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
Certificado CISM ISACA No. 221867531,
Lead Auditor ISO27001:2013 registro ERCA No.1001545 e
Certificado HSEQ, registro IAC No. GEC68940

REVISADO POR:

OLGA LUCIA VARGAS COBOS
JEFE OFICINA DE CONTROL INTERNO

BOGOTÁ, abril 2023

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)

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

Evaluar el modelo de la seguridad de la información de la entidad, mediante las buenas prácticas como es la Norma Certificable ISO 27001, el código de buenas prácticas ISO 27002 y complementarias, con el fin de determinar el mantenimiento, la mejora continua del mismo y la implementación de las iniciativas del Modelo de Seguridad y Privacidad de la Información - MSPI. Se realizará la verificación de 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 existen en la entidad, analizar las vulnerabilidades y riesgos existentes, en cumplimiento de las medidas y políticas de seguridad establecidas.

2.2 Analizar las políticas y procedimientos de seguridad definidos y se revisa su grado de cumplimiento.

2.3 Verificar y evaluar el cumplimiento del marco normativo que lo rige: Resoluciones, Decretos y Normas.

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).

Contemplara la evaluación de los requisitos mínimos seleccionados para el establecimiento del Sistema de Seguridad de la información en base al ciclo de vida PHVA.

Periodo a evaluar:

- Desde: 1/03/2022
- Hasta: 28/02/2023

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

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

Para el desarrollo de la presente auditoría se tuvo 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 DE SOLUCIONES DE SOFTWARE

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 3701 de 2011 - Política en ciberseguridad y ciberdefensa
- 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 presencial y virtual con los diferentes referentes designados, verificando y constatando el cumplimiento la conformidad de los requisitos normativos acorde a las listas de verificación elaboradas. 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, con el objetivo de verificar o constatar la conformidad de algunos de los requisitos normativos seleccionados, respecto al sistema de gestión de seguridad de la información SGSI.

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

Revisión de la documentación de seguridad de la información: El auditor solicitó y revisó la documentación existente en la entidad con respecto a la gestión de la seguridad de la información, verificando los documentos de políticas de seguridad de la información, procedimientos, guías, registros de actas entre otros documentos. De la misma manera se revisaron los procesos definidos para determinar la relación con el modelo de seguridad de la información SGSI.

Consultas con el personal designado: El auditor realizó consultas específicas a los funcionarios designados de la entidad y consulto piezas comunicativas elaboradas, con el fin de conocer el nivel de concientización frente a la seguridad de la información.

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

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

Introducción

El Modelo de Seguridad y Privacidad de la Información también conocido como - MSPI y 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 está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales, tamaño, 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 acerca de la adecuada gestión de riesgos, 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.

Finalmente, es importante tener presente que la norma ISO27001:2013 certificable, evalúa el ciclo de vida del sistema de acuerdo a sus 7 dominios y el código de buenas prácticas ISO27002:2013 evalúa 14 dominios y sus 114 controles, todos estos elementos descritos hacen parte del instrumento de autoevaluación que el MinTIC exige a cada entidad para conocer el nivel de avance en la implementación del modelo y para efectos de la presente auditoria se eligieron algunos de los requisitos para determinar su conformidad.

Cabe señalar que se tuvo en cuenta la actualización de la norma ISO27002:2022 y el mapeo de los nuevos controles establecidos; sin embargo, en común acuerdo con los auditados en la reunión de apertura, dichos controles serán tenidos en cuenta en el plan de mejoramiento del presente informe, permitiendo que la entidad se encuentre en sintonía con los marcos de referencia actualizados.

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

Dominios de la Norma	Cumple	Oportunidad de Mejora	Total general
5 Liderazgo	**7**	**4**	**11**
5.1 Liderazgo y compromiso	2	1	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	**2**	**1**	**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
10 Mejora	**1**		**1**
10.2 Mejora continua	1		1
Total general	**23**	**7**	**30**

Tabla 1: Norma ISO27001:2013

La tabla resume la evaluación realizada frente a los 6 dominios y 30 requisitos seleccionados, de los cuales 23 es decir el 76% de estos requisitos, están conformes mientras que 7 requisitos es decir 24%, requieren iniciar una oportunidad de mejora. Es importante señalar que, en este último, los requisitos se cumplen, pero es indispensable dar inicio a un plan de mejoramiento para fortalecer y afianzar cada uno de estos elementos.

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

Dominios y controles	Cumple	Oportunidad de Mejora	Total general
A.10 Criptografía	1	1	2
A.10.1 Controles criptográficos	1	1	2
A.11 Seguridad física y del ambiente	5	2	7
A.11.1 Áreas seguras	3	1	4
A.11.2 Equipamiento	2	1	3
A.12 Seguridad de las operaciones	9		9
A.12.1 Procedimientos operacionales y responsabilidades	4		4
A.12.2 Protección contra código malicioso	1		1
A.12.3 Respaldo	1		1
A.12.4 Registro y monitoreo	1		1
A.12.6 Gestión de la vulnerabilidad técnica	2		2
A.13 Seguridad de las comunicaciones		2	2
A.13.2 Transferencia de información		2	2
A.14 Adquisición, desarrollo y mantenimiento del sistema	3	2	5
A.14.1 Requisitos de seguridad de los sistemas de información	1		1
A.14.2 Seguridad en procesos de desarrollo y soporte	2	2	4
A.15 Relaciones con el proveedor	3		3
A.15.1 Seguridad de la información en las relaciones con el proveedor	2		2
A.15.2 Gestión de entrega del servicio del proveedor	1		1
A.16 Gestión de incidentes de seguridad de la información	2	2	4
A.16.1 Gestión de incidentes de seguridad de la información y mejoras	2	2	4
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del nego	1	3	4
A.17.1 Continuidad de la seguridad de la información		3	3
A.17.2 Redundancias	1		1
A.18 Cumplimiento	1	2	3
A.18.1 Cumplimiento con los requisitos legales y contractuales		2	2
A.18.2 Revisiones de seguridad de la información	1		1
A.6 Organización de la seguridad de la información	3	1	4
A.6.1 Organización interna	1	1	2
A.6.2 Dispositivos móviles y trabajo remoto	2		2
A.7 Seguridad ligada a los recursos humanos	3		3
A.7.1 Previo al empleo	2		2
A.7.2 Durante el empleo	1		1
A.8 Administración de activos	5		5
A.8.1 Responsabilidad por los activos	2		2
A.8.2 Clasificación de la información	2		2
A.8.3 Manejo de los medios	1		1
A.9 Control de acceso	5	1	6
A.9.1 Requisitos de negocio para el control de acceso	2		2
A.9.2 Gestión de acceso del usuario	2		2
A.9.4 Control de acceso al sistema y aplicaciones	1	1	2
Total general	**41**	**16**	**57**

Tabla 3: Norma ISO27002:2013

La tabla anterior, resume la evaluación realizada frente a 13 dominios y 57 controles seleccionados, de los cuales 41 controles es decir el 72% cumplen; mientras que 16 controles es decir el 28%, requieren iniciar una oportunidad de mejora. Es importante señalar que, en este último, los controles se cumplen; pero es indispensable dar inicio a un plan de mejoramiento para fortalecer y afianzar cada uno de estos elementos.

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

6.1 Esquema de la Líneas de Defensa

TEMAS REVISADOS	ASPECTOS VERIFICADOS
6.2 Ambiente de control: Es el conjunto de normas, procesos y estructuras que proveen las bases para llevar a cabo el control interno a través de la organización	Contempló la revisión de diferentes procedimientos operativos, procedimientos SIG 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.
6.3 Actividades de Control (incluye la revisión de políticas de operación procedimientos, normatividad interna y externa, Plan Operativo Anual	1. Se verificó y evaluó el cumplimiento de los requisitos y controles del alcance, además de los procedimientos existentes para la gestión de la seguridad de la información. 2. Se verifico y evaluó el cumplimiento del marco normativo aplicable, resoluciones y decretos. 3. A nivel de control se tuvo en cuenta los procedimientos, instructivos y documentación complementaria que hacen parte del repositorio de información documental evaluados para este alcance. 4. Se evaluó mediante encuesta, el nivel de percepción frente a los valores institucionales y como a través de campañas de sensibilización y adherencia se está dando a conocer a todas las partes interesadas.
6.4 Evaluación del Riesgo y controles (incluye análisis de contexto, riesgos relacionados identificación de controles y su operación, posibles riesgos detectados)	Se llevó a cabo revisión y verificación de la gestión de riesgos propios de la seguridad de la información, la evaluación fue realizada por los referentes de seguridad de la información en cada una de las dependencias, la solicitud masiva se hizo a 31 dependencias y se obtuvo la matriz diligenciada de las 31 dependencias para una eficacia del 100%, la nueva solicitud para el año 2023, se remitió a las áreas el día 10 de marzo y se espera respuesta de la autoevaluación de riesgos con fecha límite el día 15 de mayo 2023. Si bien es cierto, se realiza una gestión de riesgo y cuenta con varios elementos presentados, evidenciamos que al comparar el mismo registro de riesgo de un año a otro identificamos que la severidad se mantiene a valor "MODERADO"; sin embargo, la severidad pudo haber disminuido a causa de la implementación y la eficacia de los controles; pero esto en la evaluación no se ve representado y año a año se presenta el mismo comportamiento, lo cual no es del todo lógico. Dicho lo anterior, se deriva una oportunidad de mejora que busca fortalecer la valoración de los riesgos existente.

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

6.5 Actividades de monitoreo (incluye las acciones que la primera y segunda línea de defensa ejercen para mitigar la ocurrencia de los riesgos sean este seguimiento al cumplimiento de políticas, actividades, directrices, metas)	Se llevó a cabo la verificación y el resultado fue el siguiente: Primera Línea (Autocontrol): • Implementar acciones correctivas: Se consultan las acciones registradas en el aplicativo isolucion, producto de la auditoria al sistema realizada en el año 2022, acciones de mejora que la mayoría fueron implementadas y se comprobó su eficacia. • Ejecutar procedimientos de riesgo y control: El gestor o referente de seguridad informa que, el monitoreo de los controles no es una tarea constante y se realiza una vez al año, mediante el instrumento de autoevaluación se logra identificar, evaluar, controlar y mitigar los riesgos de la gestión de seguridad de la información y mediante la verificación realizada a las fuentes de información suministradas, se identifican registros de riesgos transversales, así como la valoración cualitativa de los mismos. Si bien es cierto, se realiza una gestión de riesgo y cuenta con varios elementos presentados, evidenciamos que al comparar el mismo registro de riesgo de un año a otro identificamos que la severidad se mantiene a valor "MODERADO", sin embargo, la severidad pudo haber disminuido a causa de la implementación y la eficacia de los controles, pero en la evaluación no se ve representado y año a año se presenta el mismo comportamiento, lo cual no es del todo lógico. Dicho lo anterior, se deriva una oportunidad de mejora que busca fortalecer la valoración de los riesgos existente. Segunda Línea (Autoevaluación): • Aseguran que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente. • Supervisan la implementación de prácticas de gestión de riesgo eficaces por parte de la gerencia. Resultado: Mediante la verificación realizada a las fuentes de información proporcionadas de cara a la gestión de riesgos desarrollada por la dependencia, se evidencian matrices de registros de riesgos transversales de SI. Se cuenta con el plan de gestión riesgos de seguridad, el cual será implementado a largo del año 2023. Cabe resaltar que el plan contempla adicionalmente las actividades de implementación de controles y monitoreo de los riesgos.

6.6 Información y comunicación	• Se verifico el proceso, procedimientos, registros e información compartida, así como los diferentes aplicativos utilizados. • Se consultaron diferentes piezas comunicativas (TIPS informativos), que reflejan las campañas de sensibilización desarrolladas respecto a conceptos, prácticas y recomendaciones frente a la seguridad de la información. • Se cuenta con el rol de gestor de Seguridad de la información en cada una de las dependencias, quienes tienen como responsabilidad, multiplicar o replicar los conocimientos adquiridos a los colaboradores de cada dependencia; sin embargo, al consultar con las áreas se informa que la actividad no se realiza y desconocen del tema, por lo que el control no es del todo eficiente y se deriva una oportunidad de mejora. • Se cuenta con registros de actas de reuniones de revisión por la dirección, comité técnico y comité institucional de gestión y desempeño como mecanismos de comunicación de los diferentes temas a los interesados.

A continuación, mediante tablas se comparten los puntos evaluados que requieren oportunidad de mejora:

Norma ISO27001:2013

DEFINICION DEL CONTROL	Resultado de la Evaluación
5.1 Liderazgo y compromiso **Literal d) comunicar la importancia de una gestión de Seguridad de la información eficaz y de la conformidad con los requisitos del SGSI**	El control se realiza por medio de las capacitaciones o charlas a los referentes de seguridad de la información en la entidad, así mismo se cuenta con piezas comunicativas de diferentes temas relacionados con la SI y se difunde por medio del correo institucional, el cual es remitido de manera masiva a todos los colaboradores de la entidad y mediante las pantallas digitales y el subsitio en la intranet de seguridad de la información. Las capacitaciones hacia los gestores de seguridad se realizan de manera anual y cada 6 meses se realiza una capacitación a público en general, cabe señalar que el rol de Gestor de SI, fue definido por las dependencias y tienen la responsabilidad de transmitir el conocimiento de las buenas prácticas de seguridad. Se obtiene la materia de capacitación elaborado del día 7 diciembre del 2022, se suministra la presentación y se cuenta con un video elaborado. Temas abordados: política general y específicas y tips de seguridad y se cuenta con registro de asistencia de 104 personas mediante el mecanismo virtual. Sin embargo, la figura o rol de gestor de seguridad tiene la responsabilidad de multiplicar los temas impartidos pero al consultar en algunas dependencias no se cuenta con registros al respecto, para el caso del gestor de salud pública, de acuerdo a lo informado realizo la capacitación pero no quedo registro de la actividad y en las otras dependencias al preguntan informan que la actividad no se realizó lo que demuestra que el control está siendo del todo eficiente y deriva en una oportunidad de mejora.

DEFINICION DEL CONTROL	Resultado de la Evaluación
5.2 Política Literal f) ser comunicada dentro de la organización	La política fue divulgada en primera instancia en la mesa técnica de gobierno y seguridad digital realizada el 29 de septiembre de 2022, igualmente en el comité institucional de gestión y desempeño realizado el 27 de febrero del 2023 y también se dio a conocer en la reunión de gestores de SI el día 10 de marzo del 2023 y en la capacitación del día 7 de diciembre del 2022. Se hizo la presentación especifica de las políticas de seguridad de información a los profesionales de la Dirección de Provisión de Servicios de Salud y a todos los colaboradores de la entidad, tanto de planta como de contrato, se realizó la divulgación mediante las piezas comunicativas al correo institucional. A la consulta el correo del 20 de abril del 2022, se recuerda la política específica de escritorios limpios. El gobierno de SI, remite de manera anual, memorando a cada una de las dependencias solicitando a los gestores de seguridad que tendrán la responsabilidad de brindar asistencia y orientación a los usuarios internos y externos sobre la SI, memorando y radicado nro. 2022IE3410 del 14 de febrero del 2023, igualmente se consulta memorando radicado: 2022IE3410 del 14 de febrero del 2023. Para efectos de comprobación de las funciones del gestor, se toma como caso la oficina de comunicaciones, jurídica y OCI, a fin de determinar si el gestor de Seguridad está realizando la retroalimentación de los temas impartidos por el coordinador de SI. Sin embargo, al consultar con estas áreas evidenciamos que la actividad no se realiza, no se tiene registro de ello y los funcionarios desconocen los cambios frente a las políticas y demás temas lo que deriva en una oportunidad de mejora, ya que el control no es del todo eficiente.

DEFINICION DEL 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.**	Se cuenta con la matriz de roles y responsabilidades por medio de la cual se definen los diferentes roles con lo que está conformado el sistema de SI, al consultar la matriz de fecha 14 de septiembre del año 2022, encontramos los siguientes 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 en cada dependencia, partes interesadas, colaboradores, aliados, y por último proveedores. Es clave señalar que la estructura está conformada por 9 roles; sin embargo, dichos roles no han sido comunicados según lo manifestado, es decir, en la entidad quien ejerce el rol, desconoce las responsabilidades que tiene frente al sistema. De acuerdo a lo anterior, se deriva una oportunidad de mejora toda vez que el control no es del todo eficiente y se debe dar a conocer los diferentes los roles y responsabilidades definidas del sistema y se debe comunicar a los referentes para que sea efectiva la estructura.

DEFINICION DEL 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 sistema se realiza mediante el comité institucional y desempeño. Trimestralmente la Dirección TIC, reporta el estado del sistema 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 en la política de seguridad digital, el reporte consultado corresponde al corte del primero de julio al 30 de septiembre del 2022 y los temas reportados fueron: continuidad de negocio, análisis de impacto, lineamientos y seguridad de SI, avance en seguridad en la nube, análisis de vulnerabilidades. En síntesis, del periodo evaluado, se planeó un 7% y se cumplió el 7%. Como segunda medida se cuenta con el tablero de indicadores de gestión de Seguridad Digital con fecha primero de febrero del 2023 y se cuenta con el informe de presentación de resultados del desempeño presentado en la mesa técnica. Los resultados de los indicadores presentados fueron los siguientes: medición primero de enero a diciembre 31 del 2022. Indicador1: 93,5% correspondiente al reporte de activos de información, indicador2: 100% correspondiente al plan de sensibilización, indicador3: 100% correspondiente a la gestión de los incidentes reportados y específicos de SI, indicador4: 100% control de acceso a la red de datos e indicador5: se obtuvo un 70%, que corresponde al conocimiento de las políticas de SI, es decir que no todos los funcionarios conocen la política, lo cual es una debilidad existente y se debe fortalecer. Por lo anterior se establece como acción de mejora.

DEFINICION DEL 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;**	Se suministra documento DECLARACION DE APLICABILIDAD-SOA de fecha noviembre 30 del año 2022 y al consultar el documento, evidenciamos que existen controles que están documentados y se consideran que "no se cumplen", pero en la operación son necesarios, por consiguiente, de deriva una oportunidad de mejora que permitirá actualizar dicho documento.

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

DEFINICION DEL 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.**	Se informa que la evaluación es realizada por parte de los referentes de seguridad de la información en cada una de las dependencias, para ello se hizo la solicitud a 31 dependencias y se obtuvo respuesta de la matriz diligenciada para las 31 dependencias. La nueva solicitud para el año 2023, se remitió a las áreas el día 10 de marzo año 2023 y se espera respuesta de la autoevaluación de riesgos con fecha límite el día 15 de mayo 2023. Podemos concluir que la evaluación de riesgos año a año se mantiene y se realiza una vez al año de acuerdo a la directriz de planeación institucional y calidad, sin embargo, evidenciamos lo siguiente: al comparar el mismo registro de riesgo de un año a otro identificamos que la severidad del riesgo se mantiene en valor: "MODERADO", sin embargo, la severidad pudo haber disminuido a causa de la implementación y la eficacia de los controles lo cual no se ve representado en la evaluación realizada. Por lo que al comparar año a año se presenta el mismo comportamiento, lo cual no es del todo lógico. Dicho lo anterior, se deriva una oportunidad de mejora que busca fortalecer la valoración de los riesgos En lo que respecta a la identificación del riesgo en la matriz para cada una de las dependencias, evidenciamos que no se tiene establecido un consecutivo o identificador único para el riesgo y tampoco se cuenta con un mapa de calor que consolide por IDENTIFICADOR los riesgos más relevantes en la entidad, la matriz es un elemento esencial que presenta el estado de los riesgos a la alta dirección y con ello permite la toma de decisiones. En la actualidad los 31 archivos son matrices individuales y no se ha realizado una presentación de los resultados.

Anexo A o Norma ISO27002:2013

Dominio y Control	Resultado de la Evaluación
A.10 Criptografía **A.10.1.1** **Política sobre el uso de controles criptográficos**	Al consultar el documento de políticas específicas codificado SDS-TIC-POL-001 versión 11, 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 la 5 (Correspondientes al cifrado de Discos Duros y cifrando mediante contraseñas de diferentes documentos) no se están aplicados ya que no se cuenta con evidencia al respecto. 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. 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 toma pantallazo de la consulta realizada al certificado Digital del sitio WEB PAI el cual utiliza control criptográfico del proveedor DIGICERT. Cabe señalar que en la actualidad se encuentra en curso la etapa precontractual para la consecución de la actualización de los certificados ya que vencen en el mes de julio del año 2023. El número de certificados digitales SSL con los que cuenta la entidad son 18. Se anexa tabla de URLS de sitio web.

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

Dominio y Control	Resultado de la Evaluación
A.11 Seguridad física y del ambiente **A.11.1.2 Controles de acceso físico**	Con el fin de brindar la seguridad física de los activos, bienes y personas la Subdirección de Bienes y Servicios se adelantó el contrato de licitación pública suscrito con la empresa MEGASEGURIDAD Número 2491117 del 2021. Dicho contrato finaliza el 6 de mayo del año 2023 y se encuentra en curso la adición por 2 meses mientras surte el nuevo proceso de la contratación. 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, cámaras de seguridad y hacia la calle o zonas verdes se cuenta con barreras perimetrales o cámaras que en caso de detectar un intruso genera la alarma correspondiente. Dichas cámaras monitorean las 24 horas del día. Una vez detectado el intruso se llama a la policía. Cabe señalar que para lo que lleva el año 2023, se han tenido 3 contenciones de intrusos y se cuenta con informe del caso presentado. Así mismo en el entorno, se cuenta con controles de acceso físico por torniquetes y personal de seguridad que permiten controlar el acceso de personal no autorizado a la entidad apalancado por el sistema BIOSTAR en donde se realiza el registro del visitante, existen áreas restringidas como son: el datacenter, cuartos de rack de comunicaciones, el laboratorio por ejemplo cuenta con control de acceso biométrico y se efectúa prueba simulada del acceso a estas áreas, con lo cual se pudo comprobar la eficacia del control. Se informa que a la fecha no se ha reportado pérdida de equipos de personal interno o visitante y al consultar el informe de visitas TIS del día 13 de abril 2023, se identifican 758 registros de visitas, sin embargo, al observar el inventario encontramos que existen registros de visitantes que cuentan fecha y hora de entrada, pero no de salida, lo cual demuestra que el control no es del todo eficiente. La validación se realizó con los siguientes números de cedula: 1033682058 y 1037659626. Al investigar los hechos por parte del referente, se informa que el donante ingreso, pero salió en la buseta y el otro fue del laboratorio, pero se desconoce la hora de salida. Esto mismo ocurre para otros 3 casos consultados, que no registran fecha de salida. Acorde con lo anterior, se deriva una oportunidad de mejora ya que existe una debilidad con respecto a la eficiencia del control en la captura de los datos de fecha y hora de salida de algunos de los registros de los visitantes. Con respecto a los equipos de cómputo que ingresan a la entidad por los filtros de acceso, se cuenta con el aplicativo MEGASEGURIDAD que permite tener el registro de los equipos de cómputo ingresados a la entidad. Para efectos de comprobación se solicitó el informe consolidado del día 13 de abril y se evidencian registros que no cuentan con fecha y hora de salida de portátiles, lo que origina una oportunidad de mejora para fortalecer dicho control. Respecto al sistema de monitoreo de cámaras, se consulta a la cámara Nro. 1 del cuarto UPS y se comprueba que se encuentran trabajando dos personas del proveedor POWERSUN y se consulta registro de la autorización de ingreso o correo del personal del día 14 de abril. Cabe señalar que el personal externo que va a realizar un trabajo, debe ir acompañado por personal de la SDS y debemos asegurar que el acceso a otras dependencias se encuentre bloqueado. 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. En lo que refiere al acceso Biométrico, la mayoría de áreas utilizan tarjeta de proximidad y dactilar; pero solo el área del IDCBIS tiene acceso por reconocimiento facial.

Dominio y Control	Resultado de la Evaluación
A.11 Seguridad física y del ambiente **A.11.2.9** **Política de escritorio y pantalla limpios**	En el documento de políticas específicas denominado: SDS-TIC-POL-001 versión 11, en los numeral 6.16, se define la política de escritorio y pantalla limpia, al realizar la lectura de las reglas establecidas, los numerales 3 y 4 hacen énfasis sobre pantallas y escritorios limpios, sin embargo, los numeral 1,2, y 5 al 8 corresponden a reglas de la política de usuarios desatendidos por lo que es importante realizar los ajustes requeridos. Se deriva una oportunidad de mejora. De otra parte, se consulta pieza comunicativa de fecha 13 de abril del 2022.

Dominio y Control	Resultado de la Evaluación
A.13 Seguridad de las comunicaciones **A.13.2.2** **Acuerdos sobre transferencia de información**	Mediante el documento de políticas específicas denominado: SDS-TIC-POL-001 versión 11 en el numeral 6.19, página 57, define las políticas y procedimientos para la transferencia de información el cual establece 8 numerales. Así mismo, se establece acuerdo de intercambio de información en el numeral 6.20 y el cual consta de 4 puntos. Se procedió a verificar con las dependencias el uso y diligenciamiento del formato, así como el medio por cual se realiza la transferencia de la información. Se consulta un formato suministrado de fecha 19 de agosto 2022 para el proyecto SISEM. Sin embargo, no en todos los casos de transferencias de información, se utiliza el formato. Por lo que el control no es del todo eficiente. Dicho lo anterior, se deriva una oportunidad de mejora que permita a los gestores de SI, realizar divulgación del tema ya que los proceso desconocen el formato y procedimiento a seguir.

Dominio y Control	Resultado de la Evaluación
A.13 Seguridad de las comunicaciones **A.13.2.4** **Acuerdos de confidencialidad o no divulgación**	Con respecto a los acuerdos de confidencialidad para persona natural, se consulta el contrato en la modalidad de prestación de servicios de un profesional especializado de la dirección TIC, bajo el número de Contrato: 3478229, en donde se establece el acuerdo de confidencialidad mediante la cláusula Nro. 18. Al consultar el contrato para persona jurídica Nro.; 3018794 del 2021, que corresponde a la administración del centro de cómputo y mesa de ayuda, evidenciamos la cláusula nro.: 16, que corresponde al acuerdo de confidencialidad. Un segundo caso consultado, corresponde al contrato para el software ARCbackups, número de contrato: 4109767 del 2022 y en la cláusula nro. 16, se establece el acuerdo de confidencialidad. Respecto al contrato de personal natural de planta o curva administrativa de la SDS, al consultar el manual de funciones, el acta de posesión y por último el acto administrativo, no se evidencia el acuerdo de confidencialidad frente a la información, lo cual constituye en un riesgo, toda vez que el personal de planta podría divulgar información sensible de la entidad. En consecuencia, se deriva una oportunidad de mejora.

Dominio y Control	Resultado de la Evaluación
A.14 Adquisición, desarrollo y mantenimiento del sistema **A.14.2.3** **Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación**	Se informa que la mayoría de desarrollos están sobre la nube de Azure, dichos cambios son realizados por la fábrica de software, sin embargo, no lleva un control formal de los cambios ya que no queda registró sobre software realizado. En síntesis: En los proyectos de software de la nube en AZURE, no se lleva gestión de cambios y acorde a lo informado apenas se está implementado. Ahora bien, lo que tiene que ver con cambios o mejoras de software realizados por el equipo on-promise de la SDS, dichos cambios pasaron por el comité de cambios, fueron aprobados y se tiene trazabilidad del registro en Aranda Software. Como proceso, el desarrollador en conjunto con el líder técnico de TIC, diligencian el formato SDS-TIC-FT-025 v1, Acorde a lo anterior, se deriva una oportunidad de mejora que permita extender e implementar el proceso de gestión de cambios a los proveedores, ya que existe un riesgo frente a indisponibilidad y afectación de los usuarios respecto a los diferentes aplicativos.

Dominio y Control	Resultado de la Evaluación
A.14 Adquisición, desarrollo y mantenimiento del sistema **A.14.2.6** **Entorno de desarrollo seguro**	Se cuenta con política específica en el documento: SDS-TIC-POL-001 versión 11, en el numeral 6.7.3, se establece la seguridad en el desarrollo de sistemas de información y hace el llamado al procedimiento de soluciones de software SDS-TIC-PR-001. al consultar en la base documental de isolucion, encontramos la guía: SDS_TIC_GUI-010 v1 Guía para el análisis y diseño de sistemas, dicha guía debe ser diligenciada por cada uno de los desarrolladores y al final del proyecto entrega el documento final que debe contemplar los aspectos de seguridad de la información en su numeral 9.2. Se suministra evidencia al respecto. En lo que respeta a la fábrica de software mediante el proveedor ETB, establecen su propia metodología, Así mismo, se consulta documento por medio del cual se establece la metodología para el desarrollo seguro con cada una de sus etapas, sin embargo, dicho documento se encuentra en etapa preliminar y no se ha vuelto actualizar, cabe señalar que varios de los pasos aquí descritos, no se están aplicando en la actualidad, lo que deriva en vulnerabilidades del desarrolló del sistema que pueden ser atacadas. Se deriva una acción de mejora que permita la elaboración del documento final, su aprobación, divulgación hacia los desarrolladores y aplicación en la operación. Como evidencia se remite el documento de metodología preliminar.

Dominio y Control	Resultado de la Evaluación
A.16 Gestión de incidentes de seguridad de la información **A.16.1.2** **Informe de eventos de seguridad de la información**	Mediante las herramientas de monitoreo de los componentes de seguridad perimetral y consola de antivirus, se cuenta con el registro y trazabilidad de los eventos propios que comprometen la seguridad de la información, dichos eventos son categorizados y se estable el ranking de los eventos presentados mediante el informe de gestión del 14 enero al 13 de febrero del 2023 por medio del cual, el especialista de ETB, reporta los eventos presentados. Es clave informar que la entidad no cuenta en la actualidad, con un sistema SIEM, que permita el monitoreo de las amenazas que afectan la seguridad y permitan centralizar toda esta información, analizarla y correlacionarla para agilizar los protocolos de respuesta ante un ciberataque. En la actualidad se realiza de manera aislada para algunos de los componentes, Acorde a lo anterior se deriva una oportunidad de mejora que permita fortalecer dicho control.

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

Dominio y Control	Resultado de la Evaluación
A.16 Gestión de incidentes de seguridad de la información **A.16.1.5 Respuesta ante incidentes de seguridad de la información**	Se informa que los incidentes de seguridad, son tratados mediante el procedimiento actual para el manejo de los incidentes de servicios e infraestructura; pero no se cuenta con un procedimiento documentado y específico para el manejo de incidentes de SI. Sin embargo, cuando se presenta un caso de estas características se procede de la siguiente manera: Se detecta y confirma por lo cual un funcionario o el especialista reporta el incidente de SI mediante la mesa de ayuda, posteriormente, el grupo de primer nivel técnico verifica el posible incidente y determinar si corresponde a un incidente, se registra, se categoriza y se aplica el tratamiento en el grupo de segundo nivel, se determina si requiere apoyo adicional para la solución, se escala a un tercer nivel y al consultar la herramienta Aranda, encontramos que existe un categoría denominada: Incidentes de SI. De acuerdo a lo anterior, el control se está realizando parcialmente y no existe un procedimiento documentado. Acorde a lo anterior, se deriva una oportunidad de mejora con el fin de definir y construir el lineamiento para el manejo de incidentes de Seguridad, el cual deberá contemplar el flujo de la etapa investigativa, análisis de causa raíz y el análisis forense.

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 son parte de los planes de continuidad donde se establecen las respuestas o tratamientos de las incidencias o contingencias. Se suministra el documento plan de recuperación DRP, el cual es la respuesta ante una situación de crisis o parada de los distintos servicios críticos de la entidad como son: energía, comunicaciones, red, colapso de infraestructura. Al consultar el repositorio documental de la Dirección TIC encontramos los siguientes documentos elaborados: 1. plan de continuidad TIC - 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, observamos que se encuentra desactualizado y describe los servicios prioritarios de la entidad, sin embargo, los pasos y el detalle respecto a la forma de proceder en cada uno de los servicios, no se describe con claridad, lo que conlleva a una oportunidad de mejora toda vez que el DRP no ha sido formalizado y probado, lo que pone en riesgo la disponibilidad de los servicios e impide demostrar la eficacia del plan. Evidenciamos al consultar el plan DRP sobre el sistema de prevención y extinción de incendios, hace el llamado al procedimiento operativo: SDS-THO-PL-001 v3 que corresponde al plan de prevención, preparación y respuesta de emergencias. Si bien es cierto existe el documento DRP donde se describen cada uno de los servicios, es importante precisar que no se cuenta con pasos a seguir y el directorio con responsables y líneas de contacto se encuentra desactualizado, ya que el documento se encuentra en construcción y en consecuencia no se encuentra aprobado. Observamos que el documento preliminar define 3 fases: Preventiva la cual consta de 7 actividades, Fase de respuesta que actúa durante el desastre y establece el procedimiento de notificación DRP. Sin embargo, dicho documento no fue allegado y lo correspondiente a la fase 3 restauración.

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

	Documentos principales y anexos se encuentran en desarrollo lo que deriva en una oportunidad de mejora.

Dominio y Control	Resultado de la Evaluación
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**	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. Al consultar el documento en su última versión: 3-1-1. Sep_SDS_Plan de Recuperación de desastres, v.0.1.7 2022, dicho documento contempla 3 fases y una serie de actividades previas, durante y posterior al evento para la atención en caso de desastre. Sin embargo, dicho documento se encuentra en construcción y los procedimientos que hace el llamado el plan DRP general están en desarrollo. De cara a la implementación del DRP, se realizaron sesiones con los referentes para la preparación de los DRP el día 16 de enero 2023 en lo que respecta a la preparación de pruebas y ejercicios con el equipo de centro de cómputo. Aclaración de conceptos y objetivos respecto a la recuperación del Centro de cómputo. Sesión2 enfoca a la plataforma TIC y Sesión3 procedimientos para los servicios. Se consulta el documento plan de prueba_ 3 febr. 2023.inicial.pdf, el cual define como objetivo la "aplicación de nómina". Para generar un ataque de RANSOMWARE, cifrando las bases de datos lo que conlleva a que el proceso de liquidación de nómina una se vea afectado. Fecha establecida: 3 de febrero del año 2023. Se consulta la evidencia adicional que corresponde a la preparación y ejecución DRP_2023.pdf. Actividad. Ejecución de prácticas y ejercicios DRP. Escenario Especifico y Periodo del informe 1 al 10 de febrero del 2023. Sin embargo, evidenciamos que los documentos: Formato Plan de prueba, Formato _Reporte de actividades y lista de verificación no se encuentran diligenciados para la prueba especificada y no se evidencian resultados de la prueba planificada lo que conlleva a una oportunidad de mejora.

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.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	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, se deriva en una oportunidad de mejora.

Dominio y Control	Resultado de la Evaluación
A.18 Cumplimiento **A.18.1.1** **Requisitos Legales, estatutarios, reglamentarios y contractuales** **Identificación de la legislación vigente y los requisitos contractuales**	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. Al consultar el normograma propio del proceso TIC, encontramos varios registros de la legislación aplicable, sin embargo, lo que respecta a la ley 1581 de Protección de datos personales y ley 23 sobre derechos de autor, estas 2 no se encuentran registradas por lo que es indispensable realizar el registro. Es clave mencionar que respecto a la ley 1581 de protección de datos, se viene implementando ya que los diferentes aplicativos desarrollados de cara al ciudadano contemplan datos sensibles**, e**s por eso que al ciudadano se le informa al momento del registro que la entidad salvaguardara la información pertinente a partir de su política de protección de datos personales. Para efectos de comprobación, se consultó el tramites en línea de Registro y autorización de títulos en el área de la salud y al realizar el trámite se evidencia el control del manejo de datos personales para ello se obtiene pantallazos. En el enlace: https://tramitesenlinea.saludcapital.gov,co/registro/tratamiento_datos.

Dominio y Control	Resultado de la Evaluación
A.18 Cumplimiento **A.18.1.2** **Derechos de propiedad intelectual**	Mediante el documento codificado SDS-TIC-POL-001 versión 11, encontramos la política específica numeral 6.7.3 sobre la seguridad en el desarrollo de sistemas de información y define los derechos patrimoniales de derechos de autor y propiedad intelectual de todo proyecto de desarrollo de software y su correspondiente documentación pertenecen a la SDS. Es por eso que cada uno de los desarrolladores entrega la información del proyecto en el repositorio indicado o DEVOPS. De otro lado, se consulta pieza comunicativa de fecha 6 de abril del 2022 que informa sobre la instalación de programas no autorizados. Sin embargo, no se evidencia registros de piezas comunicativas al personal sobre las consecuencias de la violación de las políticas de uso de software por lo cual se debe fortalecer dicho aspecto. Se realiza la validación de los inventarios de activos de información del año 2022 que contempla los activos tipo software TIC que están afectados por derechos de propiedad intelectual. Al consultar la matriz, encontramos 94 registros que corresponden a los aplicativos desarrollados por y para la entidad.

Dominio y Control	Resultado de la Evaluación
A.6 Organización de la seguridad de la información **A.6.1.3** **Contacto con autoridades**	Colcert: Se informa que se presentó un incidente de seguridad el 8 de septiembre del 2022 y se comprometió el buzón de correo por malware phishing al interior y al exterior de la entidad. Desde la Dirección TIC, se reporta el incidente al correo electrónico del COLCERT y solicitaron información adicional. Se cuenta el soporte de correo electrónico del día 9 de septiembre del 2022, reporte de seguridad digital al colcert. Alta consejería: la SDS a través de la dirección TIC ha tenido contacto constante con ellos, nos han hecho invitaciones a las sesiones del programa "compartic" a nivel distrito. Se cuenta con registros de las sesiones realizadas. La alta consejería solicito en diciembre el instrumento de autoevaluación del MSPI y el instrumento de diagnóstico de datos personales. CSIRT de la policía: Nos reportan noticias TIC y alertas de seguridad mediante boletines informativos, el último reporte fue del día 12 de enero del 2022. Sin embargo, después de esa fecha no se han vuelto a recibir boletines por lo que es indispensable ponerse en contacto con la autoridad competente para garantizar este aspecto. Se deriva oportunidad de mejora.

Por último;

Dominio y Control	Resultado de la Evaluación
A.9 Control de acceso **A.9.4.3** **Sistema de gestión de contraseñas**	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 administrador 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 se desconoce, lo cual es una debilidad existente ya que si en una eventualidad el administrador renuncia, se llevaría los usuarios y contraseñas de ámbito administrador o root. Dado lo anterior, es necesario fortalecer este aspecto mediante la implementación de software gratuito para la Gestión de Contraseñas.

Nota: El resultado de la ejecución del plan de auditoria se presenta en detalle mediante las listas de verificación, las cuales se entregan en medio digital para posteriormente ser analizadas por los responsables del sistema de la entidad. El informe final es la síntesis de todo el ejercicio realizado. Es importante resaltar que la auditoría realizada, implicó la revisión y evaluación de acuerdo al cronograma establecido, las evidencias y soportes suministrados fueron cotejaron para algunos de los activos de información pertenecientes a los diferentes procesos del alcance.

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

7. ASPECTOS POSITIVOS (NIA 2410 A2).

- El Datacenter actual de la entidad, se encuentra en fase de migración a un datacenter- conteiner tipo TIER III adquirido e instalado, que ofrece un lugar seguro y protegido para almacenar información crítica de la entidad, responde a la recuperación de desastres y garantiza la disponibilidad de los servicios.

- Se cuenta con activos de información críticos de la entidad, implementados en la nube de Azure, que responde a un esquema de alta disponibilidad.

- Los controles de acceso físico a las instalaciones y dependencias de misión crítica son adecuados, ya que tiene implementado controles biométricos, la mayoría de áreas utilizan tarjeta de proximidad, dactilar y en el área del IDCBIS acceso por reconocimiento facial.

- Producto de las actividades de mantenimientos preventivos establecidos en conjunto con los proveedores, se vienen detectando debilidades de seguridad en los sistemas, errores, omisiones o fallos que pueden ser objeto de posibles ataques.

- Se cuenta con el lineamiento y la practica necesaria para realizar periódicamente, análisis de vulnerabilidades con herramientas especializados para detectar posibles brechas de seguridad y aplicar los correctivos o remediaciones necesarias.

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

- El recurso humano conoce las entradas y las salidas de cada uno de los procedimientos evaluados y determina los recursos físicos y tecnológicos que son necesarios para la operación del sistema.

- 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.

- 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).

NO IDENTIFICADAS.

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

9.1. Si bien es cierto, el líder del sistema de seguridad de la información viene convocando y realizando las jornadas de capacitación y sensibilización a los referentes de seguridad en los diferentes escenarios, evidenciamos que la responsabilidad especifica de retroalimentar o multiplicar el conocimiento a los colaboradores del cada una de las dependencias sobre los contenidos impartidos como es el caso de las política general y especificas aprobadas, no se está realizando y no existe registro de ello, en consecuencia, se deriva un potencial riesgo por desconocimiento de los colaboradores, ya que van tener dificultades para adaptarse y aplicar las últimas tecnologías en sus tareas y se van a obviar las nuevas medidas y controles de seguridad establecidos en la entidad, por lo anterior, se hace necesario implementar las mejoras que haya lugar para dar cumplimiento en su totalidad a los requisitos numerales 5.1 literal d), 5.2 literal f) y 5.3 literal b)
Responsable: Dirección TIC

9.2. Pese a que se cuenta con una matriz RACI de roles y responsabilidades, además de una estructura jerárquica de seguridad de la información establecida para la entidad, se evidencia que dichos roles no han sido comunicados ya que las personas o colaboradores que ejercen los roles dentro de la entidad, desconocen las responsabilidades que tienen frente al sistema, en consecuencia, se deriva un potencial riesgo ya los colaboradores trabajarán de forma individual y no se lograran 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 al requisito numeral 5.3
Responsable: Dirección TIC

9.3. A pesar de que existe una declaración de aplicabilidad – SOA que establece los controles necesarios para gestión de riesgos y justifica cada uno de los controles aplicables, así como las exclusiones, se evidencia que el documento excluye controles o establece que los controles ”no se cumplen” y en la práctica son obligatorios, en consecuencia, se deriva un potencial riesgo frente a la brecha de las medidas de seguridad no implementada, por lo anterior, se hace necesario actualizar e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad al requisito numeral 6.1.3 literal d).
Responsable: Dirección TIC

9.4. Mediante las matrices de riesgos de seguridad de la información que posee la entidad para las 31 dependencias en donde se identifica y valora los riesgos, evidenciamos que el valor de la SEVERIDAD del riesgo al comparar un año a año no cambia o se mantiene y es no todo sería lógico, toda vez que la implementación de los controles debió haber contribuido a la disminución de la SEVEREDAD del riesgo, así mismo no se tienen definidos "identificadores únicos" para el manejo de cada riesgo por dependencia, lo cual no permite ver representado el riesgo en un MAPA DE RIESGOS para la toma de decisiones, en consecuencia, se deriva un potencial riesgo frente a los peligros existentes y su valoración inadecuada, por lo anterior, se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad con el requisito numeral 8.2.
Responsable: Dirección TIC

9.5. 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 los numerales 3 y 5 correspondientes al cifrado de Discos Duros y cifrado mediante contraseñas de diferentes documentos, no se está aplicado en la entidad, por lo anterior, se deriva un potencial riesgo frente a la pedida de confidencialidad de la información sensible de la entidad, por lo anterior, se hace necesario implementar las mejoras que haya lugar para dar cumplimiento en su totalidad con el control número A.10.1.1.
Responsable: Dirección TIC

9.6. Al consultar el informe de visitas generado mediante el software TIS del día 13 de abril 2023 por parte del equipo de seguridad y control, se identifican 758 registros de visitas de personas externas de la secretaria, sin embargo, existen registros de visitantes que no cuentan con fecha y hora de salida, se validaron los números de cedula: 1033682058 y 1037659626 y al investigar los hechos por parte del auditado, se informa que la persona ingreso pero no quedo registrada la hora de salida, esto mismo ocurrió con otros registros consultados, lo cual demuestra que el control no es del todo eficiente. En consecuencia, se deriva un potencial riesgo ante un posible daño o acceso a información sensible, por lo anterior, se hace necesario implementar las mejoras que haya lugar para dar cumplimiento en su totalidad con el control número A.11.1.2
Responsable: Subdirección de Bienes y Servicios

9.7. pese a que existe la política específica de escritorio y pantallas limpias definida en el documento SDS-TIC-POL-001 versión 11, evidenciamos que los numerales 1,2, y 5 al 8 corresponden a reglas específicas de la política de usuarios desatendidos. En consecuencia, existe una debilidad con respecto al control, por lo anterior, se hace necesario realizar los ajustes que haya lugar para dar cumplimiento en su totalidad con el control número A.11.2.9
Responsable: Dirección TIC

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

9.8. Si bien es cierto, los acuerdos de confidencialidad se están aplicando como requisitos en los contratos de prestación de servicios de personal natural y los contratos de persona jurídica como se pudo comprobar, evidenciamos que los contratos que tienen que ver con personal natural de planta o curva administrativa de la SDS en lo que respecta a los documentos manual de funciones, acta de posesión y acto administrativo, no se evidencia el acuerdo de confidencialidad frente a la información. en consecuencia, se deriva un potencial riesgo frente a una posible fuga de información sensible de la entidad, por lo anterior, se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad con el requisito numeral 13.2.4
Responsable: Dirección TIC y Talento Humano

9.9. pese a que la gestión de los cambios o mejoras sobre software se viene realizando por el equipo de desarrollo de la SDS, los cambios o mejoras de software que son realizado por la fábrica de software de ETB y que reposan en la nube de Azure, no hacen parte del proceso de gestión de cambios y no se encuentra registro de ello, en consecuencia, se deriva un potencial riesgo frente a la disponibilidad de los servicios ya que un cambio no informado y aprobado puede generar una afectación sobre los servicios, por lo anterior, se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad con el requisito numeral 14.2.3
Responsable: Dirección TIC

9.10. Pese a que existe una política especifica el desarrollo seguro definida en el documento SDS-TIC-POL-001 versión 11 en su numeral 6.7.3, evidenciamos que la metodología para el desarrollo seguro se encuentra en elaboración mediante un documento preliminar que fue suministrado y que a la fecha no se ha vuelto actualizar, en consecuencia, existe una debilidad respecto a posibles huecos de seguridad en el software que pueden ser utilizadas por un atacante, por lo anterior, se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad con el requisito numeral 14.2.6
Responsable: Dirección TIC

9.11. Si bien es cierto, existe el Plan de recuperación de desastres v.0-1-2_2022.pdf, evidenciamos que dicho documento se encuentra desactualizado, los pasos de recuperación respecto a cada uno de los servicios críticos no se describen con claridad, no se cuenta con el directorio de responsables, ni líneas de contacto y por ende no ha sido aprobado ni puesto a prueba, por consiguiente, existe un potencial riesgo ante una posible afectación o desastre que afecte la disponibilidad de los servicios, por lo anterior, se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad al requisito numeral 17.1.1
Responsable: Dirección TIC

9.12. 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 para iniciar el 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

9.13. Si bien es cierto, se cuenta con herramientas de monitoreo de los componentes de seguridad perimetral y consola de antivirus desagregados, evidenciamos que la entidad en la actualidad no cuenta con una herramienta SIEM que permita centralizar y consolidar toda la información de las diferentes fuentes, analizarla, correlacionarla y dar respuesta ante un ciberataque, en consecuencia, existe una debilidad en cuanto a la gestión integral y consolidada de eventos de seguridad, por lo anterior, se hace necesario definir e implementar las mejoras que haya lugar para dar cumplimiento en su totalidad al requisito numeral 16.1.2
Responsable: Dirección TIC

9.14. Pese a que la gestión de contraseñas es realizada por el directorio activo para los usuarios en general y se sincroniza para los diferentes aplicativos, evidenciamos que para lo que tiene que ver con los activos de información tipo servidores o dispositivos CORE de la entidad, las contraseñas son administradas de manera individual y no son centralizadas, es decir, no existe un repositorio de contraseñas unificadas, en consecuencia, existe una debilidad que podría afectar la disponibilidad y confidencialidad de la información, 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

10. CONCLUSIONES. (NIA 2410-A1).

- La infraestructura de seguridad existente, permite contener el nivel de riesgo al que puede estar expuesta la entidad ente posibles amenazas de índole humano y se ajusta al modelo de defensa en profundidad.

- A fin de realizar un monitoreo 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, será indispensable que la entidad adquiera e implemente un sistema SIEM, ya que en la actualidad no se cuenta con dicho elemento y hace parte de los elementos de la arquitectura de seguridad que utilizan muchas organizaciones. Sera de mucha utilidad.

- 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, lo cual permitirá 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.

- Existe cumplimiento respecto a los criterios impuestos por la Ley de Protección de Datos Personales.

- La gestión de incidentes y la mesa de ayuda (SOC-NOC) cumple con los requisitos funcionales de negocio, sin embargo, será necesario definir y aplicar procedimiento específico para la respuesta a los incidentes de seguridad de la información.

- La estructura de roles y responsabilidades definida frente a la seguridad de información en la entidad, debe ser dada a conocer y puesta en práctica.

- La evaluación de riesgos se debe fortalecer, ya que la severidad del riesgo por múltiples controles no cambia y no se tiene definidos identificadores del riesgo por cada dependencia que permita verlos reflejados en un mapa de riesgo.

- Es indispensable seguir fortaleciendo las campañas de sensibilización a toda la organización para que el lenguaje sea común frente a los diferentes conceptos, 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, permitiendo generar una cultura de seguridad institucional.

- 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.

- 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 y largo 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.

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.

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

12. ANEXOS.

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

- LISTADEVERIFICACION AUDITORIA-SI2023_Parte1.xlsx
- LISTADEVERIFICACION AUDITORIA-SI2023_Parte2.xlsx

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

Francisco Javier Pinto González

APRUEBA JEFE OFICINA DE CONTROL INTERNO.

Olga Lucia Vargas Cobos

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