INFORME FINAL DE AUDITORÍA

AUDITORIA INTERNA 2020 AL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN RESPECTO A LA NORMA NTC ISO/IEC 27001:2013 PARA LA SECRETARIA DISTRITAL DE SALUD - SDS

OFICINA DE CONTROL INTERNO

AUDITOR (ES):
LÍDER: FRANCISCO JAVIER PINTO GONZALEZ
Auditor Líder Certificado en ISO27001:2013
Registro ERCA No.1001545

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

BOGOTÁ, Julio 2020

SECRETARÍA DISTRITAL DE SALUD

Contenido

1. OBJETIVO GENERAL DE LA AUDITORÍA.

Determinar de manera integral el estado actual de la gestión de la seguridad información en los procesos muestra definidos por la Secretaria Distrital de Salud - SDS mediante la auditoria interna, teniendo como referente la norma ISO/IEC 27001:2013 y anexo A. El ejercicio permitirá emitir el informe final, el cual definirá y contemplará las oportunidades de mejora que haya lugar.

2. OBJETIVOS ESPECÍFICOS DE LA AUDITORÍA.

- Elaborar el plan de auditoría y los instrumentos de auditoria para la recolección de información, evidencias y pruebas que se llevarán a cabo.
- Establecer la situación actual en cuanto a la seguridad de la información (Nivel de Madurez).
- Elaborar y entregar a los líderes del SGSI el informe final de auditoria con recomendaciones y observaciones del auditor que permitan a la entidad implementar las oportunidades de mejora que haya lugar.

3. ALCANCE DE LA AUDITORÍA.

Comprende la revisión y evaluación de las directrices trazadas con relación a la Seguridad y Privacidad de la Información descritas en la norma IEC ISO 27001:2013 y su anexo A, como uno de los habilitadores transversales de la Política de Gobierno Digital y su respectivo manual del Modelo de Seguridad y Privacidad de la Información MSPI, establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC. Contempla la revisión y evaluación de la implementación de lo dispuesto en la legislación vigente sobre protección y tratamiento de datos personales Ley 1581 del 2012, lineamientos establecidos en el Modelo Integrado de Planeación y Gestión – MIPG y Norma ISO27032 - Ciberseguridad.

DEPENDENCIAS AUDITADAS:

- DIRECCION TIC
- DIRECCION DE TALENTO HUMANO
- DIRECCION ADMINISTRATIVA
- OFICINA ASESORA DE COMUNICACIONES
- OFICINA ASESORA JURIDICA
- OFICINA DE CONTROL INTERNO
- OFICINA DE ASUNTOS DISCIPLINARIOS
- SUBDIRECCION DE CONTRATACION

- DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD

PROCESOS AUDITADOS (como muestra se consultó:)

- GESTION DE TIC
- GESTION DEL TALENTO HUMANO
- GESTION DE URGENCIAS EMERGENCIA Y DESASTRES
- GESTION DE COMUNICACIONES

4. CRITERIOS DE AUDITORÍA.

- Norma IEC ISO 27001:2013 y Anexo A
- Decreto 1008 de 2018 Política de Gobierno Digital, habilitadores transversales SI
- CONPES 3854 del 2016 Política Nacional de Seguridad Digital
- Ley 1581 del 2012 protección y tratamiento de datos personales
- Norma IEC ISO 31000:2018 y 27005 para Gestión de Riesgos
- Norma 1EC ISO 22301:2012 Continuidad de Negocio.
- Framework NIST 801-53 –Cyberseguridad ISO 27032
- Decreto 1499 de 2017 - MIPG

5. MARCO LEGAL.

- Decreto 1008 de 2018 Política de Gobierno Digital, habilitadores transversales SI
- CONPES 3854 del 2016 Política Nacional de Seguridad Digital
- Ley 1581 del 2012 protección y tratamiento de datos personales
- Decreto 1499 de 2017 - MIPG
- Norma IEC ISO 27001:2013 y Anexo A

6. METODOLOGÍA UTILIZADA.

Con el objetivo de evaluar los requerimientos de la Norma Certificable ISO27001:2013 y los 114 controles agrupados en 14 dominios definidos en el ANEXO-A el auditor se tuvo en cuenta la siguiente metodología:

- **Visita de Sitio**

  El auditor realizo visita a las instalaciones de la sede administrativa PISO 3,4,6 y 7, porterías, acceso a los parqueaderos, con el objetivo de verificar uno a uno los requisitos normativos con respecto al sistema de gestión de seguridad de la información SGSI.

- **Revisión de la documentación de seguridad de la información**

  El auditor solicitó y revisó la documentación existente en la entidad respecto a la gestión de la seguridad de la información verificando los documentos de políticas de seguridad de la información, procesos, procedimientos, guías, registros de actas entre otros documentos, 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, con el fin de conocer el nivel de concientización frente a la seguridad de la información en la operación diaria.

- **Listados de verificación con los Auditados**

  El auditor entrega la lista de requisitos de revisión, la cual se diligenció en compañía de los referentes de las diferentes dependencias, dueños de proceso 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.

7. ANÁLISIS DE INFORMACIÓN Y DE DATOS.

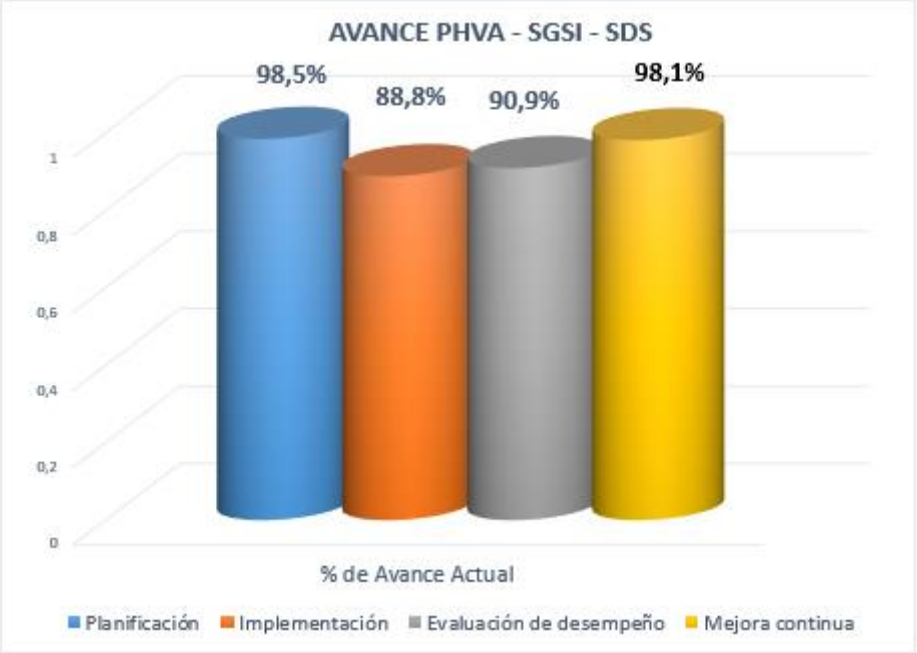
El resultado de la ejecución del plan de auditoria se presenta en detalle en las listas de verificación, las cuales se entregan en medio digital para posteriormente ser tratados por los responsables del sistema de la entidad. El informe final es la síntesis de todo el ejercicio realizado.

Es importante resaltar que la auditoría realizada, implicó la revisión y evaluación con base al tiempo establecido y apoyados de la herramienta (TEAM) como medida de teletrabajo definida por la Secretaría para interactuar con los referentes de sistema. Las evidencias y soportes necesarios suministrados fueron cotejaron para unos activos de información pertenecientes a los procesos del alcance y no a todos.

7.1 Resultados con base a la norma NTC ISO-IEC 27001:2013

El porcentaje de cumplimiento por los 7 dominios o Ciclo PHVA de la norma certificableNTC ISO-IEC 27001:2013 es el siguiente:

Figura 1. % de Avance Ciclo PHVA NTC ISO-IEC 27001:2013



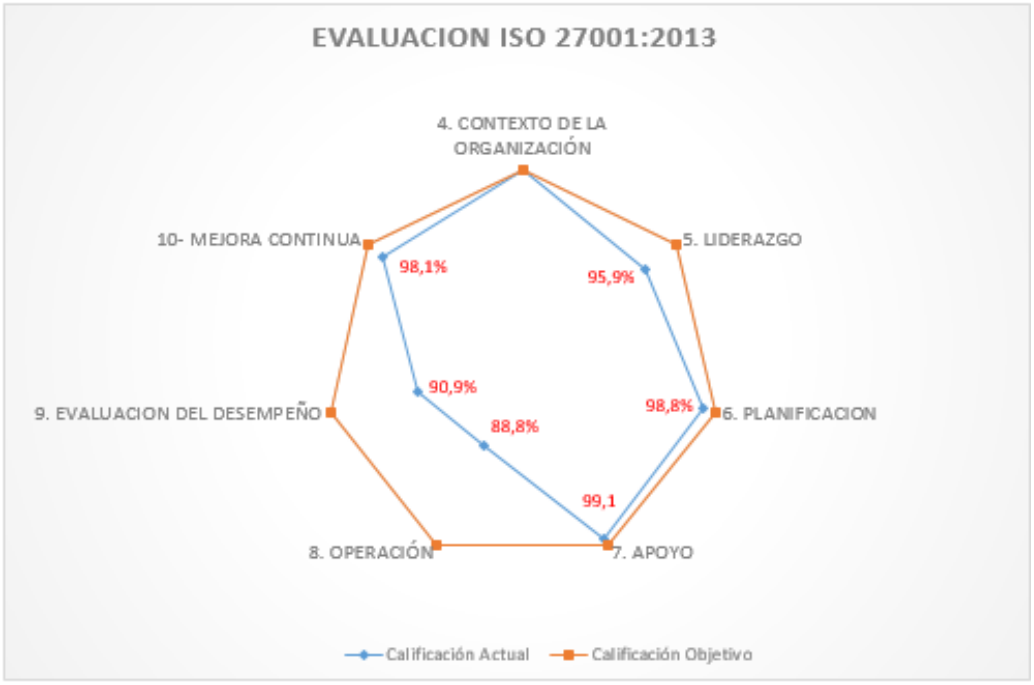
Fuente: Auditor

Tabla 1. % de Avance por Dominio NTC ISO-IEC 27001:2013

Ciclo PHVA	Dominios de la Norma	% Avance Requisitos	% Avance	Meta
P	4 Contexto de la Organización	100%	98,5%	100%
	5 Liderazgo	95,9%		100%
	6 Planificación	98,8%		100%
	7 Apoyo	99,1%		100%
H	8 Operación	88,8%	88,8%	100%
V	9 Evaluación de desempeño	90,9%	90,9%	100%
A	10 Mejora	98,1%	98,1%	100%
Total general		**96%**	**94%**	100%

Fuente: Auditor

Figura 2. % de Avance por Dominio NTC ISO-IEC 27001:2013



Fuente: Auditor

Figura 3. Resultado evaluación de requisitos norma NTC ISO-IEC 27001:2013

Fuente: Auditor

Tabla 2. Requisitos clasificados a partir de la evaluación, norma NTC ISO-IEC 27001:2013

Dominios	Cumple	No Conformidad Menor	Oportunidad de Mejora	Total general
4 Contexto de la Organización	10			10
5 Liderazgo	19		3	22
6 Planificación	46		2	48
7 Apoyo	33		1	34
8 Operación	5		3	8
9 Evaluación de desempeño	25	2	7	34
10 Mejora	15		1	16
Total general	**153**	**2**	**17**	**172**

Fuente: Auditor

Se evidencia un cumplimiento general con base al total de requisitos evaluados de la Norma ISO27001:2013 del **96%.** Ver resultados de lista de verificación para mayor detalle.

7.2 Resultados con base al Anexo A

Porcentaje de cumplimiento por cada uno de los 14 dominios y 114 controles de la norma NTC ISO-IEC 27001:2013 es el siguiente:

Figura 4. Análisis de Brecha 14 Dominios ANEXO A

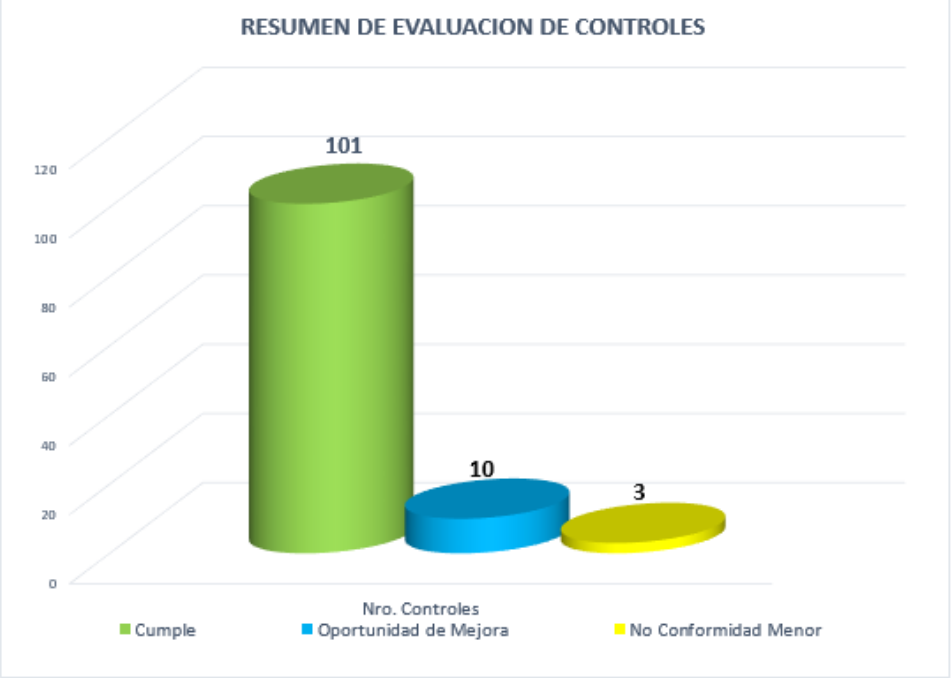
Fuente: Auditor

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

ID	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Controles Requeridos	Calificación Objetivo
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	70%	2	100%
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	95,7%	7	100%
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100%	6	100%
A.8	GESTIÓN DE ACTIVOS	94%	10	100%
A.9	CONTROL DE ACCESO	100%	14	100%
A.10	CRIPTOGRAFÍA	100%	2	100%
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	100%	15	100%
A.12	SEGURIDAD DE LAS OPERACIONES	97,9%	14	100%
A.13	SEGURIDAD DE LAS COMUNICACIONES	100%	7	100%
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	100%	13	100%
A.15	RELACIONES CON LOS PROVEEDORES	88%	5	100%
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	92,9%	7	100%
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	75%	4	100%
A.18	CUMPLIMIENTO	92,5%	8	100%
PROMEDIO EVALUACIÓN DE CONTROLES		**96%**	**114**	**100%**

Fuente: Auditor

Figura 5. Resultado de evaluación de los 114 controles ANEXO A



Fuente: Auditor

Tabla 4. Clasificación de controles evaluados, norma NTC ISO-IEC 27002:2013

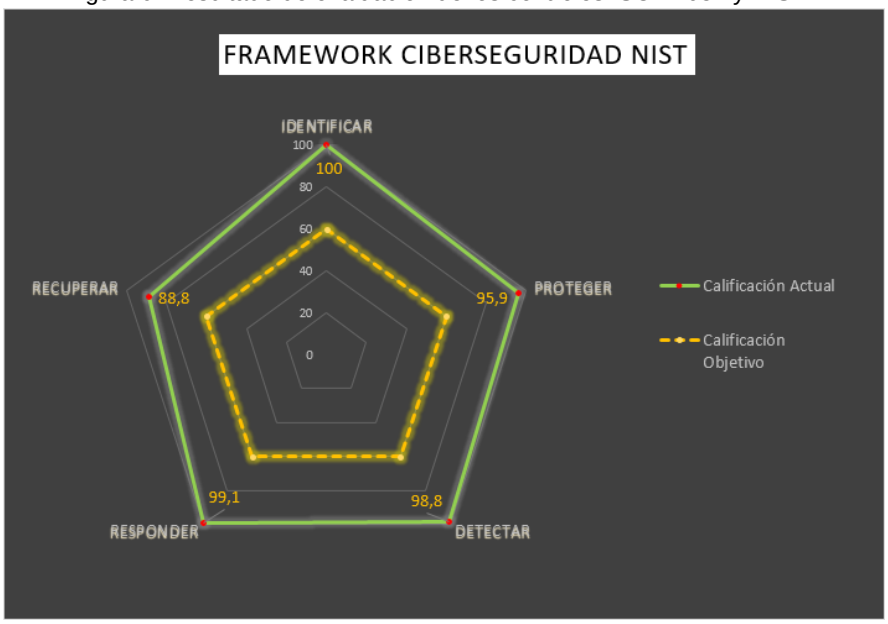
Dominios	Cumple	No Conformidad Menor	Oportunidad de Mejora	Total general
A.5 Políticas de seguridad de la información			2	2
A.6 Organización de la seguridad de la información	6		1	7
A.7 Seguridad ligada a los recursos humanos	6			6
A.8 Administración de activos	8		2	10
A.9 Control de acceso	14			14
A.10 Criptografía	2			2
A.11 Seguridad física y del ambiente	15			15
A.12 Seguridad de las operaciones	13		1	14
A.13 Seguridad de las comunicaciones	7			7
A.14 Adquisición, desarrollo y mantenimiento del sistema	13			13
A.15 Relaciones con el proveedor	3		2	5
A.16 Gestión de incidentes de seguridad de la información	6	1		7
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	2	2		4
A.18 Cumplimiento	6		2	8
Total general	**101**	**3**	**10**	**114**
Relación Porcentual	**87,7%**	**4,3%**	**7,8%**	**100%**

Fuente: Auditor

Se evidencia un cumplimiento promedio general con base al total de requerimientos del Anexo-A del **96%**. Ver resultados en la lista de verificación para mayor detalle.

7.3 Resultados del componente de Ciberseguridad - ISO 27032

Figura 6. Resultado de evaluación de los controles ISO 27032 y NIST



Fuente: Auditor

Tabla 5. Clasificación por fases, norma NTC ISO-IEC 27032

FASE DEL CICLO	REQUISITOS EVALUADOS	CALIFICACION OBTENIDA
DETECTAR	16	15,2
IDENTIFICAR	30	28,58
PROTEGER	122	119
RECUPERAR	3	2,5
RESPONDER	18	17
Total general	**189**	**182,28**

Fuente: Auditor

Se evidencia un cumplimiento general del 96% con base al total de requerimientos de la Norma. Ver resultados en la lista de verificación para mayor detalle. Hoja: CIBER

8. ASPECTOS POSITIVOS.

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

- Existe el compromiso firme de la alta dirección encaminado a promover la cultura de la seguridad de la información como elemento estratégico de la entidad.

- Se cuenta con una infraestructura sólida, protegida y pertinente a los propósitos y objetivos de la Secretaria.

- La infraestructura de seguridad con la se cuenta es adecuada para contener el nivel de riesgo al que puede estar expuesta la entidad, se ajusta al modelo de defensa en profundidad con capas especializadas que mitigan eventos de seguridad.

- Existe cumplimiento con algunos criterios impuestos por la Ley de Protección de Datos Personales.

- El Datacenter es un lugar seguro, responde a los requisitos de control de acceso, normas técnicas nacionales y demás requisitos de seguridad de estándar ISO 27001.

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

9. NO CONFORMIDADES.

9.1. Después de revisar los requisitos del componente numeral 9.1 Seguimiento, medición, análisis y evaluación (evaluar el desempeño de la seguridad de la información y la efectividad del SGSI) puede afirmarse que no se están aplicando los literales a, b, c, d, e y f y por ende incumpliendo dicho requisito, por cuanto la información proporcionada no define: Metodología clara de seguimiento y medición que defina entre otras cosas quien y cuando debe analizar y evaluar los resultados. Además de conservar información documentada apropiada como evidencia de los resultados.
Responsable: Dirección TIC.

9.2. Durante la auditoría realizada no se evidencian resultados de análisis de incidentes, que permitan identificar ciertos patrones y comportamientos similares y con ellos responder de manera rápida y eficaz a incidentes que se puedan presentarse en el futuro, en procedimientos actuales no se tiene documentado y en la operación no se realiza, con esto puede afirmarse que el aprendizaje de los incidentes de seguridad de la información basado en las buenas prácticas de la gestión del conocimiento KDB no se está realizando, lo que conlleva a un incumplimiento del requisito normativo id control: 16.1.6.
Responsable: Dirección TIC.

9.3. Después de realizar las entrevistas a los referentes y revisar los planes de contingencia de la plataforma de TIC del año 2019 y 2020 respectivamente, puede afirmarse que se incumple con el control ID: A.17.1.3 verificación, revisión y evaluación de la continuidad de la seguridad de la información, toda vez que plan no ha sido probado en su totalidad, las evidencias suministradas no son suficientes para respaldar un ejercicio adecuado que garantice la continuidad de las operaciones y servicios que provee la entidad, es necesario poner en práctica y realizar el simulacro del plan de contingencia para los sistemas críticos de la entidad y determinar su eficacia.
Responsable: Dirección TIC

9.4. La entidad cuenta con algunos elementos redundantes lo cual es soportado mediante la evidencia aportada y se encuentra documentado en el Plan de contingencia de la plataforma TIC enero 30 2020.pdf, sin embargo, se incumple el control id: A.17.2.1 toda vez que no se cuenta con las “redundancias suficientes” para cumplir con la disponibilidad de los servicios y sistemas críticos de entidad que pudieran verse afectados o comprometidos por un evento o incidente de alto impacto.
Responsable: Dirección TIC

10. ACCIONES PARA ABORDAR RIESGOS.

10.1. Aprobar, fortalecer la divulgación y publicar la política general y específicas de la seguridad de la información, toda vez es que un requisito obligatorio de la norma y se estaría cumpliendo parcialmente con los controles, ID: 5.2 literales f, g, ID: 7.3 y controles del anexo A, IDs: A.5.1.1 y A.5.1.2. Evidenciamos que las políticas se encuentran documentadas y actualizadas es una versión preliminar documento ANEXO, pero no se encuentran aprobadas por el comité institucional, además las mejoras sobre las políticas no se han divulgado. Es importante mencionar que campaña de divulgación y toma de conciencia sobre aspectos de seguridad de la información se realiza mediante TIPs informativos y sesiones presenciales se realiza, sin embargo, las oportunidades de mejora están encaminadas en:

a. Aprobar las políticas,
b. Fortalecer o reforzar el ejercicio de toma de conciencia para dar a conocer la importancia de seguridad de la información en la entidad (como ejercicio continuo en el tiempo), impulsando otras estrategias de comunicación como son: pantallas digitales, e-learnings, Boletines informativos, Videos e involucrar a otros interesados como son: Contratistas, Pasantes, proveedores y al público que hace uso de los servicios de la entidad y
c. Publicar en los repositorios establecidos.

Responsable: Dirección TIC, OAC

10.2. Actualizar la matriz SOA – Declaración de aplicabilidad, por cuanto esta desactualizada y estaría cumpliendo de manera parcial el numeral 6.1.3 literal d) generar una Declaración de Aplicabilidad que contenga los controles necesarios y además de la justificación de inclusiones y exclusiones de controles del Anexo A.
Responsable: Dirección TIC

10.3. Actualizar el INSTRUCTIVO CONTROL DE CAMBIOS.xlsx en los siguientes 3 aspectos:

- En lo que se refiere a los tiempos establecidos para la ejecución de tareas, no define con que periodicidad se hace o que día se hace, quien convoca y mediante que mecanismo se realiza.
- La fase de registro de RFC no está documentado, no se especifica que herramienta se utiliza, quien lo hace y con qué periodicidad.
- La fase de presentación de resultados del proceso mediante el comité institucional o revisión por la dirección no se está documentado. El objetivo es mostrar la eficacia del proceso en lo que respecta a número de cambios tramitados vs los ejecutados en un periodo determinado, clasificado por dependencias, tipos de cambios (normal o de emergencia) otros elementos de medición.

Toda vez que se cumple de manera parcial a los requisitos numeral 8.1 Planificación y Control operacional y Control anexo A ID: A.12.1.2.

Responsable: Dirección TIC

10.4. Definir los mecanismos, medir y obtener los resultados del Plan de seguridad y privacidad de la información enero 10 2020.pdf, toda vez que no define como se evaluaran los resultados de dicho plan, cumpliendo de manera parcial al requisito numeral 6.2 literal j.
Responsable: Dirección TIC

10.5. Definir e implementar las acciones para el tratamiento de los riesgos de seguridad de la información, toda vez que la evidencia aportada no es suficiente para demostrar el cumplimiento al requisito numeral 8.3. La fase del plan de tratamiento de los riesgos está programada para el segundo semestre del 2020.
Responsable: Dirección TIC

10.6. Crear un control más eficiente para conservar la información de los resultados de los riesgos de seguridad de la información en todas sus fases (registro, clasificación, valoración, tratamiento y medición de la eficacia, toda vez que los riesgos identificados están documentados en WORD y el manejo y control no es el más idóneo para demostrar el cumplimiento al requisito numeral 8.3
Responsable: Dirección TIC

10.7. Fortalecer los mecanismos que permitan realizar el análisis de las "no conformidades" registradas en la herramienta isolucion, determinar patrones o comportamientos similares o reincidencia y generar las acciones correctivas que eliminen la no conformidad por cuanto no se tiene evidencia actual que demuestre el cumplimiento al requisito 10.1 numeral 3. **Responsable:** Dirección TIC, Dirección de Planeación Institucional y Calidad.

10.8. Fortalecer el contacto con otros grupos de interés (foros especializados, universidades, proveedores especialistas en seguridad) que les permita crear nuevas alianzas de cooperación para mitigar el riesgo de posibles bugs, vulnerabilidades, nuevas amenazas y conocer nuevas tendencias, toda vez que la evidencia aportada cumple parcialmente con el control id: 6.1.4. La evidencia consultada demuestra el contacto que se tiene en la actualidad con los grupos de interés del Distrito.
Responsable: Dirección TIC

10.9. Crear el esquema de etiquetado de la información basado en la ley 1851 o 1712 para los documentos aprobados del sistema, toda vez que la evidencia presentada da cumplimiento parcial al control ID: A 8.2.2. por cuanto el etiquetado en el pie de página de algunos documentos aparece como: COPIA NO CONTROLADA pero no especifica si es un documento Sensible o Crítico.
Responsable: Dirección TIC, Subdirección de Bienes y servicios y Dirección de Planeación Institucional y Calidad

10.10. Crear el procedimiento formal para que el borrado seguro de la información de las unidades de almacenamiento que fueron dadas de baja para que sea inaccesible e ilegible utilizando herramientas gratuitas de borrado seguro, toda vez que el formateo de disco básico que se realiza en la actualidad no es suficiente para garantizar que la información fue borrada en su totalidad cumpliendo parcialmente el control ID: A.8.3.2 eliminación de medios.
Responsable: Dirección TIC

10.11. Definir en el clausulado para todo tipo de contrato los siguientes requisitos:

a. CONTROL DE PERSONAL de tal forma que se le pueda exigir al proveedor que mantenga informado de cualquier cambio de personal dedicado a la prestación de servicios dentro del acuerdo firmado.
b. CONTROL DE PROCEDIMIENTOS es decir clausulas específicas para que el proveedor mantenga procesos de seguridad, manejo de USO DEL SOFTWARE, GESTION DE INCIDENTES, GESTION DE CAMBIOS y
c. Para todos los contratos por “PRESTACION DE SERVICIOS” en persona natural contemple los requisitos de seguridad de la información y la aplicación de la matriz de riesgos.

Por cuanto la evidencia suministra demuestra un cumplimiento parcial a los controles ID: A.15.1.1 y A.15.1.2
Responsable: Subdirección de Contratación

10.12. Actualizar el Normograma por cuanto las consultas realizadas al inventario en isolucion identificamos que no se tienen registro de documentos como: CONPES 3854 y Ley 1912 de propiedad intelectual, incumpliendo el control Id: A.18.1.1 Identificación de la legislación vigente y los requisitos contractuales.
Responsable: Dirección TIC y Dirección de Planeación Institucional y Calidad

10.13. Fortalecer los mecanismos para dar cumplimiento en su totalidad a la buena práctica de tratamiento de datos personales defiendo: el líder, grupo o comité existente, responsable del tratamiento de datos personales en la entidad y debe existir en el inventario el riesgo orientado a la protección de datos personales el cual debe ser tratado, toda vez que la evidencias presentada no es suficiente para garantizar en su totalidad cumpliendo al control ID: A.18.1.4
Responsable: Dirección TIC

11. CONCLUSIONES.

- Para los objetivos de seguridad de la información es recomendable definir métricas y medir el desempeño de los planes o acciones trazados que dan cumplimiento a cada objetivo, esto con el fin de determinar si los objetivos de seguridad se están cumpliendo.

- Seguir fortaleciendo las campañas de sensibilización a toda la organización para que el lenguaje sea común frente a los diferentes conceptos. Es una tarea continua en el tiempo no se puede descuidar. Estrategias que deben seguir fortaleciéndose son: medios institucionales, cursos virtuales, intranet, correo electrónico y posters ubicados en sitios estratégicos, pantallas digitales, sesiones presenciales entre otros, esto permitirá general cultura de seguridad.

- Seguir realizando ejercicios de auditorías internas de seguridad de la información de manera periódica que permitan seguir evaluando el alcance y cumplimiento de los requisitos de la norma, de esta manera se lograrán preparar a la organización para una posible certificación internacional en el largo plazo.

- Crear el plan de mejoramiento por parte de los responsables de las diferentes dependencias con base a las no conformidades y oportunidades de mejora detectadas. Para ello se debe determinar la causa raíz de cada no conformidad y presentar el plan de mejora que permita mitigación, reducir, evitar o eliminar la no conformidad logrando el cumplimiento total del sistema de gestión de seguridad de la información.

- Medir con base al nivel de relevancia o importancia los indicadores definidos del Sistema de Gestión de Seguridad de la Información que aplicaría para todos procesos de la entidad que generan información y servirán de insumo para la revisión por la Dirección y con ello la toma de decisiones.

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

12. PLAN DE MEJORAMIENTO

ES RESPONSABILIDAD DE LAS DEPENDENCIA ELABORAR EL PLAN DE MEJORAMIENTO ADECUADO QUE ELIMINE LAS NO CONFORMIDADES Y RESPONSA A LAS OPORTUNIDADES DE MEJORA ESPECIFICADAS.

NOTA: DE SER NECESARIO, DEBERAN REALIZAR LAS MESAS DE TRABAJO PARA PARA ABORDAR LAS ACCIONES QUE INVOLUCREN LA INTERACION CON OTRAS DEPENDENCIAS

13. ANEXOS.

LISTA DE VERIFICACION AUDITORIA 27K-2020 SDS vjul final.xlsx

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

FRANCISCO JAVIER PINTO GONZALEZ

APRUEBA JEFE OFICINA DE CONTROL INTERNO,

OLGA LUCIA VARGAS COBOS