INFORME FINAL TRABAJO DE AUDITORÍA

SEGURIDAD DE LA INFORMACION BAJO LA NORMA ISO27001 y 27002:2013

OFICINA DE CONTROL INTERNO

AUDITOR:

LÍDER: FRANCISCO JAVIER PINTO GONZALEZ
Lead Auditor ISO27001:2013 registro ERCA No.1001545
CISM ISACA No. 221867531 y
Líder en Ciberseguridad con Certiprof

REVISADO POR:

OLGA LUCIA VARGAS COBOS
JEFE OFICINA DE CONTROL INTERNO

BOGOTÁ, septiembre 2024

SECRETARÍA DISTRITAL DE SALUD

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

Contenido

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

Abreviaturas

- AD: Directorio Activo de Windows
- CONPES: Consejo Nacional de Política Económica y Social
- ERP: Sistema de planificación de recursos empresariales
- IEC/ISO: norma internacional creada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC)
- IDCBIS: Instituto Distrital de Ciencia, Biotecnología e Innovación en Salud
- NIA: Norma Internacional de Auditoría
- MINTIC: Ministerio de Tecnologías de la información y comunicaciones.
- MIPG: Modelo Integrado de Planeación y Gestión.
- MSPI: Modelo de Seguridad y Privacidad de la Información
- NIST: Instituto Nacional de Estándares y Tecnología
- OCI: Oficina de control interno
- POGD: Plan operativo de Gestión y Desempeño
- SEGPLAN: Sistema de Seguimiento al Plan de Desarrollo Distrital mediante los Proyectos de Inversión
- SDS: Secretaria Distrital de Salud
- SNMP: Protocolo simple de administración de red
- SOA: Declaración de Aplicabilidad
- SOC: Centro de Operaciones de Seguridad
- TIS: Total integratión System
- URL: Localizador de Recursos Uniforme
- WEB: World Wide Web que en español traduce “red informática mundial” o Sitio en Internet.

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

INTRODUCCION

Las auditorias son una herramienta que las entidades o compañías utilizan para conocer el estado de los procesos y productos, determinando su eficiencia y eficacia mediante una evaluación objetiva y metódica que permite tomar decisiones y controlar las necesidades o debilidades identificadas. La auditoría especifica con énfasis en riesgo a la gestión de la seguridad de la información en la SDS, busca identificar las debilidades o falencias existentes de acuerdo con el modelo de protección y seguridad de la información y los diversos controles que lo componen. Así mismo, se busca mejorar, mantener y darle continuidad a las prácticas que viene siendo exitosas y que han permitido a nivel institucional cumplir con los objetivos establecidos. De acuerdo con lo anterior, la auditoria se realizó bajo una mirada transversal que involucró diferentes dependencias, evaluando los diferentes requisitos con base en la normatividad y legislación relacionada.

MARCO CONCEPTUAL

El Modelo de Seguridad y Privacidad de la Información también conocido como – MPSI liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, imparte los lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas en materia de seguridad de la información, tomando como referencia el estándar internacional ISO27001 e ISO27002, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), logrando a su vez la alineación e implementación de la Política de Gobierno Digital - Decreto 1008 de 2018 y su habilitador transversal de seguridad de la información. La planificación e implementación del Modelo MSPI en la SDS, está determinado por las necesidades, objetivos, requisitos de seguridad, el mapa de procesos, estructura de la SDS y su objetivo principal consiste en preservar la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas, dicho modelo es actualizado periódicamente y recogerá los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras.

La normatividad y legislación en Colombia respecto al tema viene en aumento, es por eso, que han surgido los siguientes elementos que deberán serán adoptados gradualmente por las entidades como son:

- CONPES 3701 de 2011, busca generar lineamientos de política en ciberseguridad y ciberdefensa, con el fin de desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas.

- CONPES 3854 de 2016, corresponde a la política nacional de seguridad digital, que

estable la gestión de riesgos como elemento primordial para abordar la seguridad digital.

- CONPES 3995 de 2020, corresponde a la Política Nacional de Confianza y Seguridad Digital y tiene por objetivo establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital.

El modelo pretende facilitar la construcción de la política de privacidad por parte de la entidad y fija los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con la información.

Es importante tener presente que la norma ISO27001:2013 certificable, evalúa el ciclo de vida del sistema de acuerdo a los 6 dominios y en lo que respecta al código de buenas prácticas ISO27002:2013, se evalúan 14 dominios y 114 controles, todos estos elementos descritos hacen parte del instrumento de autoevaluación del MinTIC y permite a cada entidad conocer el nivel de avance en la implementación del modelo de seguridad de la información. Para efectos de la presente auditoria se seleccionaron varios de los requisitos para determinar su conformidad.

Finalmente, el plan de auditoria definido, contemplaba la revisión mediante la norma actualizada ISO27002 versión: 2022; sin embargo, en la reunión de apertura, los auditados argumentaron que la entidad no está preparada para este cambio y los controles no han sido implementados o adoptados, en consecuencia, se propuso que se evalué con base con la Norma ISO27001 en versión 2013. Es importante precisar, que en la vigencia 2023 para la misma auditoría realizada en el mes de abril, se evidenció esta misma situación y se propuso que en el plan de mejoramiento presentado en el informe final, se vinculara esta mejora permitiendo que la entidad se encuentre en sintonía con los marcos de referencia actualizados. A la fecha se sigue presentando o reiterando esta misma debilidad y por consiguiente se deriva una oportunidad de mejora.

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

Determinar el estado de la seguridad de la información en la entidad con base al ciclo PHVA y las buenas prácticas como es la Norma Certificable ISO 27001, el código de buenas prácticas ISO 27002 y complementarias. Así mismo, verificar la gestión y los componentes de control, en lo que tiene que ver con: ambiente de control, actividades de control, gestión del riesgo, actividades de monitoreo e información y comunicación.

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

2.1 Evaluar las medidas de protección (controles) que se tiene implementados en la entidad y analizar los riesgos existentes, en cumplimiento de las medidas y políticas de seguridad establecidas.

2.2 Analizar las políticas y procedimientos de seguridad definidos de cara a los requisitos establecidos.

2.3 Verificar el estado de implementación del marco normativo y regulatorio asociado.

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. (NIA 2220).

Contempló la evaluación de requisitos mínimos seleccionados para conocer estado de la Seguridad de la Información de la entidad de acuerdo con ciclo de vida PHVA o lo concerniente al modelo MSPI o Modelos de protección y seguridad de la información impartida por el ministerio de las TIC y la alta consejería para las TICs.

Periodo a evaluar:

- Desde: 1/01/2023
- Hasta: 31/07/2024

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

Para el desarrollo de la presente auditoría se tuvieron en cuenta los siguientes elementos:

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

Procedimientos:

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

Políticas:

- Seguridad de la información
- Manual de seguridad de la información

4.2 Externos (leyes y regulaciones que apliquen)

- Norma IEC ISO 27001:2013 y Anexo A
- Norma IEC ISO 31000:2018 y 27005 para Gestión de Riesgos
- Norma IEC ISO 22301:2012 Continuidad de Negocio.
- Decreto 1008 de 2018 - Política de Gobierno Digital, habilitadores transversales SI
- Decreto 1499 de 2017 – MIPG
- CONPES 3854 del 2016 - Política Nacional de Seguridad Digital
- CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital
- Ley 1273 de 2009 - Delitos informáticos
- Ley 1581 del 2012 protección y tratamiento de datos personales

Ejercicio basado metodológicamente en listas de chequeo a partir de los requisitos seleccionados para este propósito.

5. METODOLOGÍA UTILIZADA. (NIA 2300).

La presente auditoría se desarrolló mediante mesas de trabajo presenciales con los diferentes referentes designados, verificando y constatando la conformidad de los requisitos normativos seleccionados mediante lista de verificación elaborada. Se realizó la toma de casos aleatorios y análisis de la información referente a los procedimientos, registros documentales, registros de riesgos, herramientas, entre otros. Las mesas de trabajo fueron agendadas acorde a la programación establecida.

Adicionalmente el auditor tuvo en cuenta los siguientes aspectos:

Visita de Sitio: El auditor realizo visita a las instalaciones de la sede administrativa pisos 1 y 6, porterías, acceso a los parqueaderos y áreas sensibles, con el objetivo de verificar o constatar la conformidad de los controles de seguridad físicos y del ambiente seleccionados, que hacen parte de la normatividad asociada y al modelo de seguridad de la información.

Revisión de la documentación de seguridad de la información: El auditor solicitó y revisó la documentación existente y relacionada con la gestión de la seguridad de la información, entre los documentos consultados se encuentran: política de seguridad de la información, manual de política de seguridad de la información, procedimientos varios, registros de actas de reunión, registros de asistencia, entre otros.

Consultas con el personal designado: El auditor realizó consultas específicas a los funcionarios designados de la entidad y consultó piezas comunicativas elaboradas y desplegadas en el periodo, con el fin de determinar el nivel de concientización frente a la seguridad de la información aplicada en la entidad.

Listados de verificación para los auditados: El auditor entrega de manera anticipada la lista de requisitos de revisión, la cual se trabajó en compañía de los referentes designados y personal que acompaño el ejercicio. Estos listados serán una imagen cualitativa del estado de la seguridad de la información de la entidad respecto a la norma ISO 27001:2013 y el ANEXO-A.

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

La presente auditoría, se llevó a cabo mediante recolección de información de diferentes fuentes, canales y como resultado de las diferentes mesas de trabajo realizadas, acompañadas de listas de chequeo, y verificación de matrices de riesgos, entre otros documentos e instrumentos, que permitieron conocer los procedimientos y las prácticas utilizadas en la entidad para garantizar la seguridad de la información. En cuanto a los resultados de la evaluación, estos fueron analizados, con el fin de determinar posibles debilidades o falencias, evidenciando las causas que las originan y proponiendo alternativas que permitan mitigarlos, dichos resultados serán presentados a lo largo del presente informe.

6.1 ANALISIS POR COMPONENTES DEL MECI

A continuación, el análisis general por componente:

TEMAS REVISADOS	ASPECTOS VERIFICADOS
6.1.1. Ambiente de control: Es el conjunto de procesos y estructuras que proveen las bases para llevar a cabo el control interno a través de la organización	Contempló la revisión de las herramientas y técnicas empleadas para el establecimiento de las actividades y los recursos que son necesarios para la operación diaria y que apoyan la seguridad de la información en la entidad. Es importante señalar que el despliegue a nivel institucional es amplio, toda vez que la seguridad de la información es un tema transversal y requiere del compromiso de todos los colaboradores para dar cumplimiento a las políticas establecidas. Desde la estructura jerárquica, se cuenta con un líder del sistema y gestores de seguridad de la información en cada una de las dependencias, estos gestores asisten al comité técnico convocado por el líder y es el escenario para dan a conocer temas relacionados con la seguridad de la información a su vez los gestores deben retroalimentar a los colaboradores en cada una de las dependencias, asegurando la multiplicación de conocimiento. Contempló la revisión de diferentes procedimientos operativos, procedimientos ligados al proceso, instructivos, guías y demás controles definidos, al fin de brindar un cubrimiento transversal de cara la seguridad de la información. Estos elementos permiten llevar a cabo una revisión anual por parte de la oficina de control interno. **Respecto** al particular, se cuenta con listado de preguntas realizadas en cada una las mesas y en tal medida nos permitió constatar el cumplimiento de los criterios evaluados.
6.1.2. Actividades de Control (incluye la revisión de políticas de operación procedimientos, normatividad interna y externa, Plan Operativo Anual	1. Consistió en la verificación y evaluación del marco normativo y la legislación asociada, así como las políticas internas definidas: • **Norma IEC ISO 27001:2013 y Anexo A**: contempla un conjunto de 114 Controles Técnicos y Administrativos

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

	agrupados en 14 dominios, para efectos del ejercicio y mediante lista de verificación se seleccionaron y evaluaron 63 controles y de la norma certificable se seleccionaron 30 criterios. • **Norma IEC ISO 31000:2018 y 27005:** permite el análisis y la gestión de Riesgos de Seguridad de la información. Al particular se constata falencias y debilidades en la gestión del riesgo, toda vez que la práctica se realiza una vez al año, no todos los proceso remiten la información en los tiempos establecidos, se evidencian riesgos que se han materializado, lo que demuestra que los controles actuales no han sido eficaces o suficientes, ahora bien, el riesgo se materializa pero el proceso no toma los correctivos inmediatos y las matrices de riesgos no sufren ningún cambio. El proceso argumenta que se encuentra adelantando la definición de una metodología diferente para dar respuesta a esta situación evidenciada. • **Decreto 1008 de 2018 - Política de Gobierno Digital**, en lo que respecta al habilitador transversal de seguridad de la información, al particular, se informa, que se viene implementado gradualmente en la medida que el ministerio de las TIC en conjunto con la Alta consejería de las TIC imparte objetivos a realizar año a año de cara al Modelo de Seguridad y privacidad de la información. • **Decreto 1499 de 2017 – MIPG**, contempla la implementación de las políticas de gobierno Digital y Seguridad digital. En lo que respecta a la política Seguridad Digital, se seleccionaron y evaluaron 63 controles del Anexo A y de la norma Certificable se seleccionaron y evaluaron 30 requisitos. • **CONPES 3854 del 2016 - Política Nacional de Seguridad Digital**. Al particular se informa que la implementación se origina a partir de los requerimientos presentados por el ministerio de la TIC a solicitud y no por iniciativa propia. No se cuenta con un instrumento que permita conocer el grado y estado de implementación de la política lo cual es una debilidad existente. • **CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital**. Al particular se informa que la implementación se origina a partir de los requerimientos presentados por el ministerio de la TIC a solicitud y no por iniciativa propia. No se cuenta con un instrumento que permita conocer el grado y estado de implementación de la política lo cual es una debilidad existente. • **Ley 1273 de 2009 - Delitos informáticos**. De acuerdo con lo informado, la ley se encuentra en vigor, no obstante, a la fecha no se han identificado incidentes de seguridad que hayan puesto en riesgo la seguridad de la información y que permita demostrar que hubo un delito informático. • **Ley 1581 del 2012 protección y tratamiento de datos personales:** actualmente se encuentra implementada ya que varios de los sistemas de información en operación, han implementado la política de datos personales y sensibles.

	Dichas bases son reportadas a la SIC y la información sensible que reposa en las bases solo es accedida y consultada por personal autorizado. 2. La evaluación contemplo la política general y el manual de seguridad de la información que contiene los objetivos y las políticas específicas. 3. Así mismo, se evaluaron los procedimiento codificados: • SDS-TIC-PR-005 SEGURIDAD INFORMÁTICA • SDS-TIC-PR-002 GESTIÓN DE INCIDENTES Y REQUERIMIENTOS • SDS-TIC-PR-001 GESTIÓN SOLUCIONES DE SOFTWARE Instructivos y documentación asociada que hacen parte del repositorio documental para el presente alcance.
6.1.3. Evaluación del Riesgo y controles (incluye análisis de contexto, riesgos relacionados identificación de controles y su operación, posibles riesgos detectados)	Primer aspecto verificado: Al particular, existe un grupo de matrices de riesgos de seguridad de la información que son responsabilidad de cada proceso en la entidad. Metodológicamente se tiene establecido que cada proceso tiene la responsabilidad de diligenciar la matriz, así como el instrumento de autoevaluación con base en la guía establecida, dicha actividad es liderada por la Dirección TIC. A principio del año y mediante memorando formal se remite a todas las dependencias; sin embargo y de acuerdo a lo evidenciado, no todas las matrices son remitidas en los tiempos establecidos y es necesario reiterar la solicitud para que las dependencias faltantes lo hagan, sin embargo, trascurridos 6 meses de haber hecho la solicitud, aún no se tienen todas las respuestas, lo cual corresponde a una debilidad del proceso y a una primera situación evidenciada. Nota: Las dependencias que a la fecha no han reportado o remitido las matrices son: Subdirección de Bienes y Servicios, Subsecretaria Corporativa, DAEPS, Laboratorio y Dirección de Servicio a la Ciudadanía. Segundo aspecto verificado: En lo que respeta a las matrices remitidas, al consultar algunas de ellas, se observan los riesgos identificados y valorados. Además, se cuenta con el plan de tratamiento y el seguimiento respectivo mediante el instrumento de autoevaluación. Al comparar la valoración del riesgo residual de un año a otro evidenciamos de un proceso en específico, sigue siendo la misma. Si bien es cierto, se gestiona el riesgo y se cuenta con elementos que respaldan dicho ejercicio, al comparar el registro de riesgo del 2024 con el del año 2023, identificamos que la severidad del riesgo se mantiene; si los controles implementados han sido eficaces y suficientes y el instrumento de autoevaluación reporta que no hubo materialización, esto conllevaría a que la severidad del riesgo residual cambie. Tercer aspecto verificado: a lo largo del año 2024 y en el último mes, ha sido reiterativo las caídas por corte de fluido eléctrico

	que han afectado las estaciones de trabajo y demás dispositivos en el edificio administrativo por cortes del operador CODENSA en el sector sin previo aviso. En el mes de marzo de acuerdo con el reporte presentado, hubo una caída de energía que afectó el datacenter contenedor y el servidor de HIPERCONVERGENCIA que agrupa varios servicios de la entidad. Es importante señalar que el restablecimiento del servicio no fue inmediato y tomó en algunos casos varios días. Así mismo se conoció un caso en donde los servicios no fueron restablecidos, ya que la información almacenada mediante backup no fue recuperada. Dicha situación expuesta, demuestra que los controles actuales no son eficaces y suficientes lo que conllevo a la materialización del riesgo y por consiguiente dicha situación deriva en una oportunidad de mejora.
6.1.4. Actividades de monitoreo (incluye las acciones que la primera y segunda línea de defensa ejercen para mitigar la ocurrencia de los riesgos sean este seguimiento al cumplimiento de políticas, actividades, directrices, metas)	Se llevó a cabo la verificación y el resultado fue el siguiente: **Primera Línea (Autocontrol):** • La Dirección TIC ejerce su rol de liderazgo frente al sistema, articula y direcciona todas las necesidades mediante los comités técnicos y el comité de gestión y desempeño, no obstante, el cumplimiento de los controles de seguridad está en manos de cada colaborador y se está dando respuesta a las políticas de seguridad definidas. Así mismo, cada gestor de seguridad de la información, juega un papel crucial, ya que debe impartir los conocimientos adquiridos a todos los colaboradores de su área o dependencia. • Implementar acciones correctivas: Se consultan las acciones registradas en el aplicativo isolucion, producto de la auditoria al sistema realizada en el año 2023, acciones de mejora que la mayoría fueron implementadas y se comprobó su eficacia. **Segunda Línea (Autoevaluación):** **Obligaciones:** • Asegurar 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. **Resultados:** • La Dirección TIC, establece y adopta las metodologías para que cada referente en la entidad, presente la información de cara a la gestión de activos de información y los riesgos de seguridad de la información. • Los controles de tipo administrativo y técnicos que fueron objeto de la presente evaluación, serán presentados mediante tablas determinando cuales requisitos: “Cumplen”, “No Cumplen”, y cuales derivan en Oportunidades de Mejora.

	• En lo que respecta a la supervisión de la metodología de la gestión de riesgo hasta el momento y de acuerdo a lo evidenciado, no está siendo eficaz, toda vez que no todas las dependencias la están aplicando, no hacen entrega de información en los tiempos definidos, no se realiza actualización dinámica y propia de las matrices, y algunos riesgos se han materializado, a la fecha los controles siguen siendo ineficaces y no ha sido reformulados o adicionando nuevos controles. El referente auditado, informa que el proceso de gestión de riesgo será reformulado.
6.1.5. Información y comunicación	• Se verificó el proceso, procedimientos, registros e información compartida, así como aplicativos con interfaz WEB puestos en producción. Es clave mencionar que de cara a la política de desarrollo seguro, se evidencia que existen algunos aplicativo en el ambiente de producción que utilizan protocolo HTTP puerto 80 y 8080 o protocolo no seguro. Lo cual va en contravía de la política definida y corresponde a una vulnerabilidad que puede ser aprovechada por un atacante. Dicho lo anterior, se deriva una oportunidad de mejora. • Se solicitaron y consultaron algunas piezas comunicativas que reflejan las campañas de sensibilización en temas de seguridad de la información desarrolladas, Para crear una cultura de seguridad, es indispensable fortalecer dichas campañas incorporando temas que no han sido abordados y reiterando las temas ya impartidos. Así mismo, se cuenta registros de inducción y reinducción realizados a los funcionarios de carrera administrativa. • Por último, se cuenta con registros de actas de reuniones de revisión por la dirección y comités técnicos que son escenarios para comunicar los diferentes temas a las partes interesadas.

Una vez realizado el análisis de la información obtenida, resultado de las mesas de trabajo realizadas, encontramos los siguientes resultados:

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

6.2 Evaluación integral mediante lista de chequeo

El ejercicio mediante lista de chequeo, contempló la evaluación así: 30 requisitos de la Norma ISO27001:2013 y 63 requisitos de Norma ISO27002:2013, y con ellos los procedimientos relacionados. A continuación, mediante tablas agrupadas, se presentan los requisitos y los resultados obtenidos.

Nota: El detalle de la evaluación para cada requisito y control hace parte de los papeles de trabajo utilizados, así mismo se cuenta con las grabaciones realizadas que soportan el ejercicio como evidencia digital.

A continuación, mediante tablas se representan los resultados obtenidos respecto a los requisitos y controles seleccionados:

Convenciones: Color Verde: Cumple, Color Rojo: No cumple y Color Azul: Acción para abordar riesgo u Oportunidad de mejora

Requisitos evaluados	CUMPLEN	OPORTUNIDAD DE MEJORA.	NO CUMPLE.	TOTAL REQUISITOS
10 Mejora	1			1
10.2 Mejora continua	1			1
5 Liderazgo	8	3		11
5.1 Liderazgo y compromiso	3			3
5.2 Política	5	1		6
5.3 Roles organizacionales, responsabilidades y autoridades		2		2
6 Planificación	5	1		6
6.1.2 Valoración de riesgo de la seguridad de la información	2			2
6.1.3 Tratamiento de riesgo de la seguridad de la información	2	1		3
6.2 Objetivos de seguridad de la información y planificación para lograrlos	1			1
7 Apoyo	5			5
7.1 Recursos	1			1
7.2 Competencias	2			2
7.5 Información documentada	2			2
8 Operación	1	2		3
8.1 Planificación y Control operacional	1			1
8.2 Valoración de riesgo de la seguridad de la información		1		1
8.3 Tratamiento de riesgo de la seguridad de la información		1		1
9 Evaluación de desempeño	3	1		4
9.1 Seguimiento, medición, análisis y evaluación	1	1		2
9.2 Auditoría interna	1			1
9.3 Revisión por la dirección	1			1
Total general	**23**	**7**		**30**

Tabla 1: Norma ISO27001:2013

La tabla1, resume la evaluación realizada de cara a los 6 dominios de la norma y los 30 requisitos seleccionados, de los cuales 23 requisitos que equivalen al 77% del universo, “Cumplen”, mientras que 7 de los requisitos evaluados que equivale al 23%, presentan debilidades que fueron evidenciadas y documentadas. De acuerdo a lo anterior, para las

oportunidades de mejora presentadas, será indispensable definir un plan de mejoramiento que permita fortalecer y afianzar cada uno de estos elementos.

Evaluación x Dominios	CUMPLE.	OPORTUNIDAD DE MEJORA.	NO CUMPLE.	Total Requisitos
A.10 Criptografía	1	1		2
A.11 Seguridad física y del ambiente	5	4		9
A.12 Seguridad de las operaciones	6	3		9
A.13 Seguridad de las comunicaciones	2			2
A.14 Adquisición, desarrollo y mantenimiento del sistema	4	1		5
A.15 Relaciones con el proveedor	3			3
A.16 Gestión de incidentes de seguridad de la información	4	1		5
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	1		3	4
A.18 Cumplimiento	2	1		3
A.6 Organización de la seguridad de la información	4			4
A.7 Seguridad ligada a los recursos humanos	4	2		6
A.8 Administración de activos	4	1		5
A.9 Control de acceso	5	1		6
Total general	**45**	**15**	**3**	**63**

Tabla 2: Norma ISO27002:2013

La tabla 2, resume la evaluación realizada frente a 13 dominios y 63 controles seleccionados, de los cuales 45 controles equivalente 71% del universo evaluado “Cumplen”, identificamos que 15 controles que equivalen a un 24% de la población requieren iniciar una oportunidad de mejora, mientras que 3 controles “no cumplen” y se decreta una no-conformidad. Es importante señalar que, este último, requerirá de una acción correctiva que hará parte del plan de mejoramiento y que busca fortalecer y afianzar cada una de las debilidades detectadas.

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

Evaluación agrupada X Dependencias	CUMPLE.	OPORTUNIDAD DE MEJORA.	NO CUMPLE.	Total Requisitos
Asuntos Disciplinarios	1			1
Bienes y Servicios	4	3		7
Dirección TIC	30	8	3	41
Dirección TIC/Talento Humano	1			1
Talento Humano	2	2		4
Dirección TIC - Equipo de Desarrollo	5	1		6
Oficina Jurídica/Dirección TIC	2	1		3
Total general	**45**	**15**	**3**	**63**

Tabla 3: Norma ISO27002:2013 (Agrupado por dependencias)

A continuación, mediante tablas se listan los hallazgos encontrados que derivan en oportunidades de mejora:

Parte 1: Análisis con respecto a la Norma ISO27001:2013

Numero de Hallazgo	**1**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control	**Resultado de la Evaluación**
5.2 Política Literal f) ser comunicada dentro de la organización	La política fue divulgada en la mesa técnica de gobierno y seguridad digital, comité institucional de gestión y desempeño y también se dio a conocer en la reunión de gestores de SI realizadas en el año 2023 y 2024 y la divulgación específica de las políticas de seguridad de información se informa que se brindó a los colaboradores de la entidad, tanto de planta, como de contrato y se enviaron algunas piezas comunicativas mediante el correo institucional. La Dirección TIC como gobierno de SI en la entidad, remitió memorandos a cada una de las dependencias y definió la responsabilidad de los gestores de seguridad de brindar asistencia y orientación a los usuarios internos y externos sobre la SI. Mediante el contrato suscrito, se tiene contemplado el plan de capacitación con el proveedor “GAMA ingenieros” que actualmente es el proveedor encargado del centro de operaciones de seguridad – SOC. Como evidencia se cuenta con el memorando nro. 2024-IE-13060 de fecha 20 de mayo que corresponde al plan de sensibilización en seguridad de la información, dicha actividad se llevó a cabo de forma presencial en el Auditorio del Hemocentro el día 29 de mayo. Por último, se informa que se tiene contemplado la contratación de una persona para los temas de uso y apropiación que realizara entre otras cosas las capacitaciones necesarias a todos el personal de la entidad, no obstante, al entrevistar algunos de los colaboradores de entidad, específicamente de la subdirección de bienes y servicios, informan que no han recibido capacitación alguna, se procede a corroborar dicha afirmación, ya que existe un memorando que soporta la invitación a dicha dependencia. Adicionalmente, los referentes participantes, afirman literalmente: “que la Dirección TIC solo se limita a enviar

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

	el correo con un documento y creen que con eso ya con eso las personas se lo saben de memoria". De acuerdo a lo anterior, se deriva una oportunidad de mejora que busca dar continuar y reforzar las campañas de sensibilización a todo el personal utilizando diferentes mecanismos.

Numero de Hallazgo	**2**
Dependencia Auditada:	Dirección TIC
Dominio y Control	**Resultado de la Evaluación**
5.3 Roles organizacionales, responsabilidades y autoridades *La alta dirección debe asegurar que las responsabilidades y las autoridades para los roles pertinentes a la seguridad de la información son asignados y comunicados.*	Si bien es cierto, se cuenta con la matriz de roles y responsabilidades conformada por 9 roles: Líder de SI, director TIC, líderes de proceso, comité de institucional de gestión y desempeño, mesa técnica de gobierno y seguridad digital, gestores de SI por cada dependencia, partes interesadas, colaboradores, aliados, y proveedores, dichos roles y responsabilidades no han sido comunicados o divulgados y en tal medida los profesionales a cargo o designados, desconocen las responsabilidades que se tienen frente al sistema. De acuerdo a lo indicado, los gestores de seguridad en algunas áreas no funcionan y en otras áreas no se tienen. De acuerdo con lo anterior, se deriva una oportunidad de mejora toda vez que el control no es del todo eficiente, ya que la estructura jerárgica no está aplicada a todas las dependencias. Se sugiere que la matriz RACI se envié a la dirección de gestión del talento humano, para que hagan lo pertinente e informen a todo el personal designado.

Numero de Hallazgo	**3**
Dependencia Auditada:	Dirección TIC
Dominio y Control	**Resultado de la Evaluación**
5.3 Roles organizacionales, responsabilidades y autoridades *Literal b) informar a la alta dirección sobre el desempeño del SGSI.* *9.1 Seguimiento, medición, análisis y evaluación La organización debe evaluar el desempeño de la seguridad de la información y la efectividad del SGSI.*	La evaluación del estado de la seguridad de la información, se realiza a través del Comité Institucional de Gestión y Desempeño, el cual se realiza de forma trimestral. La Dirección TIC por su parte, reporta el estado de la seguridad a la Subsecretaria Corporativa mediante el formato codificado: SDS-PYC-FT-38 versión 2, en dicho formato se reporta el avance de las actividades desarrolladas de cara a la política de seguridad digital. Así mismo y con el fin de reportar el desempeño del sistema, se cuenta con un tablero de control que consta de 5 indicadores y las respectivas fichas de cada indicador. Adicionalmente, se cuenta con la presentación realizada al comité el día 11 de enero del 2024. Al consultar el resultado de cada indicador encontramos: • Indicador Nro1: Reporte de activos de información, dicho indicador reporta un 100% de cumplimiento, sin embargo, al constatar dicha información, encontramos que 3 dependencias no presentaron las matrices y por consiguiente no se puede reportar 100%. • Indicador Nro2: Correspondiente al plan de sensibilización, dicho indicador reporta cumplimiento al 100%, No obstante, resultado de algunas entrevistas a funcionarios informan que no se les ha hecho participes de las sensibilizaciones realizadas. En tal medida el plan no ha llegado a todos los colaboradores. En tal sentido, no se puede reportar 100% de cumplimiento.

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

	• indicador Nro3 - eventos de seguridad, se está reportando cumplimiento del 2%, ya que solo hubo 2 incidentes detectados, no obstante, al consultar la base de incidentes registrados mediante el aplicativo Aranda, evidenciamos más de 10 incidentes registrados con tipología de Phishing, los cuales han sido atendidos y solucionados. • indicador Nro4 – Verificación del control de acceso de dispositivos, consideramos que dicho indicador está mal formulado, ya que de acuerdo a lo indicado, se monitorean las redes Wifi conectadas, lo cual no aporta o mide el desempeño de la seguridad, por consiguiente desde la óptica del auditor dicho indicador debe ser replanteado. Así mismo, se ve la necesidad de definir nuevos indicadores de impacto que contengan umbrales o límites ya que en la actualidad no se tienen. De acuerdo a lo indicado por el referente, se está trabajando en este aspecto, toda vez que se está montando un diagnóstico completo de Seguridad de la información y mediante el contrato suscrito del SOC con el proveedor Gamma Ingenieros, se tiene contemplado la definición de nuevos indicados que soportaran la parte operativa. De acuerdo con lo anterior, se deriva una oportunidad de mejora, encaminada a reforzar el tablero de indicadores actual.

Numero de Hallazgo	**4**
Dependencia Auditada:	Dirección TIC
Dominio y Control	**Resultado de la Evaluación**
6.1.3 Tratamiento de riesgo de la seguridad de la información *Literal d) generar una Declaración de Aplicabilidad que contenga los controles necesarios [consultar 6.1.3 b) y c)], y además la justificación de inclusiones, sean estas implementadas o no y la justificación para exclusiones de controles de Anexo A;* *A9.2.5 - Revisión de los derechos de acceso de usuario*	Se suministra documento DECLARACION DE APLICABILIDAD-SOA actualizada año 2024 y al consultar dicho instrumento, evidenciamos que existen controles que se excluyen pero desde la óptica del auditor son necesarios y obligatorios en la operación. El referente informa que los Controles numerales A6.1.2 y A9.2.5 no se van a trabajar, ya que se van restructurar el proceso a partir del nuevo lineamiento de activos de información que pretende asignar la responsabilidad directa a los dueños de los activos en cada proceso. En lo que refiere al control A9.2.5 - Revisión de los derechos de acceso de usuario", de acuerdo a lo informado por el referente, actualmente no se está realizando. Dicho control busca realizar una revisión periódica de los permisos de accesos de los usuarios debido a la terminación del empleo o cambios en la organización, es una tarea constante que debe implementar la mesa de ayuda una vez es reportado el cambio por la dirección de Gestión de Talento Humano. Se informa que los aplicativos que están atados la AD- Directorio Activo, una vez se elimine el acceso desde el AD, se verá reflejado en todos los aplicativos. No obstante, en los aplicativos que no están ligados al AD, será responsabilidad de cada administrador o dueño de activo información, realizar la revisión periódica, depurar, actualizar o revocar permisos a los funcionarios. Toda vez que se convierte en una vulnerabilidad que puede ser aprovechada generando un posible acceso no autorizado. Dicho lo anterior, se deriva una oportunidad de mejora que permita fortalecer el control, ya que se está implementado de manera parcial. En resumen, el total de controles excluidos en el SOA es de 5 y se encuentran justificados y 109 controles se vienen implementando.

Numero de Hallazgo	**5**
Dependencia Auditada:	Dirección TIC
Dominio y Control	**Resultado de la Evaluación**
8.2 Valoración de riesgo de la seguridad de la información *La organización debe conservar la información documentada de los resultados de las evaluaciones de riesgo de la seguridad de la información.* *8.3 Tratamiento de riesgo de la seguridad de la información* *La organización debe conservar información documentada de los resultados del tratamiento del riesgo de la seguridad de la información.*	De acuerdo con lo verificado, existe un inventario de matrices de riesgos de seguridad de la información, que son el resultado de la solicitud realizada a principios del año 2024 y que es responsabilidad de la cada una de las dependencias remitir en los tiempos establecidos. Metodológicamente la Dirección TIC, tiene establecido que cada proceso debe diligenciar la matriz, así como el instrumento de autoevaluación con base en la guía establecida, dicha actividad es liderada por la Dirección TIC y al inicio de cada vigencia mediante memorando formal, se remite a todas las dependencias; sin embargo y de acuerdo a lo evidenciado, no todas las matrices fueron remitidas en los tiempos establecidos y fue necesario reiterar la solicitud para que las dependencias faltantes lo hicieran, no obstante, evidenciamos que trascurridos 6 meses de haber hecho la solicitud, aun no se tienen todas respuestas, lo cual corresponde a una debilidad del proceso. Nota: Las dependencias que a la fecha no han reportado o remitido los instrumentos son: Subdirección de Bienes y Servicios, Subsecretaria Corporativa, DAEPS, Laboratorio y Dirección de Servicio a la Ciudadanía. Segundo aspecto verificado: Al consultar algunas de las matrices remitidas, se observa que los riesgos son identificados, valorados y además se cuenta con el plan de tratamiento y el seguimiento respectivo mediante el instrumento de autoevaluación, no obstante, al comparar la valoración del riesgo residual de un año a otro, evidenciamos que la severidad del riesgo se mantiene, si bien es cierto, se gestiona el riesgo y se cuenta con elementos que respaldan dicho ejercicio, al comparar el registro de riesgo del 2024 con el registro del año 2023, identificamos que la severidad del riesgo se mantiene; si consideramos que los controles implementados han sido eficaces y suficientes y el instrumento de autoevaluación reporta que no hubo materialización del riesgo, esto conllevaría a que la severidad del riesgo residual pueda cambiar. Identificamos que la revaloración del riesgo no se hace. Tercer aspecto verificado: a lo largo del año 2024 y en el último mes, ha sido reiterativo las caídas por corte de fluido eléctrico que han afectado las estaciones de trabajo y demás dispositivos en el edificio administrativo como consecuencia de los múltiples cortes de energía del operador CODENSA en el sector sin previo aviso. En el mes de marzo y de acuerdo con el reporte presentado, hubo una caída de energía que afecto el datacenter contenedor y el servidor de HIPERCONVERGENCIA que agrupa varios de los servicios de la entidad, cabe señalar que el restablecimiento del servicio no fue inmediato y tomo en algunos casos varios días, así mismo se conoció un caso en donde los servicios no fueron restablecidos, ya que la información almacenada mediante backup no fue recuperada. Dicha situación expuesta, demuestra que los controles actuales no son eficaces y suficientes lo que conllevo a la materialización del riesgo y por consiguiente dicha situación deriva en una oportunidad de mejora en varios frentes.

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

Parte 2: Análisis con respecto al Anexo A o Norma ISO27002:2013

Numero de Hallazgo	**6**
Dependencia Auditada:	**Dirección de Gestión del Talento Humano**
Dominio y Control	**Resultado de la Evaluación**
A.7.1 Previo al empleo *A.7.1.1* *Selección*	Consiste en la verificación de los antecedentes de los candidatos al empleo y comprobar la veracidad de la información. De acuerdo a lo indicado por el referente, en talento humano se revisa el cumplimiento de requisitos, la idoneidad y experiencia para efectos de comprobación, se consulta el documento diligenciado en formato codificado SDS-THO FT-037 por medio del cual se hace la verificación de cumplimiento de requisitos para el empleo. Para el personal de carrera o planta, se recibe la hoja de vida y se solicitan los documentos aportados y se valida el cumplimiento de los requisitos. Una vez posesionado el funcionario, la dirección de talento humano, procede a realizar la verificación de documentos y valida con las instituciones educativas el ítem de formación. Se consulta el caso del funcionario posesionado: Edgar Alexander Prieto para el cargo de Director TIC. Se consulta el correo de fecha 23 de mayo del 2024 mediante la cual se hizo la solicitud a la Universidad Distrital. No obstante, al consultar la base de información que controla el seguimiento de los casos consultados y las respuestas obtenidas de las instituciones que se realizar por correo, evidenciamos que no en todos los casos se obtiene respuesta, ya que al realizar el filtro sobre la base, identificamos casos del año 2023, en los que a la fecha no se ha obtenido respuesta, lo cual, incumple con la revisión y comprobación de la veracidad de la información. Ahora bien, en lo que refiere a la carpeta documental que contiene toda la información del proceso con el funcionario, logramos comprobar que la carpeta en físico existe, sin embargo, en medio digital no, al particular se informa, que es una medida que se tiene pensada para el año 2025. De igual forma, se informa que en una eventual pérdida de la carpeta física, se procede a la consecución de la información por medio de los correos electrónicos que es donde reposa la información, no obstante desde la óptica del auditor resulta algo dispendioso, ya que la búsqueda puede tomar bastante tiempo y así mismo, no toda la información pudiera encontrarse. De acuerdo con lo anterior, se deriva una oportunidad de mejora que busca fortalecer este aspecto.

Numero de Hallazgo	**7**
Dependencia Auditada:	**Dirección de Gestión del Talento Humano**
Dominio y Control	**Resultado de la Evaluación**
A.7.1 Previo al empleo *A.7.1.2* *Términos y condiciones de la relación laboral*	El control nos pide que todos los empleados y contratistas con acceso a información sensible, deben firmar acuerdos de confidencialidad o de no divulgación antes de que tengan los permisos para acceder a dicha información, así mismo los empleados y contratistas, deben estar informados de sus responsabilidades y derechos legales tales como las relativas a la legislación de protección de datos. Al particular, se informa que existe el formato codificado SDS- THO- FT-166 en versión 2, que corresponde al documento de acuerdo de confidencialidad, no obstante, se logró comprobar que no en todos los casos aplica o se diligencia, ya que se argumenta que dicho formato solo aplica para los funcionarios que tienen acceso a información sensible, lo cual es un concepto errado desde la óptica del auditor, ya que todos los funcionarios independiente de su relación contractual, deben ser conscientes y responsables del manejo de la información que se tiene. Es clave indicar que a los funcionarios de planta, se les brinda el curso de inducción y reinducción y es aquí donde se les da a conocer la entidad, los diferentes procesos y las responsabilidades que tienen de aquí en adelante con la entidad. De acuerdo con lo anterior, se deriva una oportunidad de mejora que busca fortalecer este aspecto.

Numero de Hallazgo	**8**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control	**Resultado de la Evaluación**
A.8.1 Responsabilidad por los activos *A.8.1.1* *Inventario de activos*	Se trata de realizar un inventario de activos que permita identificar los activos de información que dan soporte al negocio, clasificarlos basado en su importancia e identificar el propietario del activo, dicha información debe ser revisada periódicamente y se debe garantizar su actualización ya que un activo puede ser eliminado o destruido y nuevos activos de información pueden ingresar. Al momento de verificar la información o inventario encontramos las siguientes situaciones: Se consulta la base de matrices de activos de información que son responsabilidad de cada proceso en la entidad., metodológicamente se tiene establecido que cada proceso tiene la responsabilidad de diligenciar la matriz con base en la guía establecida una vez se hace la solicitud formal mediante memorando a principio de año, dicha solicitud es realizada por la dirección TIC a principio del año y se remite a todas las dependencias, sin embargo y de acuerdo a lo evidenciado, no todas las matrices son remitidas en los tiempos establecidos y es necesario reiterar la solicitud para que las dependencias faltantes lo hagan, no obstante, trascurridos 6 meses del año de haber hecho la solicitud, aun no se tienen todas respuestas, lo cual corresponde a una debilidad de dicho control y amerita un plan de mejora. La matriz de activos de información es dinámica en el tiempo y es responsabilidad de los dependencias y dueños de procesos mantenerla actualizada, en tal sentido, se debe verificar periódicamente ya que algunos de los activos de información

	pueden ser eliminados o destruidos o pueden ingresar nuevos activos de información y esto no se aplicando en todos los casos. De acuerdo con lo anterior, se deriva una oportunidad de mejora que busca fortalecer en ese aspecto. Vale la pena mencionar, que la Dirección TIC en conjunto con la Dirección de Planeación Institucional y Calidad, adelantan la modificación de la práctica, basado en un nuevo lineamiento, que permita definir roles y responsabilidades claras, ya que en la actualidad se cree que la Dirección TIC, es la única responsable de la actualización del inventario de activos de información lo cual es un error. Como reflexión, se considera que si no existe un responsables directo, no hay un control y eso es lo está ocurriendo en la actualidad con el inventario. Otro hecho a resaltar, es que al consultar el inventario de activos de información propio de la Dirección TIC, evidenciamos que dicho inventario no tuvo en cuenta los elementos que componen la infraestructura de TI y que para el caso la Dirección TIC es responsable y custodio de por ejemplo, routers, switches, firewall, elementos del datacenter conteiner, entre otros, en tal medida la matriz se encuentra desactualizada. De acuerdo con lo anterior, se deriva una oportunidad de mejora que busca fortalecer en ese aspecto.
Numero de Hallazgo	**9**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control A.9 Control de acceso A.9.4.3 Sistema de gestión de contraseñas	**Resultado de la Evaluación** Se informa que la gestión de contraseñas se hace mediante el directorio activo, una vez se crea el usuario nuevo y se solicita la creación de contraseñas, se sincroniza con el directorio activo. A partir del documento de políticas específicas, SDS-TIC-LN-001 version1, en el numeral 6.6.9, establece la gestión de acceso a los usuarios y en los numerales 8 y 9 se define la regla del mínimo de numero de caracteres y las características que debe tener las contraseñas, en la práctica, los administradores de servidores y demás dispositivos, cuenta con los usuarios y contraseñas respectivos, sin embargo, la centralización de las contraseñas o gestión de usuarios de las plataformas y dispositivos se desconoce, lo cual es una debilidad existente, ya que la información de cuentas y contraseñas se encuentra relacionado mediante correos electrónicos y en una eventualidad que los administradores ya no se encuentren en la entidad, se verían afectados los servicios. Dado lo anterior, es necesario fortalecer este aspecto mediante la implementación de software gratuito para la Gestión de Contraseñas.

Numero de Hallazgo	**10**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control	**Resultado de la Evaluación**
A.10 Criptografía *A.10.1.1* *Política sobre el uso de controles criptográficos*	Al consultar el manual de políticas específicas codificado SDS-TIC-POL-001, en el numeral 6.13, se establece la política específica de uso de controles criptográficos que la componen 10 numerales, sin embargo, en la práctica encontramos que los numerales 3 y 5 correspondientes al cifrado de Discos Duros y el cifrando mediante contraseñas de diferentes documentos elaborados por las dependencias) no se están aplicado. Se informa por parte del referente, que tiene proyectado enviar un correo masivo a todos los colaboradores de la entidad para que se aplique el cifrado en los documentos que manejan información sensible o manejan cierta reserva. Se propone hacer concientización a nivel institucional para implementar la buena práctica. Dado lo anterior, se deriva una oportunidad de mejora, que permita generar o elaborar piezas comunicativas para concientizar a los colaboradores de la entidad sobre el riesgo latente en la privacidad de la información y enfocada a la protección de la información en el caso de que un intruso puede tener acceso a la misma y se impone establecer un sistema de cifrado para dificultar la violación de la confidencialidad o su integridad. Adicionalmente, se logra comprobar mediante observación, que los servidores de la entidad cuentan con certificados SSL que cifran la información mediante el algoritmo SHA-256, como evidencia se consulta el certificado Digital del sitio WEB PAI el cual utiliza control criptográfico del proveedor DIGICERT.

Numero de Hallazgo	**11**
Dependencia Auditada:	**Subdirección de Bienes y Servicios**
Dominio y Control	**Resultado de la Evaluación**
A.11 Seguridad física y del ambiente *A.11.1.1* *Perímetro de seguridad física* *A.11.1.2* *Controles de acceso físico* *A.11.1.3* *Seguridad de oficinas, salas e instalaciones*	Con el fin de brindar la seguridad física de los activos, bienes y personas la Subdirección de Bienes y Servicios, se cuenta con un contrato suscrito y en curso. Con respecto a los controles biométricos de cara a la seguridad perimetral, identificamos que para acceder a cada una de las dependencias se cuenta con tarjetas de acceso y control dactilar, adicionalmente se cuenta con múltiples cámaras de seguridad hacia la calle y zonas verdes. En el caso de que se detecte un intruso mediante las cámaras en el centro de control y vigilancia se genera la alarma y se llama a la policía, dichas cámaras monitorean las 24 horas del día. Cabe señalar que para lo que lleva el año 2024, no se han reportado casos de intrusos y se cuenta con controles de acceso físico por medio de stickers que permiten controlar el acceso de personal visitante en la entidad, apoyado por el sistema TIS – Total integration System, en el entendido que las visitantes si y solo si deben dirigirse al área solicitada y no a otra, es por eso que se cuenta con un segundo y tercer filtro con personal de seguridad al ingreso de cada edificio y en cada planta se verifica y constata la acceso. En lo que respecta al control de acceso físico del personal de planta y contratistas, se tiene controlado por torniquete y registro en el sistema BIOSTAR, claramente se tienen identificadas las áreas restringidas en la entidad como son: el datacenter conteiner, gabinete de rack de comunicaciones, laboratorios, almacén de medicamentos, almacén general, archivo central, seguridad y control, entre otras, no obstante, al

realizar la prueba simulada de acceso físico a estas áreas, se comprueba que el control físico no es del todo eficiente, ya que el auditor logro ingresar el día 13 de septiembre mediante tarjeta de acceso (Carnet) y huella a estas áreas, lo cual demuestra que el control mediante tarjetas y huella debe ser restringido por áreas o segmentación de funciones. Dado lo anterior, se considera un primer aspecto a mejorar.

Con respecto al archivo central, y como recomendación de la OCI, se ve necesario implementar controles biométricos mediante tarjeta y huella, ya que el acceso es abierto y pudiera comprometerse la información sensible que reposa allí. Evidenciamos que el control de vigilancia que se encuentra junto a esta área no fue eficaz ya que el día 13 de septiembre el auditor pudo ingresar con facilidad.

Otro aspecto evidenciado y delicado, fue que el mismo día 13 de septiembre, mediante técnica de ingeniería social que pretende engañar la mente humana, se logró sacar un equipo portátil del piso 6 hasta la portería de la Carrera 33, evidencia que reposa en las cámaras de vigilancia en el intervalo de horario de 9 am a 11 am, dicha prueba permitió demostrar que el control y los diferentes filtros como fue el caso de paso al parqueadero de visitantes, fue vulnerado. Dicho lo anterior, se deriva una oportunidad de mejora.

Al consultar el informe de visitas TIS del día 6 de septiembre 2024, encontramos que existe un registro de visitante que cuenta con fecha y hora de entrada, pero no de salida, lo cual genera inquietud. El registro corresponde al número de cedula: 52.801.046 ingreso a las 5:27pm, existen doble ingreso el mismo día, pero se desconoce la hora de salida, lo que da entender que la persona no entrego el sticker o no se descargó en el sistema por parte del personal de vigilancia. La recomendación de la OCI, apunta a que el control se cumpla de principio a fin, garantizando la captura de los datos de fecha y hora de salida de todos los visitantes.

Respecto al personal externo que va a realizar un trabajo, la recomendación de la OCI apunta a que dicho personal debe ir acompañado por personal de la SDS que autoriza y se debe asegurar que el acceso a otras dependencias sea restringido, es clave indicar que el acompañamiento de las personas que realizan el mantenimiento, se realiza al momento del ingreso pero en el desarrollo de las actividades, el personal externo trabaja de manera independiente, es decir no es posible hacer un acompañamiento 100% de la actividad. Al particular se cuenta con el instructivo codificado SDS-BYS-INS-057 para el mantenimiento y obra civil. En lo que refiere al acceso biométrico, la mayoría de las áreas utilizan tarjeta de proximidad y dactilar; pero solo el área del IDCBIS tiene acceso por reconocimiento facial.
Respecto al control de acceso vehicular, este se realiza por medio de las talanqueras con control de acceso biométrico por tarjeta de acceso (carnet) o dactilar. No obstante, al poner a prueba el control, ha sucedido que ingresan 2 o 3 personas en el mismo vehículo y por descuido del personal de vigilancia, no se verifica y el personal “no autorizado” ingresa. Dicha situación, pone en riesgo las áreas que manejan información sensible en la entidad, toda vez que el control se vulnero mediante ingeniera social. De acuerdo a lo anterior, se deriva una oportunidad de mejora, que permita ajustar los protocolos y lineamientos de seguridad al ingreso y salida de la entidad.

Numero de Hallazgo	12
Dependencia Auditada:	**Dirección TIC**
Dominio y Control	**Resultado de la Evaluación**
A.11 Seguridad física y del ambiente *A.11.2.8* *Equipo de usuario desatendido*	Dicho control establece que los usuarios no deben dejar las sesiones abiertas mientras el equipo no este atendido. Además de los procedimientos de bloqueo de pantalla y las sesiones de aplicación y red debe cerrarse cuando las conexiones no se utilizan. Mediante el documento de políticas específicas denominado: SDS-TIC-POL-001 versión 11, en los numeral 6.14, establece las reglas para el manejo de equipos desatendidos y establece que las sesión Windows en cualquier estación de trabajo será bloqueada de manera automática cuando existe inactividad por más de 5 minutos, dicha política se encuentra implementada en toda la entidad. En lo que respecta a servidores Windows y Linux antes de la puesta en el ambiente de producción, se realiza hardening o endurecimiento de la configuración. Pedagógicamente y a nivel institucional se adelantó una campaña, que busca crear conciencia sobre tema de escritorios limpios, manejo de contraseñas seguras y bloqueo automático de sesiones. Para efectos de comprobación, se constata la eficacia del control, ya que una vez trascurridos los 5 minutos de inactividad, la sesión Windows en la estación del trabajo del ingeniero Erlington se bloqueó. La OCI recomienda, elaborar piezas graficas que busca crear conciencia sobre el riesgo al que están expuestos los usuarios por la ausencia del puesto de trabajo y el no bloqueo de la sesión. Así mismo, se busca que los usuarios realicen el bloqueo manual mediante la combinación de las teclas Windows + L, ya que en el lapso de 5 minutos pudiera un intruso acceder y ocasionar un incidente Digital. De acuerdo lo anterior, se deriva una oportunidad de mejora que permita fortalecer estos aspectos.

Numero de Hallazgo	**13**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control	**Resultado de la Evaluación**
A.12.1 Procedimientos operacionales y responsabilidades *A.12.1.3* *Gestión de la capacidad*	Mediante este control, se busca evitar pérdidas de disponibilidad o rendimiento de los sistemas, en sentido es necesario realizar mediciones y seguimiento del uso de los recursos y planificar las ampliaciones de capacidad de los recursos que estén limitados. Al particular, se informa que se cuenta con un catálogo que permite gestionan la capacidad de los servicios e infraestructuras. Se informa que en la actualidad siguen habiendo problemas de infraestructura. En lo que respecta al PIVOT o servidor de Hiperconvergencia, se informa que se está trabajando con nueva infraestructura. En lo que respecta al Datacenter conteiner, se cuenta con un software que permite conocer las capacidades en: UPS, energía, temperatura, aire acondicionado, entre otras y se gestiona mediante alertas y se notifica o escala a los responsables. Actualmente se monitorean los canales de datos hacia internet con la herramienta dispuestas por el proveedor y se genera informe de la seguridad perimetral que presenta el SOC y análisis del tráfico de red. No obstante, al consultar el estado de las variables como: memoria, CPU e interfaces de red de los equipos de cómputo y servidores,

	evidenciamos que dichas variables no están siendo gestionadas y monitoreadas mediante protocolo SNMP, situación que pone en riesgo la disponibilidad de los servicios, ya que pueden ocurrir incidentes por caída de los servicios. DE acuerdo a lo anterior, se deriva una oportunidad de mejora o iniciativa que busca monitorear los servidores y con ellos garantizar las capacidades.
Numero de Hallazgo	**14**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control *A.12.3 Respaldo* *A.12.3.1* *Respaldo de la información*	**Resultado de la Evaluación** Control que busca generar copias de respaldo y pruebas de la información respaldada con cierta periodicidad de acuerdo con la política establecida. Se informa que en la actualidad se opera bajo el procedimiento antiguo de generación de backup mediante la solución ARCbackup la cual ya no tiene soporte y se está trabajando en un nuevo procedimiento que involucra un nuevo aplicativo denominado VEAM Backup. Procedimiento bajo la estándar de NIST y define todo el esquema de respaldos. El clave mencionar que toda la información de las estaciones de trabajo no se encuentra ya que la capacidad de almacenamiento es limitada, es por eso que mediante las políticas de seguridad de la información, se establece que todo usuario debe hacer la solicitud mediante formato a la Dirección TIC para proceder a respaldar la información. En la actualidad se siguen generando backups con el software ARCbackup y VEAM backups, dicho software cuenta con licenciamiento activo. En el caso de BEANbackup, se están realizando Fullbackups de todos los servidores que están en onpremise o en el datacenter Conteiner. Se informa que hubo inconvenientes a nivel de almacenamiento, por demoras en la consecución de cintas y en tal medida fue necesario la reutilización de cintas. De acuerdo a lo indicado, mediante el nuevo lineamiento se van a tener backups sobre la infraestructura específica y para eso se cuenta con un nuevo proceso de contratación que soporte el almacenamiento, se busca que el nuevo esquema supla las deficiencias actuales. Por último, resultado de los incidentes reiterativos producto de la caída del fluido eléctrico en el mes de marzo 2024, se vieron afectados múltiples servicios del PIVOT 3 o servidor de Hiperconvergencia que se concentran más de 100 servicios, de acuerdo al informe final, el restablecimiento de los servicios fue gradual y en algunos de los casos volver a la normalidad tomo varias horas e incluso varios días. El auditado acepta que hubo 2 sistemas de información que no pudieron recuperarse y otros donde hubo pérdida de información de 1 día. Específicamente a lo que refiere al ERP – SI-Capital, en este se logró recuperar toda la información. La dirección de Asuntos disciplinarios por su parte, informa que debido al incidente ocurrido, presentaron perdida de información que se encontraba alojada en la carpeta de one-drive. Otro aspecto que no está siendo cubierto, es la verificación de la integridad de los backup y la realización de pruebas de recuperación para garantizar la información se mantiene. De acuerdo con la anterior, el control no es del todo eficiente y por consiguiente se deriva una oportunidad de mejora.

Numero de Hallazgo	**15**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control	**Resultado de la Evaluación**
A.12.6 Gestión de la vulnerabilidad técnica ***A.12.6.1 Gestión de las vulnerabilidades técnicas***	El control busca obtener información acerca de las vulnerabilidades técnicas detectadas de los sistemas de información y tomar las medidas apropiadas (remediaciones) para abordar el riesgo asociado. Al particular, se cuenta con un lineamiento para el desarrollo de pruebas de vulnerabilidades técnicas y actualmente con el contrato del SOC suscrito, se tiene contemplado la realización de análisis de vulnerabilidades para 100 IPs y a la fecha se ha ejecutado en 4 sistemas diferentes: 1. SALUDATA. Encuestas del SDS, LAVANTAGE y pagina WEB. De otra parte, se está a la espera de la entrega del informe final de 36 dispositivos analizados. Evidenciamos análisis de vulnerabilidades en dispositivos como: Switches, Routers, firewalls, entre otros dispositivos, que no se están cubriendo, lo cual implica un riesgo alto, ya que estas vulnerabilidades puedes ser explotadas por un atacante. Por último, evidenciamos que aplicaciones WEB que son liberadas por parte del grupo de QA mediante el concepto técnico emitido y que deben pasar al ambiente de producción, no hacen parte del plan de trabajo del grupo de seguridad, esto con el fin de aplicar las correspondientes pruebas de análisis de vulnerabilidades sobre sitios WEB. De acuerdo con las buenas prácticas de seguridad, previo al paso a producción de los diferentes aplicativos, estos deben pasar por el proceso de análisis de vulnerabilidades mitigando posibles riesgos. De acuerdo con lo indicado, por grupo de desarrollo de software, se cuenta con un catálogo de aplicativos, que será el insumo a utilizar por parte del grupo de Seguridad, a fin de que realice la programación de los nuevos análisis de vulnerabilidades sobre los aplicativos que están a puertas del paso a producción. De acuerdo con lo anterior, se deriva una oportunidad de mejora que permitirá fortalecer esta práctica contemplado todos los elementos.

Numero de Hallazgo	**16**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control	**Resultado de la Evaluación**
A.14.2 Seguridad en procesos de desarrollo y soporte *A.14.2.1 Política de desarrollo seguro*	La política consiste en aplicar buenas prácticas de seguridad a lo largo del ciclo de vida de desarrollo de software con la finalidad de prevenir posibles vulnerabilidades y disminuir posibles ataques. Se cuenta con el documento denominado: SDS-TIC-POL-001 y mediante el numeral 6.7.3, se define la seguridad en el desarrollo de sistemas de información y dicho componente hace el llamado al procedimiento de soluciones de software SDS-TIC-PR-001. Así mismo, al consultar en la base documental de isolucion, encontramos el documento denominada: SDS_TIC_GUI-010 v1, Guía para el análisis y diseño de sistemas, dicha guía es diligenciada por cada uno de los desarrolladores y al final de cada proyecto de software, se entrega el documento final que debe contemplar los aspectos de seguridad de la información establecidos en el numeral 9.2. Como segundo aspecto, se cuenta con el manual de política de seguridad de la información y en el numeral 5.1, se define la política específica para el desarrollo seguro, por parte del auditado se informa, que el control de código fuente se realiza mediante el aplicativo DEVOPS, se cuenta con separación de ambientes

	para el desarrollo y manejo de control de versiones del software. Se informa además que, para los diferentes frentes de desarrollo, se utiliza la misma herramienta DEVOPS y todos los proyectos de software finalizados, cuentan con toda documentación y el código fuente alojado en la nube de Azure de Microsoft. En lo que respeta a la fábrica de software proveedor que apoyo el ejercicio de desarrollo de software hasta 31 de diciembre del año 2023, logramos constatar mediante el documento compartido la metodología definida para el desarrollo seguro, Por último, se consulta el lineamiento SDS-TIC-LN-016 versión 1 orientado al desarrollo seguro en la SDS y define los siguientes criterios: Arquitectura que empleara la aplicación, Plataforma donde correrá la aplicación, tipos de datos, Tipos de registros, privilegios de acceso a recursos, perfiles de usuario y modo de autenticación. No obstante, al consultar el catálogo de aplicativos, se evidencia que existen aplicativos nuevos y antiguos en el ambiente de producción que utilizan URL o dominios WEB no seguros, ya que utilizan protocolo HTTP o puerto TCP 80, 8080, lo cual se considera una debilidad importante, ya que un atacante pudiera aprovecharse de esta vulnerabilidad, acceder de forma no autorizada y comprometer la información. Para efectos de comprobación, se relacionan algunas URL o sitios web que presentan esta vulnerabilidad: http://appa.saludcapital.gov.co/GestionPruebas/, http://sdsdlf01.saludcapital.gov.co:10000/edelphynbb/login.jsp, http://fappd.saludcapital.gov.co/crue/ - SIDCRUE De acuerdo con lo anterior, la política está cumpliendo de manera parcial y por consiguiente se deriva una oportunidad de mejora que permitirá fortalecer esta mala práctica.

Numero de Hallazgo	**17**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control A.16 Gestión de incidentes de seguridad de la información A.16.1.5 Respuesta ante incidentes de seguridad de la información	**Resultado de la Evaluación** Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados, dicho procedimiento debe permitir controlar el proceso de resolución, mantenga registros de los incidentes y evidencias, se deben registrar en detalle las acciones llevadas a cabo y los resultados de las mismas y por último, debe permitir realizar análisis y determinar causas raíz. Al particular, se informa que los incidentes de seguridad, son tratados mediante el procedimiento actual codificado, SDS-TIC-PR-002 GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC, sin embargo, al consultar dicho procedimiento, no especifica o documenta el manejo de los incidentes de seguridad que actualmente son gestionados y tratados por el grupo del SOC. De acuerdo con lo informado por el auditado y los diferentes representantes invitados a la mesa de trabajo, se informa que una vez se identifica un caso o incidente de seguridad, se procede a escalarlo al grupo de especialistas del SOC, dichos casos son registrados, categorizados y se determina si requiere apoyo adicional para la resolución. Al consultar la herramienta Aranda, encontramos que existe una categoría denominada: Incidentes de SI, al consultar la base de incidentes registrados, identificamos 10 registros de tipo “Phishing”, que han sido resueltos a la fecha. No obstante, en la mesa de trabajo se presenta el documento en construcción y borrador que

	documenta y formaliza el procedimiento para el manejo de incidentes de seguridad bajo el estándar del NIST. De acuerdo a lo anterior, el control se está aplicado de manera parcial, lo cual deriva una oportunidad de mejora que permita documentar, formalizar, divulgar el procedimiento para manejo de incidentes de Seguridad, dicho procedimiento deberá contemplar el flujo de la etapa investigativa, análisis de causa raíz y análisis forense.
Numero de Hallazgo	**18**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control	**Resultado de la Evaluación**
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio *Seguridad de la información durante la interrupción* *A.17.1.1 Planificación de la continuidad de la seguridad de la información*	Se trata de implementar medidas de protección y de recuperación ante posibles desastres para minimizar los daños y facilitar el restablecimiento de las operaciones. Los planes de contingencia, establecen las respuestas o tratamientos de los incidencias, y debe dar respuesta ante una situación de crisis o parada de los distintos servicios críticos de la entidad como es el caso de: energía, comunicaciones, red, infraestructura, entre otro. Sin embargo, al consultar el repositorio documental que nos provee el auditado encontramos los siguientes documentos en borrador o construcción: 1. IRBC análisis de impacto.pdf 2. BIA_Reporte de valores iniciales RTO-RTO_Dic2022.pdf para el proceso de Gestión financiera, 3. Dic_PRD-DRP.pdf presentación a los especialistas del centro de cómputo. 4. 3.2.2_jun_SDS_Plan de recuperación de desastres v.0-1-2_2022.pdf. Dicho documento al consultar, se observa que se encuentra desactualizado, ya que los pasos y el detalle respecto a la forma de proceder en cada uno de los servicios, no se describe con claridad, los documentos DRP no han sido formalizados y aprobados, lo que pone en riesgo la disponibilidad de los servicios e impide demostrar la eficacia del plan. Si bien es cierto existe un documento borrador DRP, es importante precisar que no cuenta o describe los pasos a seguir, no cuenta con directorio de responsables y líneas de contacto. Dicho documento que se encuentra en borrador desde el año 2023. Es decir, no hubo grandes avances al momento de la presente auditoria y los documentos principales y anexos se encuentran en desarrollo. Dicho lo anterior y en vista que es un tema que reincide bajo la acción 2871 de la auditoria año 2023 y que aún sigue abierta, se decreta una no conformidad.

Numero de Hallazgo	**19**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio A.17.1.2 Seguridad de la información durante la interrupción *Implementación de la continuidad de la seguridad de la información*	**Resultado de la Evaluación** El plan de respuesta debe contener: 1. Designación de los responsables, responsabilidades y niveles de competencia frente a la recuperación de los sistemas y 2. Documentación y procedimientos: Como se va a gestionar un evento crítico y como se va a mantener la Seguridad de la información a un nivel mínimo. El documento DRP y los procedimientos que hace el llamado al DRP de acuerdo a lo indicado se encuentran en desarrollo. El año pasado en la auditoria, se informó que la implementación del DRP, se tenía proyectada para el primer trimestres del 2023, sin embargo para la presenta evaluación, no se presentaron o compartieron avances al respecto. En conclusión, implementación de DRP y plan de pruebas y resultados no se presentaron, Dicho lo anterior y en vista que es un tema que reincide bajo la acción 2871 de la auditoria año 2023 y que aún sigue abierta, por lo que se decreta una no conformidad.

Numero de Hallazgo	**20**
Dependencia Auditada:	**Dirección TIC**
Dominio y Control A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio Seguridad de la información durante la interrupción A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**Resultado de la Evaluación** La revisión permite que un sistema se mantenga vivo en el tiempo. 1. Nuevos activos de Información no se queden fuera del plan. 2. Revisar la implicación del personal en las tareas de recuperación verificando que todo el mundo esté al tanto de sus responsabilidades. Respecto a lo anterior, no se evidencia actualización del plan basado en los nuevos activos vinculados en las operaciones y servicios de la entidad y al no contar con resultados de la prueba planificada, no es posible determinar la eficacia del plan y lecciones aprendidas para el mejoramiento, Dicho lo anterior y en vista que es un tema que reincide bajo la acción 2871 de la auditoria año 2023 y que aún sigue abierta, se decreta una no conformidad.

Numero de Hallazgo	**21**
Dependencia Auditada:	**Dirección TIC/ Oficina de Asuntos Jurídicos**
Dominio y Control A.18 Cumplimiento A.18.1.1 *Requisitos Legales, estatutarios, reglamentarios y contractuales* *Identificación de la legislación vigente y los requisitos contractuales*	**Resultado de la Evaluación** Es clave señalar que los requisitos pueden venir en forma de leyes, requisitos de seguridad, derechos de propiedad intelectual, leyes de derechos de autor, leyes de protección entre otras, sin embargo, al consultar el normograma propio del proceso de Gestión TIC, no identificamos registros de legislación y normatividad aplicable como son: • Ley 23 sobre derechos de autor • Decreto 1360 de 1989 y decreto 1474 de 2002 sobre propiedad intelectual • Decreto 1747 de 2000 reglamenta certificados y las firmas digitales • Ley 1221 de 2008 regla el teletrabajo • Ley 1581 de 2012 protección de datos personales • Decreto 338 del 2022, lineamiento para fortalecer la gobernanza de la seguridad digital. • Norma técnica ISO/IEC 27001:2013

En lo que respecta a la evaluación realizada a la oficina de asuntos jurídicos, se informa que dicha oficina aplica lo correspondiente a la normatividad con enfoque a salud y en caso darse un nuevo decreto en salud, la oficina Jurídica procede a determinar las implicaciones que conllevan en salud y generar un pronunciamiento al respecto. En lo que respecta a la regulación que emite el ministerio de las TIC, la oficina jurídica informa que si se necesita un concepto de cómo va afectar la nueva legislación a la entidad, se pude emitir con concepto jurídico de ser requerido y cada proceso es responsable de su ámbito normativo y legal.

Respecto a lo anterior, la dirección TIC se debe mantener documentado y actualizado todos los requisitos legales y contractuales que afecten a la entidad, dicho lo anterior, el punto está cumpliendo de manera parcial y en consecuencia se deriva en una oportunidad de mejora.

Nota: El presente informe contiene la síntesis de todo el ejercicio realizado y es importante resaltar que la auditoría, implicó la revisión y evaluación de cada uno de los aspectos trazados en el cronograma establecido, las evidencias y soportes suministrados fueron cotejaron con varios de los activos de información pertenecientes a los diferentes procesos del alcance.

7. ASPECTOS POSITIVOS (NIA 2410 A2).

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

- De acuerdo con plan de mantenimiento preventivos y correctivos establecidos con los proveedores de tecnología bajo los contratos suscritos, se vienen adelantado la detección de debilidades, errores, omisiones o fallos de seguridad en los sistemas y dispositivos que pueden ser objeto de posibles ataques y se vienen subsanando.

- Con el propósito de realizar monitoreo constante de las amenazas que afectan la seguridad y lograr centralizar o consolidar toda la información de las diferentes fuentes, analizarla, correlacionarla y dar respuesta ante un ciberataque, la entidad cuenta con un contrato suscrito con Gamma Ingenieros que permite dar soporte y respuesta a los servicios del SOC entre ellos la implementación del sistema SIEM que hace parte de la arquitectura de seguridad.

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

- El recurso humano conoce las entradas y las salidas de cada uno de los procedimientos evaluados y determina de forma preventiva los recursos físicos y

tecnológicos que son necesarios para la operación de la seguridad de la información.

- 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.

8. NO CONFORMIDADES. (NIA 2431).

Pese a que en el año 2023 se adelantaron varios documentos borrador de cara a la continuidad de negocio, como es el caso del DRP, BIA, plan de prueba, preparación de prueba simulada, evidenciamos que a la fecha de la presente auditoria los documentos señalados siguen en versión borrador, sin aprobación, publicación e implementación, al consultar el documento Plan de recuperación de desastres v.0-1-2_2022.pdf, no describe los pasos a seguir para cada uno de los servicios críticos afectados, no se cuenta con directorio de responsables, líneas de contacto, escalamiento y los otros documentos señalados presentan el mismo comportamiento, así mismo se pudo constatar que un año después no hubo avances al respecto, tema que reincide bajo la acción 2871 de la auditoria año 2023 y que aún sigue abierta, en consecuencia, existe un riesgo de cara la indisponibilidad de los servicios y se decreta un incumplimiento de los numerales: A17.1.1, A17.1.2 y A17.1.3 de la norma ISO27002, por lo que hace necesario e indispensable tomar las acciones correctivas del caso.
Responsable: Dirección TIC

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

9.1. Pese a que ha se vienen convocando y realizando jornadas de sensibilización y divulgación con los diferentes gestores de seguridad y a grupos de funcionarios en la entidad, evidenciamos que la responsabilidad especifica de retroalimentar y multiplicar el conocimiento adquirido a los colaboradores sobre los contenidos impartidos, no está llegando a todos los colaboradores, ya al entrevistar algunas de las personas informan que no han recibido ningún tipo de capacitación o sensibilización, en consecuencia, existe una debilidad en cuanto al desconocimiento de los colaboradores frente a los temas de seguridad de la información y controles de seguridad que deben ser aplicados por cada uno de los colaboradores, por lo anterior, se hace necesario implementar las mejoras que haya lugar para dar cumplimiento en su totalidad los numerales 5.1 literal d), 5.2 literal f) y 5.3 literal b) de la norma ISO27001
Responsable: Dirección TIC, Oficina Asesora de Comunicaciones

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

9.2. Si bien es cierto, se cuenta con la matriz de roles y responsabilidades – RACI y a su vez con una estructura jerárquica de seguridad de la información establecida para la entidad, se evidencia que dichos roles no han sido comunicados o divulgados, ya que los colaboradores que ejercen dichos roles en la entidad, desconocen las responsabilidades que tienen frente al sistema, en consecuencia, existe una debilidad que no permitirá el logro de los objetivos de previstos del modelo de seguridad, por lo anterior, se hace necesario implementar las mejoras que haya lugar para dar cumplimiento en su totalidad del numeral 5.3 de la norma ISO27001.
Responsable: Dirección TIC

9.3. Aun cuando existe un grupo de matrices de activos de información que son responsabilidad de cada proceso en la entidad, evidenciamos, que no todas las matrices son remitidas en los tiempos establecidos y no son actualizadas a voluntad propia por cada proceso, ya que nuevos activos ingresan y otros se eliminan, dicha situación no se ve reflejada, adicionalmente el auditor procede a verificar la matriz de la dirección TIC y encuentra que varios de los activos de información que hacen parte de la infraestructura de TI no han sido inventariados, en consecuencia, existe una debilidad, una mala práctica en lo correspondiente a la gestión de activos y se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad al numeral 8.1.1 de la norma ISO27001
Responsable: Dirección TIC

9.4. Si bien es cierto, el estado y desempeño de la seguridad de la información cuenta con un instrumento o tablero de control de indicadores y los resultados son dados a conocer en diferentes instancias con cierta periodicidad, evidenciamos que los indicadores 1, 2 y 3 están reportando un cumplimiento mayor al real o verificado y os indicador 3 y 4 se encuentran mal formulados, adicionalmente se ve la necesidad de definir nuevos indicadores de impacto que establezcan umbrales o límites, ya que en la actualidad no se tienen, por lo anterior, existe una debilidad y se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad de los numerales 5.3 literal b) y 9.1 de la norma ISO27001
Responsable: Dirección TIC

9.5. Aun cuando existe un grupo de matrices de gestión riesgos de seguridad de la información e instrumentos de autoevaluación que son responsabilidad de cada proceso en la entidad, evidenciamos, que no todas las matrices son remitidas en los tiempos establecidos y ha sido necesario reiterar la solicitud a los procesos faltantes y transcurridos 6 meses de haber hecho la solicitud, aun se sigue sin obtener la totalidad de las respuestas, 2. Por directriz interna la gestión de riesgos se hace una vez al año, no obstante, algunos de los riesgos se han materializado ya que los controles no han sido del todo eficaces y suficientes, en consecuencia, existe una debilidad, una mala práctica en la gestión de riesgos y se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad de los numeral 6.1.2, 8.2 y 8.3 de la norma ISO27001
Responsable: Dirección TIC

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

9.6. Si bien es cierto, existe la política específica de uso de controles criptográficos en el documento denominado: SDS-TIC-POL-001 versión 11 en su numeral 6.13 y la conforman 10 numerales, evidenciamos que el numeral correspondiente al cifrado de documentos mediante contraseñas, no se está implementando en la entidad, por lo anterior, existe un riesgo frente a la pedida de confidencialidad y se hace necesario implementar las mejoras que haya lugar para dar cumplimiento en su totalidad con el control número A.10.1.1 de la norma ISO27001.
Responsable: Dirección TIC

9.7. Pese a que los controles físicos de ingreso y salida del edificio de la SDS están soportados por personal de vigilancia, torniquetes y cámaras de vigilancia, evidenciamos que dichos controles presentan una debilidad importante, toda vez que al realizar pruebas simuladas de acceso físico mediante tarjeta de proximidad (Carnet) o huella dactilar en áreas como: Almacén de medicamentos, Almacén General, Seguridad y Control, permitió el acceso autorizado al auditor, así mismo, mediante técnica de ingeniería social, el día 13 de septiembre, se logró vulnerar los controles existentes, ya que permitió retirar un equipo portátil de la entidad sin ningún tipo de verificación, evidencias que reposan en las cámaras de vigilancia, en consecuencia, existe un potencial riesgo frente a la perdida de información o posible fuga de información sensible de la entidad, lo que hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad con los requisitos A.11.1.1, A.11.1.2 y A.11.1.3 de la norma ISO27001.
Responsable: Subdirección de Bienes y Servicios.

9.8. Aun cuando el proceso de gestión del talento humano, realiza la verificación del cumplimiento de los requisitos para el empleo del personal de planta o carrera y comprueba la veracidad de la información suministrada, como es el caso de los antecedentes, formación, experiencia e idoneidad, dicho ejercicio es soportado mediante el formato codificado SDS-THO FT-037 y una vez posesionado el funcionario, se procede a realizar la verificación de los documentos con las instituciones educativas en el ítem de formación, para ello la dirección de talento humano utiliza una base de información en formato Excel, que controla el seguimiento a los casos consultados y las respuestas obtenidas de las instituciones, no obstante, se evidencia casos del año 2023, que a la fecha no se ha obtenido respuesta, lo cual, incumple con la revisión y comprobación de la veracidad de la información. Ahora bien, en lo que refiere a la carpeta documental que contiene toda la información del proceso con el funcionario, se logra comprobar que la carpeta físico existe, pero en medio digital no, al particular se informa, que es una medida que se tiene pensada para el año 2025, por lo anterior, se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad del numeral 7.1.1 de la norma ISO27002
Responsable: Dirección de Gestión del Talento humano

9.9. Pese a que existe una política y un lineamiento especifico de cara al desarrollo seguro de aplicaciones y la metodología se viene aplicando continuamente para los proyectos de software, evidenciamos que existen aplicativos nuevos y antiguos en el ambiente de producción, que utilizan protocolos no seguros, como es el caso del protocolo HTTP o puerto TCP 80, 8080, en sitios como: http://appa.saludcapital.gov.co/GestionPruebas/,http://sdsdlf01.saludcapital.gov.co:10000/edelphynbb/login.jsp, http://fappd.saludcapital.gov.co/crue/ - SIDCRUE, en consecuencia, existe un potencial riesgo por acceso no autorizado y perdida de confidencialidad, por lo anterior, se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad con el requisito numeral 14.2.1
Responsable: Dirección TIC

9.10. Aun cuando existe el procedimiento formal de gestión de incidentes y requerimientos de servicios denominado TIC - SDS-TIC-PR-002, identificamos que dicho procedimiento no trata los incidentes específicos de seguridad de la información, toda vez que los flujos respecto a la etapa investigativa, análisis de causa raíz, análisis forense y la aplicación de las acciones correctivas, no se define, en consecuencia, existe una debilidad que afecta el tiempo de oportunidad de la activación de los servicios y no se cuenta con los elementos probatorios o de cadena de custodia para dar inicio al proceso judicial, por lo anterior, se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad al requisito numeral 16.1.5
Responsable: Dirección TIC

9.11. Pese a que las diferentes contraseñas de aplicativos, dispositivos y hardware son de manejo individual por cada administrador o propietario, evidenciamos que dichas contraseñas son manejadas y controladas mediante correos electrónicos y las personas responsables se puede retirar de la entidad y se perdería la información, en consecuencia, existe una debilidad que se podría afectar la confidencialidad y la disponibilidad de la información, y las contraseñas no son centralizadas o unificadas mediante un software de gestión de contraseñas, por lo anterior, se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad al requisito numeral 9.4.3
Responsable: Dirección TIC

9.12. Si bien es cierto, se cuenta con la política específica de respaldos de información para los activos de información de la entidad y el cumplimiento se soporta mediante la solución ARCbackup y se complementa con la solución VEAM Backup, evidenciamos que dicha política no ha sido del todo efectiva, ya que resultado de las múltiples caídas del servidor de HIPERCONVERGENCIA o PIVOT3 y sumado a las intermitencias de energía que afectaron la infraestructura de la entidad, fue necesario el restablecimiento de la información mediante las copias generadas, no obstante, el restablecimiento no fue efectivo en todos los casos, ya que tomo varias horas e incluso varios días y otros sistemas de información no se lograron recuperar, como

fue el caso de los servicios: Aprender Salud, SICAI, KOHA, Repositorio institucional (DSPACE), entre otros, en consecuencia, se hace necesario garantizar la integridad de las copias y realizar pruebas de recuperación permitiendo dar cumplimiento en su totalidad al requisito numeral 12.3.1 de la norma ISO27002
Responsable: Dirección TIC

9.13. Pese a que se cuenta con un Directorio Activo o Active Directory (AD) que permite organizar y gestionar todos los elementos de la red: ordenadores, grupos, usuarios, dominios, políticas de seguridad, entre otros, evidenciamos que no todos los elementos de la SDS están siendo gestionados bajo este enfoque, y es responsabilidad de los administradores, realizar la depuración de contraseñas en los diferentes sistemas de información de manera periódica, en consecuencia, existe una debilidad que se podría afectar la confidencialidad y la disponibilidad de la información y se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad de los numerales 9.2.5 y 9.4.3 de la norma ISO27001.
Responsable: Dirección TIC

9.14. Aun cuando existe el normograma propio del proceso de gestión TIC, que busca mantener el inventario de la normatividad y legislación aplicables, evidenciamos que varias registros como son: Ley 23 sobre derechos de autor, Decreto 1360 de 1989 y decreto 1474 de 2002 sobre propiedad intelectual, Decreto 333 de 2014 que reglamenta certificados y las firmas digitales, Ley 1221 de 2008 reglamento para el teletrabajo, Ley 1581 de 2012 protección de datos personales, Decreto 338 del 2022, lineamiento para fortalecer la gobernanza de la seguridad digital y Norma técnica ISO/IEC 27001:2013 o 2022, no se encuentran registrados, por lo anterior, existe una desactualización del inventario y se desconoce el estado real de implementación de la normatividad y legislación aplicable, en tal medida existe un cumplimiento parcial de cara al numeral A18.1.1 de la norma ISO27002.
Responsable: Dirección TIC

10. CONCLUSIONES. (NIA 2410-A1).

- Es indispensable seguir fortaleciendo las campañas de sensibilización a toda la organización para crear cultura de seguridad y un lenguaje común frente a los diferentes conceptos de seguridad, se considera una tarea continua en el tiempo mediante los siguientes mecanismos: cursos virtuales, intranet, correo electrónico y posters ubicados en sitios estratégicos, pantallas digitales, sesiones presenciales entre otros.

- La infraestructura existente mediante el datacenter conteiner, permite contener el nivel de riesgo al que puede estar expuesta la entidad ente posibles indisponibilidades y se ajusta al modelo de alta disponibilidad, no obstante, debido a cortes de fluido eléctrico sin previo aviso por codensa, se han presentado caídas

que han afectado la disponibilidad de los diferentes servicios críticos de la entidad que de acuerdo al plan de modernización se migraran a la nube de AZURE.

- Los controles de acceso físico a las instalaciones y dependencias de misión crítica deben fortalecerse, ya que algunos controles biométricos en puertas o áreas con información sensible, no están siendo eficaces ya que personal de otras dependencias tienen acceso abierto y pueden ingresar a estas áreas poniendo en riesgo la información.

- Como recomendación de la OCI, se ve necesario implementar controles biométricos en el archivo central de la entidad, ya que el acceso se realiza mediante llave o simplemente tocando la puerta ya tienes acceso, lo cual pudiera comprometer la información sensible que reposa o se almacena allí.

- Los diferentes filtros de acceso físico mediante personal de vigilancia en áreas sensibles están siendo vulnerado, toda vez que se logró comprobar que el personal no revisa el paso de equipos de cómputo y fácilmente se dejó engañar y en esa medida se logró sacar el portátil de la oficina de las instalaciones de la SDS obviando los controles humanos. Es de anotar que mediante los registros de las cámaras de vigilancia se puede apreciar y comprobar el ejercicio realizado.

- Se cuenta con el lineamiento aprobado y cronograma de programación de análisis de vulnerabilidades WEB para 100 IPs, utilizando herramientas especializados para detectar posibles brechas de seguridad y aplicando los correctivos o remediaciones necesarias con el equipos del SOC, no obstante, aplicaciones desarrolladas que pasaron recientemente al ambiente de producción, no han sido objetivo de este análisis, en esa medida existe potencial riesgos de perdida de información por acceso no autorizado a los sistemas de información.

- Sera indispensable implementar para robustecer la arquitectura de seguridad, servidores de detección de intrusos - IDS de tipo host o red, así como servidores de prevención de intrusos – IPS, ya que en la actualidad no se tienen, dichos elementos permitirán detectar actividades sospechosas o no autorizadas, como los ataques de suplantación de identidad (phishing), la infección y distribución de virus, la instalación/descarga de malware y ransomware, la denegación de servicio (DOS), los ataques de intermediarios, los ataques de día cero, la inyección SQL, entre otros.

- Se debe documentar el procedimiento específico para la gestión y respuesta a los incidentes de seguridad de la información y deberá contemplar el análisis forense.

- La estructura de roles y responsabilidades definida frente a la seguridad de información en la entidad, debe ser dado a conocer a todas las partes interesadas y debe ponerse en práctica.

- Las matrices de riesgos no son diligenciadas y remitidas por todos los procesos, dicha situación se debe fortalecer, ya que el lineamiento se está incumpliendo y pueden materializarse los riesgos de activos de información que no fueron reportados.

- El contacto con autoridades con es el caso de la policía nacional se debe seguir fortaleciendo ya que boletines informativos sobre incidentes de seguridad que se venían reportando periódicamente no volvieron a llegar y será necesario contactar a esta unidad y verificar que puede estar ocurriendo.

- El control de acceso vehicular se realiza por medio del control de acceso biométrico con tarjeta de acceso (carnet) o dactilar y la habilitación de las talanqueras, no obstante, al ingresar 2 o 3 personas en el mismo vehículo no se realiza la verificación correspondiente y en personas sin autorización ingresan a la entidad.

- Al realizar el mapeo de controles de la Norma ISO27002 versión 2013 a la nueva versión 2022, se identifican 11 nuevos controles, por lo será recomendable para el proceso de Gestión TIC, definir e implementar en el mediano plazo, las mejoras que haya lugar para dar cumplimiento en su totalidad de los controles de los numerales: 5.23. Seguridad de la información para el uso de servicios en la nube, 5.30. Preparación de las TIC para la continuidad del negocio, 5.7. Inteligencia de Amenazas, 7.4. Supervisión y Seguridad física, 8.10. Eliminación de Información, 8.11. Enmascaramiento de datos, 8.12. Prevención de fuga de datos, 8.16. Actividades de Seguimiento, 8.23. Filtrado WEB, 8.28. Codificación Segura y 8.9. Gestión de configuración, permitiendo que la entidad se encuentre en sintonía con los marcos de referencia actualizados. Dicha recomendación fue presentaba en el informe de auditoría del año 2023 y la fecha de la presente auditoria sigue sin avance, argumentando que no están preparados para esta evolución.

- Planes de recuperación ante desastres - DRPs que permiten dar respuesta ante una crisis, siguen en desarrollo, dicha situación fue evidenciada en la auditoria del año 2023 y con sorpresa y preocupación reportamos el mismo estado, ya que los documentos siguen en construcción o han dicho aprobados y no se ha ejecutado ningún tipo de prueba. La acción del plan de mejora nro. 2871 sigue sin avance y sin eficacia después de más de un año, dicho lo anterior, se decreta una no-conformidad con el grupo de controles del dominio 17 de la norma ISO27002.

- Es recomendable seguir realizando ejercicios de auditorías internas de seguridad de la información que permitan evaluar el cumplimiento de los requisitos de la norma y de esta manera preparar a la organización ante una posible certificación internacional en el largo plazo.

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

- A pesar de que existe una declaración de aplicabilidad – SOA, que define los controles necesarios para gestión de riesgos y justifica cada uno de los controles aplicables, así como las exclusiones, se constata que el instrumento excluye controles que en la práctica son necesarios y obligatorios, por lo anterior, es necesario reevaluar la implementación de los controles excluidos, a fin de dar cumplimiento en su totalidad con el numeral 6.1.3 literal d) de la norma ISO27001. El SOA es un documento que define lo que se debe desplegar a nivel institucional y no es una camisa de fuerza.

- En lo que respecta al componente PIVOT3 o servidor de HIPERCONVERGENCIA que se vio afectado con varios incidentes de servicio, se informa que no continúa funcionando en la entidad, no obstante, cuando ocurrió el incidente, se restablecieron los servicios en un 95% y los aplicativos que se vieron afectados de forma crítica, representan el 5%. Desde la dirección TIC, se informa que se está trabajando en la adquisición de infraestructura backups, que responda con el tema de espacio, integridad y seguridad de la información.

- El proceso de gestión del talento humano, no exige a todos los servidores públicos diligenciar el formato de confidencialidad, toda vez que es un deber, como servidor público, la confidencialidad de la información que maneja en razón de sus funciones de conformidad con lo señalado en el artículo 38 de la Ley 1952 de 2019, “Por medio de la cual se expide el Código General Disciplinario, se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario”. En el TÍTULO IV - DERECHOS, DEBERES, PROHIBICIONES, INCOMPATIBILIDADES, IMPEDIMENTOS, INHABILIDADES Y CONFLICTOS DE INTERESES DEL SERVIDOR PÚBLICO, el artículo 38 señala: Son deberes de todo servidor público: Numerales 5 y 6: Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función; las facultades que le sean atribuidas, o la información reservada a la que tenga acceso por razón de su función, en forma exclusiva para los fines a los que están afectos, y custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso; e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidas”.

- Como mecanismo de control de acceso físico en portería para visitantes, se cuenta con el aplicativo TIS, no obstante, al consultar la base de información, se observan registros de visitas que no cuentan con fecha/hora de salida, al parecer no se realizó la descarga en el aplicativo del sticker entregado.

11. PLAN DE MEJORAMIENTO (NIA 2500).

Como resultado de la auditoría, el proceso auditado deberá cumplir con el lineamiento establecido por la dirección de planeación institucional y calidad para la elaboración del plan de mejoramiento que haya lugar, con el fin de realizar el tratamiento adecuado 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. Nota: Sera responsabilidad de los referentes elaborar el plan de mejoramiento adecuado que responda a las oportunidades de mejora identificadas.

12. ANEXOS.

Corresponde a los papeles de trabajo utilizados en cada mesa de trabajo realizadas y que serán remitidos a las partes interesadas para el análisis de cada uno de los casos.

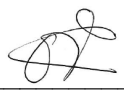
- LISTADEVERIFICACION AUDITORIA-SI.xlsx

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

Firmado digitalmente por Francisco Javier Pinto Gonzalez

Francisco Javier Pinto González

APRUEBA JEFE OFICINA DE CONTROL INTERNO.



Firmado digitalmente por OLGA LUCIA VARGAS COBOS

Olga Lucia Vargas Cobos

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