servicios y Asuntos Disciplinarios juegan un papel fundamental dentro del sistema, pero no están definidas sus responsabilidades en el esquema de roles y responsabilidades.

- Seguir fortaleciendo mediante campañas de sensibilización a todos los funcionarios de la entidad de tal forma que se maneje un lenguaje común frente a los diferentes conceptos en el marco de la seguridad de la información.

- El documento de “política general” no ha sido revisado como buena práctica y por lo tanto no ha tenido ajustes o mejoras desde su creación, adicionalmente no se encuentra en el formato institucional.

- El documento SOA o la Declaración de Aplicabilidad se encuentra desactualizado, varios de los controles no han sido documentados y las exclusiones no se encuentran justificadas, lo que se considera una debilidad.

- La continuidad de negocio es un tema estratégico y transversal en la organización, sin embargo, algunos de los componentes que se han adelantado están bajo la responsabilidad de la Dirección TIC.

- El estado de los elementos del plan de continuidad de negocio es el siguiente: BIA-Análisis de Impacto el negocio se encuentra en un avance del 25%, RTO, RPO y SDO no han sido definidos, DRPs se encuentra en un avance del 25% ya que los planes de recuperación no han sido formalizados y probados o que se considera una debilidad importante.

- El Análisis de vulnerabilidades técnicas realizado en el mes enero del 2022, fue aplicado a solo 4 IPs y no a todos los elementos considerados críticos

dentro de la entidad, por lo que existe una exposición importante frente a las diversas vulnerabilidades que no se conocen. El escaneo debe involucrar la detección de las versiones de los sistemas operativos, la detección de las versiones de las diferentes aplicaciones, escaneo de puestos TCP y UDP, escaneo de vulnerabilidades WEB entre otro. Por último el plan de remediación no ha sido aplicado lo que se considera una debilidad importante.

- La evaluación de riesgos de seguridad y controles que se encuentra definida por la dirección de planeación institucional y calidad mediante el formato de “autoevaluación”, no ha sido del todo eficaz ya que varias de las dependencias no remitieron la información en los tiempos establecidos y pasado los 6 meses después sigue sin ser solucionado, lo que considera una debilidad importante.

- Encontramos que los inventarios de activos de información, no cuentan con elementos de TIPO: hardware, como son: servidores, firewall, switches, routes, entre otros, ya que los referentes del proceso indican que estos elementos no contienen información. Lo cierto es que dichos elementos son esenciales para garantizar la disponibilidad y continuidad de los servicios ofrecidos, por lo tanto, deberán ser incluidos para garantizar un inventario sólido. Dicho aspecto se considera una debilidad importante.

- No todos los registros de cambio documentados mediante el formato SDS-TIC-FT-025, han sido registrados en la herramienta ARANDA, lo que genera una debilidad importante al proceso ya que no está llevando una gestión eficiente de los casos incumpliendo con el instructivo definido.

- El grupo de desarrolladores no ejerce ninguna de las buenas prácticas para el manejo de desarrollo seguro por lo que existe una amenaza latente frente al código vulnerable. Al no existir la política incumple con el requisito y deriva en una no-conformidad.

- Políticas de seguridad en relación los proveedores existen y establece 6 aspectos a aplicar, sin embargo, la actividad de divulgar a los proveedores las políticas y procedimientos de seguridad de la SDS no se hace, lo que se considera una debilidad importante.

- En la secretaria el proceso de gestión de incidentes de seguridad no trata la gestión "postincidente", es decir el análisis causa raíz, determinar el origen o atacante y definir las medidas para evitar que ocurra no se realiza hoy en día, lo que deriva en una oportunidad de mejora.

- Es indispensable seguir realizando con cierta periodicidad ejercicios de auditorías internas con énfasis a la seguridad de la información, que

permitan evaluar los diferentes requisitos de norma y determinar el nivel de madurez del sistema.

- Oportunidades de mejora, así como las no conformidades en algunos de los casos fueron unificadas para facilitar el ejercicio de elaboración del plan de mejoramiento.

- Las actividades programadas del plan de seguridad del año 2021 no se cumplieron en su totalidad y se reprogramaron en el plan del año 2022, una situación que se viene presentado año a año y no se han tomado los correctivos del caso.

- Respecto a la continuidad en la prestación de los servicios de la mesa de servicios de TI o línea 55, es indispensable gestionar con la subdirección de contratación de manera anticipada, la etapa precontractual y contractual de tal forma que la operación no se ve afectada o disminuida como ocurrió en esta oportunidad y que fue indispensable poner en funcionamiento la contingencia. Cabe señalar que la contingencia no encuentra documentada y tampoco existe socialización a las partes interesadas lo que sugiere una oportunidad de mejora.

- El control respecto a los usuarios y contraseñas de los servicios que soportan la infraestructura está a cargo de la dirección TIC y la responsabilidad de la administración de los sistemas de información de las áreas misionales, recae sobre los administradores designados en cada dependencia.

- Para el manejo de los equipos desentendidos, escritorios limpio/pantallas limpias el grupo de seguridad de la información mediante campañas informativa, realiza con cierta periodicidad él envió de TIPS informativos mediante correo masivo institucional. Se sugiere seguir fortaleciendo esta campaña, generando nuevos contenidos y dándola a conocer a todas las partes interesadas.

12. PLAN DE MEJORAMIENTO

Es responsabilidad de las dependencias elaborar el plan de mejoramiento adecuado que elimine las no conformidades y responsa a las oportunidades de mejora especificadas.

Nota: de ser necesario, deberán realizar las mesas de trabajo para para abordar las acciones que involucren la interacción con otras dependencias.

13. ANEXOS.

Listadechequeo-GestiónTICparte1VFabr2022.xlsx
Listadechequeo-GestiónTICparte2VFabr2022.xlsx

NOMBRE, APELLIDO Y FIRMA DEL AUDITOR

FRANCISCO JAVIER PINTO GONZALEZ

APRUEBA JEFE OFICINA DE CONTROL INTERNO,

OLGA LUCIA VARGAS COBOS