

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

INFORME FINAL TRABAJO DE AUDITORÍA
 Auditoria al estado de la Seguridad de la Información con base en la Norma
 ISO27001:2022 y Anexo A

OFICINA DE CONTROL INTERNO

AUDITOR:
LÍDER: FRANCISCO JAVIER PINTO GONZALEZ
 Lead Auditor ISO27001
 CISM | CISA de ISACA
 Líder en Ciberseguridad

REVISADO POR:
 SAIRA ADELINA GUZMAN MARMOLEJO
JEFE OFICINA DE CONTROL INTERNO

Bogotá, septiembre 2026

SECRETARÍA DISTRITAL DE SALUD

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

Contenido

ABREVIATURAS.....	3
INTRODUCCIÓN	4
MARCO CONCEPTUAL.....	4
1. OBJETIVO GENERAL DE LA AUDITORÍA(NIA 2210).....	6
2. OBJETIVOS ESPECÍFICOS DE LA AUDITORÍA (NIA 2210).	6
3. ALCANCE DE LA AUDITORÍA (NIA 2220).	6
4. CRITERIOS DE AUDITORÍA (NIA 2210- A3).....	7
4.1 Internos: (políticas,normatividad interna,procedimientos lineamientos)	7
4.2 Externos(leyes y regulaciones que apliquen)	8
5. METODOLOGÍA UTILIZADA (NIA 2300).	9
6. ANÁLISIS DE INFORMACIÓN Y DE DATOS (NIA 2320).	10
GENERALIDADES	11
COMPONENTE1: EVALUACIÓN NORMA ISO27001:2022.....	12
ANÁLISIS DE NO-CONFORMIDAD DETECTADAS RESPECTO A LA NORMA ISO27001:2022.....	14
COMPONENTE2: EVALUACIÓN DE LA EFECTIVIDAD DE CONTROLES ANEXO-A ...	18
RESULTADOS GENERALES DE LA EVALUACIÓN FRENTE AL ANEXO-A.....	19
ANÁLISIS DE NO-CONFORMIDAD DETECTADAS RESPECTO AL ANEXO-A	24
7. ASPECTOS POSITIVOS (NIA 2410 A2).	32
8. NO CONFORMIDADES (NIA 2431).	33
9. ACCIONES PARA ABORDAR RIESGOS(NIA 2410-A1).	35
10. CONCLUSIONES (NIA 2410-A1).	38
RECOMENDACIONES.	41
11. PLAN DE MEJORAMIENTO (NIA 2500).	43
12. ANEXOS.	43

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

ABREVIATURAS

AZURE: Microsoft Azure Plataforma de servicios de computación en la nube de Microsoft
 BIA: Business Impact Analysis – Análisis de Impacto al Negocio
 CONPES: Consejo Nacional de Política Económica y Social
 DASHBOARD: Tablero de control / Panel de indicadores
 DNDA: Dirección Nacional Derechos de Autor
 DoS: Denial of Service – Denegación de Servicio
 DRP: Disaster Recovery Plan – Plan de Recuperación ante Desastres
 IA: Inteligencia Artificial
 ICONTEC Instituto Colombiano de Normas Técnicas y Certificación
 IDS: Intrusion Detection System – Sistema de Detección de Intrusos
 IPS: Intrusion Prevention System – Sistema de Prevención de Intrusiones
 ISO: Organización Internacional de Normalización
 LAN: Local Area Network – Red de Área Local
 MINTIC: Ministerio de Tecnologías de la información y comunicaciones.
 MIPG: Modelo Integrado de Planeación y Gestión.
 MSPI: Modelo de Seguridad y Privacidad de la Información
 NIA: Norma Internacional de Auditoría
 NIST: Instituto Nacional de Estándares y Tecnología
 OCI: Oficina de control interno
 PHVA: Planear – Hacer – Verificar – Actuar
 PMBOK: Project Management Body of Knowledge - Guía del Project Management Institute (PMI)
 PMO: Project Management Office – Oficina de Gestión de Proyectos
 POGD: Plan operativo de Gestión y Desempeño
 RPO: Recovery Point Objective – Objetivo de Punto de Recuperación
 RTO: Recovery Time Objective – Objetivo de Tiempo de Recuperación
 SCRUM: Marco ágil para gestionar proyectos complejos
 SDS: Secretaría Distrital de Salud
 SEGPLAN: Seguimiento al Plan de Desarrollo Distrital mediante los Proyectos de Inversión
 SI: Seguridad de la Información
 SIEM: Security Information and Event Management - Gestión de incidentes de seguridad
 SOA: Statement of Applicability – Declaración de Aplicabilidad
 SOC: Centro de Operaciones de Seguridad
 WEB: World Wide Web
 ZABBIX: Plataforma de monitoreo de infraestructura TI

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos
--

INTRODUCCION

Las auditorías de gestión es una herramienta estratégica que la Secretaria Distrital de Salud utiliza para conocer el estado de los procesos y sus servicios, focalizada a temas específicos y determinando su eficacia y eficiencia mediante una evaluación objetiva y metódica que resalta las fortalezas y toma decisiones frente a las debilidades identificadas. la auditoría especifica con énfasis en riesgo a la gestión de la seguridad de la información en la SDS que trata esta evaluación, busca detectar o identificar posibles debilidades, desviaciones, errores, falencias existentes permitiendo emprender acciones de mejoramiento adecuadas y oportunas de cara a la obtención de la certificación internacional ISO27001:2022 y alineado a los objetivos institucionales. De acuerdo con lo anterior, la auditoria se realizó bajo una mirada transversal que involucró diferentes dependencias y partes interesadas, además, la evaluación se realizó mediante instrumento de verificación (checklist) elaborado de conformidad con los requisitos de la normatividad y legislación relacionada. En cuanto, a la Resolución 500 de 2021 expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones- MinTIC, establece los lineamientos generales para implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) basado en la norma ISO 27001:2022, la cual deberá ser implementada por las entidades públicas colombianas. La auditoría especifica que se realizó, busca obtener una visión objetiva de qué tan preparada y protegida está la entidad frente a los riesgos de seguridad de la información que la pueden afectar, toda vez que una falla de seguridad o incidente digital materializado puede afectar no solamente la imagen de la entidad, sino también la confianza de los ciudadanos.

MARCO CONCEPTUAL

El Modelo de Seguridad y Privacidad de la Información también conocido como – MPSI liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, imparte los lineamientos para que las entidades públicas implementen y realicen la adopción de buenas prácticas en materia de seguridad de la información, tomando como referencia el estándar internacional ISO27001:2022 y anexo A, 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 2018¹ y su habilitador transversal de seguridad de la información. La planificación, implementación y mejora del Modelo MSPI en la SDS, está determinado por las necesidades de información, objetivos, requisitos de seguridad, el mapa de procesos, estructura jerárquica de la SDS. El objetivo principal de la seguridad de la información en la SDS, consiste en

¹ "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

mantener la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo y brindando confianza a las partes interesadas como es la ciudadanía frente a su información.

En Colombia la normatividad y legislación aplicable al tema de seguridad de la información viene en aumento, generando un compromiso solido por parte del gobierno nacional bajo el liderazgo del Ministerio de las TIC y la alta consejería de las TIC, de impulsar, masificar y lograr la implementación del sistema. A continuación, se relacionan algunos elementos normativos y de legislación que deberán serán adoptados por la entidad como son:

- **Resolución 500 del 2021** *“Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.*
- **Decreto 1008 de 2018** *“Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”*
- **Norma IEC ISO 27001:2022:** Norma principal internacional certificable que establece los requisitos obligatorios para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Dicha norma contiene los requisitos organizados principalmente en los siguientes dominios: Contexto de la organización, Liderazgo, Planificación, Apoyo, Operación, Evaluación del desempeño y Mejora
- **ANEXO-A:** Es un conjunto de 97 Controles de tipo tecnológicos, administrativos, físicos, y de personas, agrupados en 4 dominios que la entidad puede utilizar para tratar los riesgos identificados dentro de su Sistema de Gestión de Seguridad de la Información (SGSI).
- **Norma IEC ISO 31000:2018 e ISO 27005:2022:** Permite el análisis y la gestión de Riesgos de Seguridad de la información. La metodología actual en la SDS se redefinió con base a las buenas prácticas del DAFP.
- **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.
- **Ley 1273 de 2009²** - Delitos informáticos o de la protección de la información y de los datos. Su propósito es proteger la información, los datos y los sistemas que utilizan tecnologías de información y comunicaciones. La norma se encuentra vigente y

² *“Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”*

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

protege principalmente: Confidencialidad de la información, Integridad de los datos, disponibilidad de los sistemas y datos informáticos, datos personales, sistemas informáticos y redes de telecomunicaciones.

- **Ley 1581 del 2012³, protección y tratamiento de datos personales:** Busca garantizar que el tratamiento de los datos personales se realice respetando los derechos de los titulares y aplicando medidas que protejan la información contra: Acceso no autorizado, pérdida, alteración o adulteración, uso indebido, divulgación no autorizada y tratamiento fraudulento. La entidad debe recolectar y administrar la información de ciudadanos, funcionarios, contratistas, proveedores o usuarios de servicios y debe establecer mecanismos para garantizar la protección de esos datos.

1. OBJETIVO GENERAL DE LA AUDITORÍA (NIA 2210)

Determinar el estado de avance en la implementación del modelo de seguridad de la información con base en las buenas prácticas Norma Certificable ISO 27001:2022 y Anexo A.

Nota aclaratoria: Teniendo en cuenta que la evaluación se realizará con base en la Norma Certificable ISO 27001:2022 y su Anexo A, no serán objeto de verificación los componentes de control del MECI: Ambiente de Control, Actividades de Control, Gestión del Riesgo, Actividades de Monitoreo e Información y Comunicación considerando la especificidad y extensión que requiere la presente auditoría.

2. OBJETIVOS ESPECÍFICOS DE LA AUDITORÍA (NIA 2210)

- Evaluar el estado de la seguridad de la información conforme a los requisitos establecidos de la norma ISO27001:2022 y Anexo A
- Generar confianza en las partes interesadas (internos y externos) respecto a la seguridad de la información en los servicios que presta la entidad.
- Evaluar la eficacia y suficiencia de los controles, la gestión de los riesgos y la capacidad para proteger los activos de información.
- Identificar las desviaciones o debilidades que puedan existir y generar las medidas preventivas y correctivas necesarias.

3. ALCANCE DE LA AUDITORÍA (NIA 2220)

Contemplo la evaluación de los requisitos para el establecimiento del Sistema de Seguridad de la información con base en la Norma ISO27001:2022 y Anexo A.

Nota: Teniendo en cuenta el resultado de la preauditoría al sistema de seguridad de la información realizada por la empresa ICONTEC en junio 2026, los diferentes hallazgos, y

³ “Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011. Ver Decreto 255 de 2022”.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

no-conformidades detectadas de los diferentes requisitos evaluados por el ente externo; se precisa que no harán parte del alcance de la presente auditoría interna, toda vez que los procesos se encuentran adelantando la implementación de las acciones respectivas. Así mismo, los hallazgos evidenciados como resultado de la auditoría interna realizada al Sistema de Seguridad de la Información en la vigencia 2025 y frente a los cuales se están adelantando las acciones, no serán objeto de la presente auditoría. De igual manera las exclusiones realizadas en la declaración de aplicabilidad -SOA año 2026, no serán objeto de la evaluación contenida dentro del alcance del Plan.

Periodo a evaluar:

- Desde: 1/08/2025
- Hasta: 31/07/2026

Al ser un ejercicio de evaluación transversal, se tuvieron en cuenta los siguientes procesos:

- Desarrollo y fortalecimiento organizacional
- Gestión de TIC.
- Gestión de bienes y servicios
- Gestión del talento humano
- Gestión de comunicaciones
- Gestión Jurídica
- Control disciplinario
- Gestión de urgencias, emergencias y desastres
- Otros procesos misiones y estratégicos

4. CRITERIOS DE AUDITORÍA (NIA 2210- A3)

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

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

Políticas:

- Seguridad de la información bajo la Resolución 705 del 11 de julio del 2025
- MANUAL GENERAL DE POLÍTICAS DE OPERACIÓN DE SEGURIDAD DE LA INFORMACIÓN - SDS-DFO-MN-006
- SDS-DFO-POL-001 POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION
- SDS-DFO-PL-002 Plan de Seguridad y Privacidad de la Información y Protección de Datos Personales
- SDS-DFO-PL-001 Plan Tratamiento de Riesgos de Seguridad de la Información

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

Lineamiento

- SDS-DFO-LN-014 LINEAMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Manuales

- SDS-DFO-MN-004 MANUAL DE ROLES, RESPONSABILIDADES Y AUTORIDADES · SGSI
- SDS-DFO-MN-005 MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
- SDS-DFO-MN-006 MANUAL GENERAL DE POLÍTICAS DE OPERACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Procedimientos de operación aplicables:

- SDS-TIC-PR-005 SEGURIDAD INFORMÁTICA
- SDS-TIC-PR-002 GESTIÓN DE INCIDENTES Y REQUERIMIENTOS
- SDS-TIC-PR-001 GESTIÓN SOLUCIONES DE SOFTWARE
- SDS-DFO-PR-004 - GESTIÓN DEL RIESGO EN LA SDS

Instructivos:

- SDS-TIC-001 - GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA
- SDS-TIC-LN-014 - GESTIÓN DE BACKUP Y RESTAURACIÓN DE INFORMACIÓN
- SDS-TIC-LN-016 DESARROLLO SEGURO
- SDS-TIC-INS-004 - CONTROL DE CAMBIOS
- SDS-TIC-GUI-008 - ESTÁNDARES DE DESARROLLO DE SOFTWARE EN LA SDS

Algunos formatos utilizados:

- SDS-TIC-FT-054 - ACTA BORRADO SEGURO DE LA INFORMACIÓN
- SDS-TIC-FT-014 - FORMATO DE TRANSFERENCIA DE INFORMACIÓN
- SDS-TIC-FT-064 - GUIA DE RECUPERACIÓN DEL DRPT
- SDS-DFO-FT-039 - Declaración-de-Aplicabilidad_SGSI_2025
- SDS-DFO-FT-035 - MAPA DE RIESGOS PARA SEGURIDAD DE LA INFORMACIÓN
- SDS-DFO-FT-038 - Inventario-Actividades-Tiempos-Recursos_BIA
- SDS-DFO-FT-041 INVENTARIO DE ACTIVOS DE INFORMACIÓN, SOFTWARE, HARDWARE Y SERVICIOS

4.2 Externos (leyes y regulaciones que apliquen)

- Norma IEC ISO 27001:2022 y Anexo A
- Norma IEC ISO 31000:2018 y 27005 para Gestión de Riesgos de SI
- Norma IEC ISO 22301:2012 Continuidad de Negocio.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

- Decreto 1008 de 2018 - Política de Gobierno Digital, habilitadores transversales SI
- Decreto 1499 de 2017 – MIPG
- CONPES 3854 del 2016 - Política Nacional de Seguridad Digital
- CONPES 3975 de 2019 - Política de transformación digital e IA
- CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital
- Ley 23 de 1982 Derechos de autor
- Ley 44 de 1993 Modifica y adiciona la Ley 23 de 1982
- Ley 1273 de 2009 - Delitos informáticos
- Ley 1581 del 2012 protección y tratamiento de datos personales
- Ley 1915 de 2018 Derechos de autor y derechos conexos
- Decreto 338 de 2022 Gobernanza de seguridad digital
- Decreto 767 de 2022 Política de Gobierno Digital
- Decreto 1078 de 2015 Sector TIC
- Decreto 1360 de 1989 Protección del software
- Resolución 500 del 2021 del MinTIC - Lineamiento para implementar MPSI
- Resolución MinTIC 746 de 2022 Fortalecimiento del MSPi
- Resolución MinTIC 1519 de 2020 Seguridad digital y publicación de información
- Decisión Andina 351 de 1993 Régimen común de Derecho de Autor y Derechos Conexos
- Entre otras

Se puntualiza que el ejercicio auditor fue basado metodológicamente en listas de chequeo de los requisitos de la norma ISO27001:2022 y controles del anexo A para este propósito.

5. METODOLOGÍA UTILIZADA (NIA 2300)

La presente auditoría se desarrolló mediante mesas de trabajo virtuales y presenciales con los diferentes referentes y participantes designados, verificando y constatando la conformidad de los requisitos normativos establecidos mediante lista de verificación elaborada, las verificaciones en campo se tomaron en casos aleatorios y análisis de la información referente a los procedimientos establecidos, se solicitaron 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 visitas a las instalaciones de la sede administrativa pisos 1, 6 y 7, porterías, acceso a los parqueaderos y áreas sensibles, edificios del DUES y HEMOCENTRO, con el objetivo de verificar o constatar la eficacia de los controles físicos y tecnológicos dispuestos del anexo A.
- **Revisión de la documentación de seguridad de la información:** El auditor solicitó y revisó la documentación existente y en proceso de elaboración (borradores) relacionada con la gestión de la seguridad de la información, entre los documentos

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos
--

- consultados se encuentran: política general de seguridad de la información, manual de política de operación de la seguridad de la información, procedimientos, manuales, guías, formatos, registros de actas de reunión, registros de asistencia, entre otros.
- Consultas con el personal designado:** El auditor realizó consultas específicas a los funcionarios designados para cada uno de los procesos en la entidad y se solicitaron algunas piezas comunicativas elaboradas y desplegadas para el periodo de la evaluación, esto con el fin de determinar el nivel de concientización frente a la seguridad de la información aplicada en la entidad. Por último y no menos importante, con algunas personas participantes convocadas en las diferentes mesas de trabajo en la cual participaron representantes de los diferentes procesos, se realizó un sondeo frente al conocimiento de la política y los objetivos de seguridad, se preguntó de qué trata y su ubicación de acuerdo a la publicación de acuerdo las jornadas de concientización realizados.
 - Listados de verificación para los auditados:** El auditor entrega de manera anticipada la lista de requisitos de revisión, la cual se trabajó en compañía de los referentes designados y personal que acompañó el ejercicio. Estos listados serán una imagen cualitativa del estado de la seguridad de la información de la entidad respecto a la norma ISO 27001:2022 y el ANEXO-A.

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

La presente auditoría, se llevó a cabo mediante recolección de información como resultado de las diferentes mesas de trabajo realizadas, acompañadas de listas de chequeo para lo cual se realizó la verificación de diferentes elementos: políticas, lineamientos, guías, matriz de riesgos, formatos, modelos, documentos e instrumentos varios, entre otros, que permitieron conocer los procedimientos y las prácticas utilizadas para mantener la seguridad de la información en la SDS. En cuanto a los resultados de la evaluación, estos fueron analizados y consolidados, con el fin de determinar posibles desviaciones, debilidades o falencias, evidenciando las causas que las originan y proponiendo alternativas que permitan mitigarlos, dichos resultados serán presentados a lo largo del presente informe.

Es importante precisar que la evaluación se basó en la norma actualizada ISO27001:2022 o componente certificable, el cual contempla el ciclo de vida PHVA del sistema, así mismo, se evaluó el ANEXO-A, en su conjunto de controles de tipo tecnológicos, administrativos, físicos, y de personas, agrupados en 4 dominios que la entidad debe utilizar para tratar los riesgos identificados dentro de su Sistema de Gestión de Seguridad de la Información (SGSI), todos los elementos descritos hacen parte del instrumento de autoevaluación y permitieron conocer el nivel de avance en la implementación del modelo de seguridad de la información.

Finalmente, y como resultado de la preauditoria al sistema de seguridad de la información realizada por la empresa ICONTEC el pasado mes de junio 2026 y con miras a obtención de la certificación internacional, los diferentes hallazgos, y no-conformidades detectadas de

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

los diferentes requisitos evaluados por el ente externo, no hicieron parte del alcance de la presente evaluación, toda vez que los procesos se encuentran adelantando la implementación de las mismas. Así mismo, los hallazgos evidenciados como resultado de la auditoría interna realizada al Sistema de Seguridad de la Información en la vigencia 2025 y frente a los cuales se están adelantando las acciones, no serán objeto de evaluación, al igual que las exclusiones realizadas en la declaración de aplicabilidad -SOA año 2026, no serán objeto de evaluación.

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

GENERALIDADES

El ejercicio se basó en lista de chequeo y contempló la evaluación de 22 requisitos de la Norma ISO27001:2022 y 79 requisitos del ANEXO-A.

Nota: El detalle de la evaluación de cada uno de los requisitos y controles del ANEXO-A hace parte de los papeles de trabajo utilizados en cada una de las mesas de trabajo realizadas, así mismo se cuenta con las grabaciones que soportan el ejercicio con evidencia digital. A continuación, mediante tablas agrupadas, se presentan los resultados obtenidos de la evaluación realizada de conformidad con el alcance establecido.

Convenciones de la tabla: Color Verde: Cumple, Color Rojo: No cumple, Color Café: Acción para abordar Riesgo y Color Amarillo: No Evaluado

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos

COMPONENTE1: EVALUACIÓN NORMA ISO27001:2022

Dominios y componentes de la Norma	REQUISITOS A EVALUAR	CUMPLE:	NO CUMPLE:	ACC. ABORDA R RIESGO	REQUISITO NO EVALUADO
4 Contexto de la Organización	4	3		1	1
4.1 Comprender la organización y su contexto					1
4.2 Comprender las necesidades y expectativas de las partes interesadas	1			1	
4.3 Determinar el alcance del sistema de gestión de la seguridad de la información	2	2			
4.4 Sistema de gestión de la seguridad de la información	1	1			
5 Liderazgo	3	2		1	
5.1 Liderazgo y compromiso	1	1			
5.2 Política	1	1			
5.3 Roles organizacionales, responsabilidades y autoridades	1			1	
6 Planificación	2	2			2
6.1 Acciones para abordar los riesgos y las oportunidades6.1.1 Generalidades	1	1			
6.1.2 Valoración de riesgo de la seguridad de la información	1	1			
6.1.3 Tratamiento de riesgo de la seguridad de la información					1
6.2 Objetivos de seguridad de la información y planificación para lograrlos					1
7 Apoyo	7	7			
7.1 Recursos	1	1			
7.2 Competencias	1	1			
7.3 Toma de Conciencia	1	1			
7.4 Comunicación	1	1			
7.5 Información documentada	3	3			
8 Operación	3	2	1		
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	1		1		2
9.1 Seguimiento, medición, análisis y evaluación	1		1		
9.2 Auditoría interna					1
9.3 Revisión por la dirección					1
10 Mejora	2	2			
10.1 No conformidades y acciones correctivas	1	1			
10.2 Mejora continua	1	1			
Total general	22	18	2	2	5

Tabla1: Evaluación Norma Certificable ISO27001:2022

La Tabla1, resume el resultado de la evaluación realizada de cara a los 7 dominios de la norma ISO27001:2022, la cual consta de 27 requisitos de estructura general, sin embargo, teniendo en cuenta el alcance definido, solo 22 requisitos se evaluaron y encontramos que: 18 requisitos que equivalen al 81,8% **“Cumplen”**, 2 requisitos que equivalen al 9% que requieren una **“Acción para Abordar Riesgo”**, mientras que 2 de los requisitos que equivalen al 9% **“No Cumplen”**, para los cuales se decreta una no-conformidad y requerirá de una acción correctiva inmediata.

Nota: Es importante precisar que 5 requisitos especificados en la tabla no fueron objeto de evaluación, toda vez que resultado de la preauditoría realizada, presentan una no-conformidad decretada y se encuentra en curso de la corrección.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2026	Planificación	Contexto de la organización	11%	14%
		Liderazgo	12%	14%
		Planificación	14%	14%
		Soporte	14%	14%
	Implementación	Operación	14%	16%
	Evaluación de Desempeño	Evaluación del desempeño	8%	14%
	Mejora Continua	Mejora	14%	14%
TOTAL			88%	100%

Tabla2: Estado de avance actual implementación Norma ISO27001:2022

La tabla2, permite presentar en paralelo los resultados en términos porcentuales del avance actual vs el porcentaje deseado del sistema, haciendo uso del instrumento de autoevaluación MPSI proporcionado por el MintIC, dicha tabla permite mostrar el AVANCE DEL CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA) en términos porcentuales, para lo cual será indispensable por parte del líder de implementación del modelo, atender las brechas identificadas que corresponden a requisitos incumplidos y que se detallaran en el presente informe, esto con el fin de subsanar las brechas (diferencias) y lograr en el corto plazo el cumplimiento de cada uno de los requisitos. A partir del capítulo denominado **ANÁLISIS DE NO-CONFORMIDAD DETECTADAS RESPECTO A LA NORMA ISO27001:2022**, se detallan los diferentes hallazgos representados en (No-conformidades) que surgieron como resultado de la evaluación realizada y que será necesario que los diferentes responsables del SGSI tomen los correctivos necesarios para subsanar y lograr que la entidad certifique su sistema.

Para conocimiento del lector, en la tabla que se relaciona a mano derecha, se listan las 5 no-conformidades identificadas como resultado de la preauditoria realizada por ICONTEC y que no fueron objeto de evaluación dado el antecedente.	DOMINIO 4 Contexto de la Organización	CODIGO 4.1 Comprender organización y su contexto
	6 Planificación	6.1.3 Tratamiento de riesgo de la seguridad de la información
	6 Planificación	6.2 Objetivos de seguridad de la información y planificación para lograrlos
	9 Evaluación de desempeño	9.2 Auditoría interna
	9 Evaluación de desempeño	9.3 Revisión por la dirección

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos
--

ANÁLISIS DE NO-CONFORMIDAD DETECTADAS RESPECTO A LA NORMA ISO27001:2022

Hallazgo 1	
<i>Dominio</i>	4. CONTEXTO DE LA ORGANIZACIÓN
<i>Requisito</i>	4.2 Comprender las necesidades y expectativas de las partes interesadas La entidad debe determinar: a) las partes interesadas b) los requisitos de estas partes interesadas que sean pertinentes para el SGSI
<i>Dependencia Auditada:</i>	Dirección de Planeación Institucional y Calidad
<i>Resultado de la evaluación</i>	En mesa de trabajo realizada, se suministra el documento denominado: “PARTES INTERESADAS 2026_SGSI.xlsx en versión 2 como última fecha de actualización registrado en el control de cambio del documento del 26 de marzo de 2026. Al consultar dicho documento, se observa que se contemplaron las necesidades de las partes interesadas frente a la seguridad de la información. Al particular, se informa que cada dependencia determina las necesidades puntuales de seguridad de la información que considera y posteriormente estas necesidades se agrupan para generar la actualización del instrumento. Al consultar, se logran identificar 10 partes interesadas directamente asociadas, no obstante, se identifica que, partes interesadas como la DIRECCIÓN DE PLANEACION INSTITUCIONAL Y CALIDAD, TALENTO HUMANO, BIENES Y SERVICIOS, OFICINA DE ASUNTOS JURÍDICOS (OAJ), ASUNTOS DISCIPLINARIOS, no hacen parte de dicho instrumento, lo cual no es consistente, toda vez que la entidad debe identificar todas las partes interesadas relevantes para el SGSI, sus requisitos relevantes y como estos requisitos pueden incluir obligaciones legales, regulatorias y contractuales que no están siendo tenidos en cuenta. Por consiguiente, dicha situación, constituye una no conformidad, ya que la entidad no ha identificado a la fecha todas las partes interesadas relevantes para el Sistema de Gestión de Seguridad de la Información (SGSI), y con ellos los requisitos relevantes en materia de seguridad de la información de estas dependencias. Evidencia: - La matriz de partes interesadas no contempla dependencias o áreas de la entidad relevante en la implementación de controles de tipo tecnológicos, físicos, de personas y organizacional. - No se identifican los requisitos de seguridad de la información asociados a estas partes interesadas. Por último, si el objetivo estratégico de la Dirección de Planeación Institucional y Calidad consisten en el corto plazo llevar a la entidad a Certificar su SGSI, es obligatorio cumplir con el requisito en su totalidad. De acuerdo con lo anterior y con base en reunión de cierre, se reclasifica y se emite una acción para abordar riesgo con respecto al requisito 4.2 de la norma y se deberán aplicar las acciones de mejora que haya lugar.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

Hallazgo 2

Dominio	5 liderazgo
Requisito	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. Y Control 5.2 Anexo-A Roles y responsabilidades de la seguridad de la información
Dependencia Auditada:	Dirección de Planeación Institucional y Calidad
Resultado de la evaluación	Al particular, se informa que se emitió la Política General de Seguridad de la información a partir de la Resolución 705 del 11 de julio del 2025, dicha política fue aprobada en el comité institucional de gestión y desempeño y se cuenta con el acta de reunión donde se dio la aprobación de la política general. La política resuelve varios puntos: Declaración, objetivos, alcance, compromiso de la alta dirección, aplicabilidad y en su artículo Artículo #6, define los Roles y Responsabilidades, de otra parte, se cuenta con el documento denominado: 28_25_Manual_Roles_Responsabilidades_2026.xlsx por medio del cual se definen mediante la tabla #7 la Matriz de roles y responsabilidades del SGSI, sin embargo, se identifica que, el rol y las responsabilidades que ejerce la subdirección de bienes y servicios frente a los controles físicos no está definida, el Rol y las responsabilidades que ejerce el COMITÉ INSTITUCIONAL DE GESTION Y DESEMPEÑO frente al Sistema tampoco está definida, así como el ROL de Gestión de Riesgos del SI y Protección de Datos/Privacidad. Por último, e igual de importante es que la entidad no ha <u>asignado y comunicado de manera formal y particular</u> las responsabilidades y autoridades a cada una de las personas que ejercen los diferentes roles. Durante la auditoría y basado en los documentos suministrados, se identificó que: 1. Los funcionarios desconocen quién tiene autoridad para tomar decisiones de seguridad. 2. No están definidas las responsabilidades de seguridad de información de las diferentes áreas. 3. No existe evidencia de comunicación individual de roles y responsabilidades, por lo cual las personas asignadas desconocen su responsabilidad frente al sistema. Finalmente, si el objetivo estratégico de la Dirección de Planeación Institucional y Calidad consisten en el corto plazo llevar a la entidad a certificar su SGSI, es obligatorio cumplir con el requisito en su totalidad. De acuerdo con lo anterior y con base en reunión de cierre, se reclasifica y se emite una acción para abordar riesgo con respecto al requisito 5.3 de la norma y se deberán aplicar las acciones de mejora que haya lugar.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

Hallazgo 3	
Dominio	8. OPERACIÓN
Requisito	8.1 Planificación y Control operacional: La organización debe <u>planificar, implementar y controlar</u> los procesos necesarios para cumplir con los requisitos de seguridad de la información y para implementar las acciones definidas en el numeral 6.1. La organización además <u>debe implementar los planes</u> para lograr los objetivos de seguridad de la información, definidos en el numeral 6.2
Dependencia Auditada:	Dirección de Planeación Institucional y Calidad
Resultado de la evaluación	De acuerdo con la política seguridad de la información formalizada mediante la resolución 705 del 25 julio, y en la cual se establece en el artículo #2, 6 objetivos de seguridad, se informa que dichos indicadores serán medidos a partir de 11 indicadores establecidos. En lo que respecta a los planes y su implementación, se solicitaron en mesa los siguientes documentos: 1. Plan de seguridad y privacidad de la información año 2026- SDS-DFO-PL-002 2. Plan de tratamiento de riesgos de seguridad de la información año 2026 - SDS-DFO-PL-001 3. Cronograma de actividades y entregables en cada una de las etapas trazadas 4. Cronograma específico de cara a la auditoria de certificación 2026 y 5. Por último, los 9 productos o entregables en cada etapa del plan de seguridad de la información para corroborar el estado de avance del año 2026. Al consultar el documento denominado: “6_5_pag22_PlandeSeguridadyPrivacidaddelainformacin_ SDS-DFO-PL 001”, establece 9 macro actividades, sin embargo, el plan desglosa las siguientes subactividades: 6.1.9.2 Simulacro de incidentes de seguridad de la información, no obstante, la subactividad orientada a la realización de “simulacros de incidentes”, programada para el mes de mayo a junio del 2026, se informa que dicha actividad al momento de la auditoria no pudo ser realizada. La macro actividad de “fortalecimiento de SIEM/DLP/CSPM, DPIA en procesos críticos, Simulacros de incidentes, no presento entregables al respecto. Lo que se refiere a la Política de Tratamiento de datos personales, esta se encuentra en borrador, pero a la fecha de la presente evaluación, no ha sido aprobada, no se ha definido un responsable. Por último, el entregable es un documento de Política de Criptografía y Gestión de Claves (TLS/KMS/HSM), que a la fecha no define las directrices y reglas que dan respuesta a dicho control del Anexo. Así mismo, el numeral 6.1.11. Estrategia de Monitoreo, Respuesta y Aprendizaje, se informa que solo se tiene reportado un único incidente frente al Activo de información SIDCRUE del primer trimestre del 2026, no obstante, llevar a cabo el “aprendizaje” de los incidentes, aun no se cuenta con evidencias al respecto. A la fecha de la presente evaluación, se evidenció que: 1. Falta de evidencia documentada que permita demostrar la ejecución de las subactividades. Aun no se han implementado todas las actividades definidas, ya que no se dispone de evidencia suficiente que permita demostrar que las actividades con corte a agosto 2026, se ejecutaron conforme a lo planificado. 2. El plan, no contempla criterios de frecuencia y responsables. 3. Actividades del SGSI realizadas de manera informal y sin registros. 4. Existen diferencias reportadas entre lo planificado y lo realmente ejecutado en el instrumento POGD y

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <u>SECRETARÍA DE SALUD</u>	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

5. Falta de medición frente al cumplimiento de los objetivos de seguridad.

De acuerdo con todo lo anterior, se declara la no-conformidad con respecto al requisito 8.1 de la norma y se deberá aplicar la acción correctiva inmediata. Si el objetivo estratégico de la Dirección de Planeación Institucional y Calidad consiste en llevar a la entidad a certificar su SGSI, es obligatorio cumplir con el requisito en su totalidad.

Hallazgo 4	
Dominio	9. EVALUACIÓN DE DESEMPEÑO 9.1 Seguimiento, medición, análisis y evaluación La entidad debe evaluar el desempeño de la seguridad de la información y la efectividad del SGSI y debe determinar:
Controles	a) a qué es necesario hacer seguimiento y que es necesario medir, incluidos los procesos y controles de la seguridad de la información; b) los métodos de seguimiento, medición, análisis y evaluación, según corresponda, para asegurar resultados válidos; c) cuando se deben llevar a cabo el seguimiento y la medición; d) quien debe llevar a cabo el seguimiento y la medición; e) cuando se deben analizar y evaluar los resultados del seguimiento y de la medición; y f) quien debe analizar y evaluar estos resultados. La organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.
Dependencia Auditada:	Dirección de Planeación Institucional y Calidad
Resultado de la evaluación	Al particular, existe: - Un DASHBOARD de indicadores por proceso, por Familias, o Políticas específicos a la Seguridad de la información. - Se cuenta con la herramienta POGD que permite medir el avance de la META y Actividades y subactividades tendientes al plan de seguridad de la información. - Y, por último, se cuenta 11 fichas de indicadores formulados para el SGSI. Al consultar los resultados se identifica lo siguiente: - En el DASHBOARD se encuentran implementados algunos indicadores que dan respuesta a la política de seguridad digital, no obstante, la última medición consultada fue realizada el día 30 junio de 2026 y varios de estos indicadores no presentan resultados, indicadores como: DRP, tiempos de respuesta y medición de incidentes, aun no presentan resultados y entregables. - Al consultar el porcentaje de avance del plan de seguridad de la información en el instrumento POGD en la meta3, reporta 100%, lo cual no es consistente, toda vez que varios entregables del plan de seguridad de la información como es el caso del fortalecimiento de SIEM/DLP/CSPM, DPIA en procesos críticos, simulacros de incidentes, no presenta entregables al respecto. Así mismo, lo que se refiere a la Política de Tratamiento de datos personales, la cual se encuentra en documento borrador, pero a la fecha de la presente evaluación, no ha sido aprobada y aun no se ha definido un responsable. - Y, por último, de los 11 indicadores definidos para el SGSI bajo el formato Excel denominado: Matriz de indicadores.xlsx, aun no presentan resultados consolidados que permitan determinar el desempeño del Sistema.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz / Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos

Hallazgos generales:

1. La entidad no ha implementado de manera eficaz el mecanismo para el seguimiento, medición, análisis y evaluación del desempeño y de la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI). No se encuentran definidos los métodos de medición, periodicidad, los responsables de realizar las mediciones y de analizar y evaluar sus resultados. Así mismo, no se evidencian registros suficientes que demuestren el análisis y evaluación de los resultados obtenidos.
2. No se tienen relacionados los 11 indicadores definidos para evaluar cada uno de los objetivos del SGSI.
3. Se han recopilado, analizado y evaluado los datos actuales.
4. Los indicadores no tienen metas, criterios o parámetros de evaluación.
5. No existen informes periódicos de desempeño del SGSI.
6. No se conserva evidencia de los resultados.
7. Y, por último, no se han presentado los resultados de los 11 indicadores a la alta dirección.

De acuerdo con todo lo anterior, se declara la no-conformidad con respecto al requisito 9.1 de la norma y se deberá aplicar la acción correctiva inmediata. Si el objetivo estratégico de la Dirección de Planeación Institucional y Calidad consiste en llevar a la entidad a certificar su SGSI, es obligatorio cumplir con el requisito en su totalidad.

COMPONENTE2: EVALUACIÓN DE LA EFECTIVIDAD DE CONTROLES ANEXO-A

El ejercicio contemplo la verificación de un conjunto de 79 controles de 93 definidos en el ANEXO-A y el SOA, los cuales se encuentran agrupados en 4 dominios como se presenta en la tabla que se muestra a continuación. Sin embargo, es importante precisar que 14 controles especificados del ANEXO no hicieron parte de la evaluación, toda vez que del resultado de la preauditoría realizada por el proveedor ICONTEC el pasado mes de julio 2026, sobres estos 14 controles se decretaron las no-conformidades y a la fecha se encuentra en curso la corrección.

No.	Evaluación de Efectividad de controles			Nivel de Madurez
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	CONTROLES ORGANIZACIONALES	90	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	95	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	89	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	89	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		91	100	OPTIMIZADO

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

Tabla3: Resultado General de Evaluación de Controles

Con respecto a la tabla3, se utilizó el instrumento de autoevaluación del MinTIC el cual es de uso público, abierto y permitió obtener el porcentaje general de implementación de controles que a la fecha es del 91%. De acuerdo con lo anterior, existe una brecha del 9%, para la cual se deberán emprender las acciones inmediatas y de mejora que permitan lograr la completitud de los controles en concordancia con la Declaración de Aplicabilidad-SOA. Por último, es importante mencionar que para que un control se considere efectivo, no basta con verificar que solo se encuentre documentado, es necesario determinar y demostrar que se encuentre implementado, funcione y sea eficaz para tratar los riesgos identificados. Con base en estos criterios expuestos, se basó la presente evaluación.

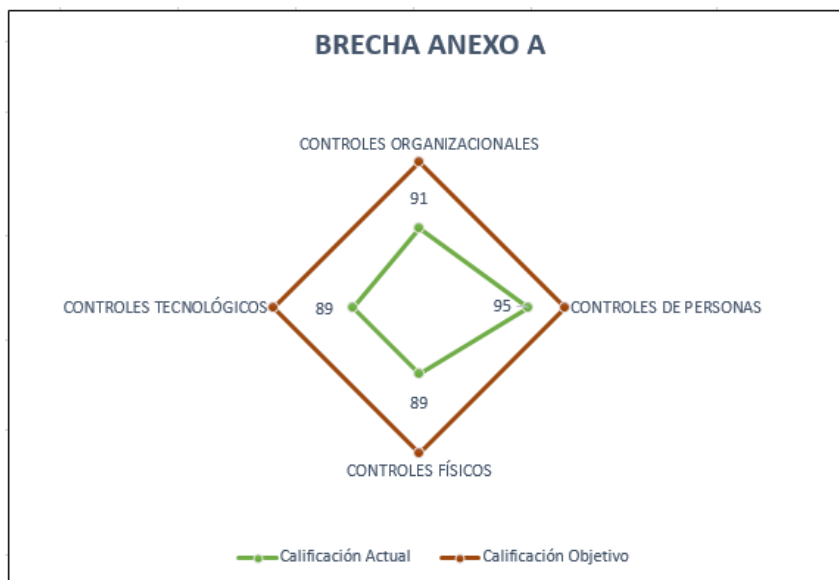


Imagen1: Resultado General de Brechas identificadas

RESULTADOS GENERALES DE LA EVALUACIÓN FRENTE AL ANEXO-A

A continuación, mediante tabla general se presenta de manera consolidada el resultado de los 4 dominios así:

	CONTROLES A EVALUAR	CUMPLEN	NO CUMPLEN	ACCION ABORDAR RIESGO	CONTROL NO EVALUADO
Dominios Anexo A					
Control de Personas	7	7			1
Controles Físicos	13	10	1	2	1
Controles Organizacionales	33	29	1	3	4
Controles Tecnológicos	26	25	1	1	8
Total general	79	71	2	6	14

Tabla4: Agrupación x dominios del Anexo A

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos
--

La tabla4, resume la evaluación realizada frente al conjunto de controles de seguridad de la información del ANEXO A, el alcance de la evaluación comprendió la selección de 79 controles de 93 agrupados en 4 dominios. Al observar la tabla, podemos determinar que, 71 controles equivalente 89,9% del universo evaluado **“Cumplen”**, 6 controles equivalente 8,45% del universo evaluado conllevan una **“Acción para Abordar Riesgo”**, mientras que 2 de los controles equivalentes al 2,53% **“no cumplen”** para los cuales se decreta una no-conformidad y requerirá de una acción correctiva inmediata. A partir del capítulo denominado **ANÁLISIS DE NO-CONFORMIDAD DETECTADAS RESPECTO AL ANEXO-A**, realizaremos el análisis detallado con respecto a los diferentes hallazgos representados en (No-conformidades y acciones para abordar riesgos) que surgieron como resultado de la evaluación realizada a cada control y que será necesario que los diferentes responsables del SGSI tomen los correctivos necesarios para subsanar y lograr que la entidad certifique su sistema.

Nota: Es importante precisar que 14 controles especificados en la tabla, fueron descartados de la evaluación, toda vez que ya fueron evaluados en la preauditoría realizada recientemente por el proveedor ICONTEC y sobre estos se decretaron las 14 no-conformidades.

A continuación, mediante tablas se presentan los resultados de la evaluación por cada Dominio y el estado de cada uno de los controles:

Dominios Anezo A	CONTROLES A EVALUAR	CUMPLEN	NO CUMPLEN	ACCION ABORDAR RIESGO	CONTROL NO EVALUADO
Control de Personas	7	7			1
6.1	1	1			
6.2					1
6.3	1	1			
6.4	1	1			
6.5	1	1			
6.6	1	1			
6.7	1	1			
6.8	1	1			

Tabla5: Resultado de Dominio de Control de Personas

La tabla5, corresponde al listado de controles seleccionados de dominio de **“Control de Personas”**, para lo cual se realizó la evaluación de 7 controles y como resultado se valida que los mismos 7 **“Cumplen”**.

Nota: Es importante precisar que un (1) control especificado en la tabla, fue descartado de la evaluación, toda vez que ya fue evaluado en la preauditoría realizada recientemente por el proveedor ICONTEC y que sobre este se decretó una no-conformidad.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos

Dominios Anexo A	CONTROLES A EVALUAR	CUMPLEN	NO CUMPLEN	ACCION ABORDAR RIESGO	CONTROL NO EVALUADO
Controles Físicos	13	10	1	2	1
7.12	1	1			
7.13	1	1			
7.14	1			1	
7.2	1			1	
7.3	1		1		
7.4	1	1			
7.5	1	1			
7.6	1	1			
7.7					1
7.8	1	1			
7.9	1	1			

Tabla6: Resultado de Dominio de Controles Físicos

La tabla6, corresponde al listado de controles seleccionados de dominio de “**Controles Físicos**”, para lo cual se evaluaron 13 controles y se determina que 10 “**Cumplen**”, 2 controles requieren una “**Acción para abordar riesgos**”, mientras que 1 de los controles “**no cumple**”, lo que deriva en una no-conformidad y requerirá de una acción correctiva inmediata. En el desarrollo del informe, se detallan cada uno de las no-conformidades y Acciones para Abordar Riesgos identificadas.

Nota: Es importante precisar que un (1) control especificado en la tabla, fue descartado de la evaluación, toda vez que ya fue evaluado en la preauditoría realizada recientemente por el proveedor ICONTEC y que sobre este se decretó la no-conformidad.

Dominios Anexo A	CONTROLES A EVALUAR	CUMPLEN	NO CUMPLEN	ACCION ABORDAR RIESGO	CONTROL NO EVALUADO
Controles Organizacionales	33	29	1	3	4
5.1	1	1			
5.10	1	1			
5.11	1	1			
5.12	1	1			
5.13					1
5.14	1	1			
5.15	1	1			
5.16	1	1			
5.17					1
5.18	1	1			
5.19	1	1			
5.2	1			1	
5.20	1	1			
5.21	1	1			
5.22	1	1			
5.23	1	1			
5.24	1	1			
5.25	1	1			
5.26	1	1			
5.27	1	1			
5.28	1	1			
5.29	1	1			
5.3	1	1			
5.30					1
5.31	1			1	
5.32	1			1	
5.33	1	1			
5.34					1
5.35	1	1			
5.36	1	1			
5.37	1	1			
5.4	1	1			
5.5	1	1			
5.6	1	1			
5.7	1	1			
5.8	1		1		
5.9	1	1			

Tabla7: Resultado de Dominio de Controles Organizacionales)

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos
--

La tabla7, corresponde al listado de controles seleccionados del dominio de “**Controles Organizacionales**”, para lo cual se evaluaron 33 controles, de cuales se determinó que 29 “**Cumplen**”, 3 controles requieren emprender una “**Acción para Abordar Riesgo**”, mientras que 1 de los controles “**no cumple**” lo que deriva en una no-conformidad y requerirá de una acción correctiva inmediata. En el desarrollo del informe, se detallan cada uno de las no-conformidades y acción para abordar riesgo identificadas.

Nota: Es importante precisar que 4 controles especificados en la tabla fueron descartados de la evaluación, toda vez que ya fueron evaluados en la preauditoría realizada recientemente por el proveedor ICONTEC y que sobre estos se decretaron las 4 no-conformidades.

Dominios Anexo A	CONTROLES A EVALUAR	CUMPLEN	NO CUMPLEN	ACCION ABORDAR RIESGO	CONTROL NO EVALUADO
Controles Tecnológicos	26	25		1	8
8.1	1	1			
8.10	1	1			
8.11					1
8.12					1
8.13					1
8.14	1	1			
8.15	1	1			
8.16	1	1			
8.17					1
8.18	1	1			
8.19	1	1			
8.2	1	1			
8.20	1	1			
8.21	1	1			
8.22	1	1			
8.23					1
8.24	1	1			
8.25	1	1			
8.26					1
8.27	1	1			
8.28	1	1			
8.29	1	1			
8.3					1
8.30	1	1			
8.31	1	1			
8.32	1	1			
8.33	1	1			
8.34	1	1			
8.4	1	1			
8.5	1	1			
8.6	1			1	
8.7	1	1			
8.8	1	1			
8.9					1

Tabla8: Resultado de Dominio de Controles Tecnológicos)

La tabla8, corresponde al listado de controles seleccionados de dominio de “**Controles Tecnológicos**”, para lo cual se evaluaron 26 controles y se determinó que 25 “**Cumplen**”, mientras que un (1) control requiere una “**Acción para abordar Riesgo**” lo que deriva en acciones inmediatas para subsanar. De acuerdo con lo anterior, en el desarrollo del informe, se detallará la acción para abordar riesgo.

Nota: Es importante precisar que 8 controles especificados en la tabla, fueron descartados de la evaluación, toda vez que ya fueron evaluados en la preauditoría realizada

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos

recientemente por el proveedor ICONTEC y que sobre estos se decretaron las 8 no-conformidades.

Para conocimiento del lector, en la tabla que se relaciona a mano derecha, se listan los 14 no-conformidades identificadas de los controles, como resultado de la preauditoria realizada por ICONTEC y que no fueron objeto de evaluación dado el antecedente.	Nuevos Dominios Id control V2022 Control		
	Controles Organizacionales	5.13	Etiquetado de la información
	Controles Organizacionales	5.17	Información de autenticación
	Controles Organizacionales	5.30	Preparación de las TIC para la continuidad del negocio
	Controles Organizacionales	5.34	Privacidad y protección de la información de identificación personal
	Control de Personas	6.2	Términos y condiciones de la relación laboral
	Controles Físicos	7.7	Política de escritorio y pantalla limpios
	Controles Tecnológicos	8.11	Enmascaramiento de datos
	Controles Tecnológicos	8.12	Prevención de fuga de datos
	Controles Tecnológicos	8.13	Respaldo de la información
	Controles Tecnológicos	8.17	Sincronización de relojes
	Controles Tecnológicos	8.23	Filtrado WEB
	Controles Tecnológicos	8.26	<u>Requisitos de seguridad de las aplicaciones</u>
	Controles Tecnológicos	8.3	Restricción de acceso a la información
	Controles Tecnológicos	8.9	Gestión de configuración

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

ANÁLISIS DE NO-CONFORMIDAD DETECTADAS RESPECTO AL ANEXO-A

A continuación, se listan y detallan los diferentes hallazgos representados en (No-conformidades) que se identificaron como resultado de la evaluación realizada.

Hallazgo 1	
Dominio	Controles Organizacionales
Controles	Control A.5.31 – Requisitos legales, estatutarios, reglamentarios y contractuales El control busca asegurar que la entidad conozca y cumpla las obligaciones que le aplican en materia de seguridad de la información, protección de datos, privacidad, propiedad intelectual, conservación de información y demás requisitos aplicables. La entidad debe demostrar qué requisitos le aplican, quién es responsable, cómo se cumplen, cuándo fueron revisados y qué acciones se toman ante cambios o incumplimientos.
Dependencia Auditada:	Dirección de Planeación Institucional y Calidad Dirección TIC Oficina de Asuntos Jurídicos (OAJ)
Resultado de la evaluación	Si bien existe un inventario o normograma de leyes, decretos, resoluciones y reglamentos aplicables a la seguridad de la información, se encuentra documentado la generalidad, se establecen los responsables y se actualiza periódicamente, evidenciamos que: - Algunos requisitos legales, estatutarios y reglamentarios relacionados con seguridad de la información no se encuentran incorporados en dicho inventario como es el caso de: Decisión Andina 351 de 1993 - Régimen común de Derecho de Autor y Derechos Conexos Decreto 1360 de 1989⁴ - Protección del software Ley 565 de 2000⁵ - Tratado sobre Derecho de Autor incluyendo protección de programas de ordenador. - No se cuenta con registros de comunicación de requisitos aplicables a las dependencias responsables. - Por último, no se cuenta con registros de verificación de seguimiento y <u>evidencia del cumplimiento</u> de cada uno de los requisitos del inventario existente, dicho mecanismo en la actualidad no se encuentra implementado, lo cual conlleva desinformación e incumplimientos. El riesgo asociado de la situación descrita conlleva al incumplimiento de obligaciones legales o contractuales, generando sanciones, demandas, pérdida de confianza y afectación de la confidencialidad, integridad o disponibilidad de la información. De acuerdo con lo anterior y con base en reunión de cierre, se reclasifica y se emite una acción para abordar riesgo con respecto al control A5.31 del anexo A y se deberán aplicar las acciones de mejora que haya lugar.

⁴ "Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor".

⁵ "Por medio de la cual se aprueba el "Tratado de la OMPI -Organización Mundial de la Propiedad Intelectual- sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996)"

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos

Hallazgo 2

Dominio	Controles Organizacionales Control A 5.32 Derechos de propiedad intelectual
Controles	Los derechos de propiedad intelectual son un componente importante del cumplimiento legal en Colombia y el marco aplicable no se limita a una sola norma: comprende derechos de autor, software, bases de datos, obras digitales, propiedad industrial y protección de contenidos y licencias. Para el caso establece que la entidad debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual relacionados con información, software, documentos, contenidos y demás activos protegidos. La entidad debe realizar: • Identificar los activos sujetos a derechos de propiedad intelectual. • Proteger documentos, diseños, bases de datos, fotografías, videos y otros contenidos. • Capacitar a funcionarios y contratistas sobre derechos de autor.
Dependencia Auditada:	Dirección de Planeación Institucional y Calidad Dirección TIC Oficina de Asuntos Jurídicos (OAJ)
Resultado de la evaluación	Desde la Oficina de Asuntos Jurídicos, se compartieron de primera mano algunos memorandos y formatos diligenciados que fueron radicados en la Dirección Nacional Derechos de Autor - DNDA, con referencia a los derechos de propiedad intelectual sobre el Arte Digital generado al interior de entidad como fueron los casos consultados de: • Temática de Personaje – SER y • Temática de TILO para salud mental. De igual forma la entidad de acuerdo con lo verificado, viene controlando los siguientes elementos: 1. Uso autorizado de software en donde se requiere la prestación de los servicios, el cual es controlado y autorizado por la Dirección TIC. 2. Condiciones contractuales de propiedad intelectual con los proveedores Externos como es el caso del aplicativo SISVEA, entre otros. 3. Control de código fuente de desarrollo de Software realizado por personal interno de la entidad. 4. Y viene adelantando la publicación de derecho de propiedad intelectual sobre el "Arte Digital" a la de Dirección Nacional Derechos de Autor - DNDA Sin embargo, se logra evidenciar que: 1. No existe un inventario de activos sujetos a derechos de propiedad intelectual. 2. No existe un lineamiento y procedimiento establecido que defina el flujo que debe surtir para que las dependencias cumplan las directrices de propiedad intelectual. 3. La entidad no cuenta con mecanismos suficientes y formalmente establecidos para identificar, controlar y proteger los derechos de propiedad intelectual asociados a diferentes activos de información como es el caso de: documentos, diseños, bases de datos, videos y otros contenidos. 4. No se tiene establecido y no cuenta con registros de capacitación a funcionarios y contratistas sobre derechos de autor. 5. identificamos que requisitos legales, estatutarios y reglamentarios relacionados con derechos o propiedad intelectual no se encuentran incorporados en inventario (normograma) e implementados como es el caso de:

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos

- Decisión Andina 351 de 1993 - Régimen común de Derecho de Autor y Derechos Conexos
- Decreto 1360 de 1989 - Protección del software
- Ley 565 de 2000 - Tratado sobre Derecho de Autor incluyendo protección de programas de ordenador.

6. Por último, se identificó ausencia o insuficiencia de evidencias que permitan demostrar el seguimiento periódico al cumplimiento de las obligaciones relacionadas con propiedad intelectual.

Las situaciones descritas, puede conllevar al uso, reproducción o distribución no autorizada de activos protegidos por derechos de propiedad intelectual, generando posibles incumplimientos legales y contractuales, sanciones, reclamaciones de terceros, pérdidas económicas y afectación de la seguridad de la información.

De acuerdo con lo anterior y con base en reunión de cierre, se reclasifica y se emite una acción para abordar riesgo con respecto al control A5.32 del anexo A y se deberán aplicar las acciones de mejora que haya lugar.

Hallazgo 3	
<i>Dominio</i>	Controles Organizacionales
<i>Controles</i>	Control A 5.8 Seguridad de la información en la gestión de proyectos Establece que la seguridad de la información debe integrarse en la gestión de proyectos, independientemente del tipo de proyecto y el control busca que los riesgos de seguridad sean identificados y tratados desde la planificación del proyecto y durante todo su ciclo de vida.
<i>Dependencia Auditada:</i>	Dirección de Planeación Institucional y Calidad Dirección TIC
Resultado de la evaluación	Si bien la entidad viene liderando proyectos en todos los ámbitos, se cuenta con directores de proyectos en las diferentes dependencias y se aplica las buenas prácticas de dirección de proyectos tradicionales basado en el PMBok, y lo que concierne a proyectos ágiles con SCRUM, Se evidenció que: - Los proyectos ejecutados al interior de la entidad no incorporan de manera sistemática los requisitos de seguridad de la información durante sus diferentes etapas de planificación, ejecución, seguimiento/control y cierre. - No se evidenció la realización de evaluaciones de riesgos de seguridad de la información relacionada con los diferentes proyectos internos que lleva a cabo la entidad, no se cuenta con registros de evaluación de impactos del riesgo de la seguridad de la información y las diferentes amenazas. Lo anteriormente descrito, evidencia que la seguridad de la información no se encuentra integrada de manera consistente e integral en la gestión de los proyectos institucional, generando el riesgo de que vulnerabilidades, incumplimientos o debilidades de seguridad sean identificados de manera tardía, permanezcan sin tratamiento y conlleva la exposición de la información a accesos, modificaciones, pérdida o divulgación no autorizada. De acuerdo con lo anterior, se declara y mantiene la no-conformidad con respecto al control A5.8 y se deberá aplicar la acción correctiva a que haya lugar con miras la obtención de la Certificación del SGSI.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos
--

Hallazgo 4

Dominio	Controles Físicos Control A 7.2 Entrada física
Controles	Las áreas seguras deben estar protegidas mediante controles apropiados de entrada y puntos de acceso, para garantizar que únicamente las personas autorizadas puedan ingresar. El control busca prevenir el acceso físico no autorizado a instalaciones, áreas críticas, equipos e información de la entidad,
Dependencia Auditada:	Subdirección de Bienes y Servicios Dirección de Planeación Institucional y Calidad
Resultado de la evaluación	El ejercicio permitió la verificación en sitio de los siguientes elementos: • Sistema de control de acceso físico de molineras en puertas principales y secundarias mediante los registros del aplicativo BIOSTAR. • Verificación de acceso con carnés, biometría, llaves en áreas de acceso con información sensible. • Registro y trazabilidad de entradas y salidas de colaboradores y visitantes. • Control de visitantes en puerta principal y bitácoras de piso. • Verificamos las protecciones de áreas críticas como centros de datos (Datacenter Container) y cuartos técnicos. • Se cuenta con procedimiento de control de acceso físico. Sin embargo, se evidenció que los controles establecidos para gestionar y restringir el acceso físico a las instalaciones y áreas donde se encuentran activos de información sensible, no se aplican de manera consistente ya que durante la auditoría se identificaron las siguientes debilidades: 1. Al revisar piso a piso las bitácoras o libros de ingreso y salida de equipos, se evidencia que no todos los equipos que salen e ingresan son registrados, en algunos casos la actualización es parcial, ya que al consultar dicha libro no se cuenta con datos de: fecha, hora y firma del funcionario que ingreso el equipo, por otro lado, existe una bitácora alterna que permite llevar el control de los visitantes, si bien se registra la persona (visitante) al momento de ingresar, no se lleva registro de la salida del mismo, lo cual permite demostrar que el control no es del todo eficaz. Nota: Dicho control mediante libro no es eficiente, por lo que se recomienda replantear el control. Frente a esta situación, se cuenta con evidencia que soporta el hallazgo. 2. Falta de cultura en cumplimiento de política de seguridad, ya que el control de acceso físico en la puerta principal y en la puerta secundarias que utilizan "las molineras" y para lo cual es indispensable la utilización de huella dactilar o tarjeta de proximidad habilitada en la herramienta, se sigue evidenciando que, los colaboradores de la entidad en general y demás visitantes, evaden o evitan el control, poniéndose en cola o detrás de la persona que si realizan el proceso de autenticación, logrando con ello acceder a las áreas sin autorización, lo cual demuestra que el control no es del todo efectivo y el riesgo de que personas no autorizadas ingresen a la entidad, lo cual constituye una amenaza constante y evidencia que el control no es del todo eficiente. 3. Al consultar el aplicativo BIOSTAR con 3 usuarios específicos para efectos de validación, se identificó que dichos usuarios no han sido depurados o actualizados en el aplicativo, en el entendido que dichas personas de curva administrativa, son exfuncionarios de la entidad y el acceso físico mediante tarjeta y huella sigue estando "activo" cuando debería estar deshabilitado en el aplicativo BIOSTAR. De acuerdo con

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

lo anterior, existe un riesgo de que personas no autorizadas, ingresen a la entidad, lo cual constituye una amenaza, lo que demuestra que el control no es del todo eficiente.

Dichas situaciones ponen en riesgo las áreas donde se alojan equipos, documentos y medios que contienen información institucional, pudiendo ocasionar pérdida, alteración, sustracción o divulgación a personas no autorizadas.

Para efectos de comprobación se listan los casos consultados de retiros y cambios de área recientes en el aplicativo BIOSTAR que todavía mantienen los permisos de acceso físicos:

- Exdirectora de la Subdirección de Bienes y Servicio (Diana Marcela Acosta),
- Profesional del LABORATORIO DE SALUD que se trasladada a la Subdirección de Contratación (Sandra Olivos), y a fecha todavía conservan acceso físico al Laboratorio.

De acuerdo con lo anterior y con base en reunión de cierre, se reclasifica y se emite una acción para abordar riesgo con respecto al control A7.2 del anexo A y se deberán aplicar las acciones de mejora que haya lugar.

Hallazgo 5

Dominio	Controles Físicos
Controles	Control A 7.3 Seguridad de oficinas, salas e instalaciones Establece que la entidad debe diseñar e implementar la seguridad física de oficinas, salas e instalaciones de acuerdo con los riesgos identificados. Dicho control busca prevenir el acceso físico no autorizado a la información y a los activos de información que se encuentran dentro de las instalaciones de la entidad.
Dependencia Auditada:	Subdirección de Bienes y Servicios Dirección de Planeación Institucional y Calidad
Resultado de la evaluación	De acuerdo con la revisión realizada en sitio, evidenciamos los siguientes controles aplicados: • Accesos físicos mediante biométricos o llaves físicas que protegen áreas donde se encuentran: Servidores/Equipos de comunicaciones/Sistemas de información/Archivos de documentos físicos, • Controles de seguridad física con biométricos que protegen acceso a pisos, oficinas y salas • Se tienen establecidas reglas para visitantes y contratistas. • Se realizan labores de inspecciones periódicas en las instalaciones. • Se cuenta con personal de vigilancia, que da paso a los visitantes en cada uno de los pisos. No obstante, se identifican las siguientes debilidades frente al control: 1. Si bien se tiene implementado control biométrico por huella dactilar o tarjeta de proximidad en puertas de acceso a dependencias o áreas sensibles, se logró demostrar que las puertas del edificio en DUES pisos 5,6,7 que fueron objeto de verificación, cuentan con el control biométrico instalado, sin embargo, al pasar la tarjeta y huella dactilar de varios colaboradores de la entidad contratistas que no son personal directo del proceso, les permitió el acceso a dichas áreas.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos

- En varios de los pisos del edificio administrativo, si bien se cuenta con biométrico instalado, las puertas permanecen abiertas a todo momento por consiguiente ingresa o accede cualquier persona sin autorización.

De acuerdo con lo anterior, se evidenció que las medidas de seguridad física implementadas para proteger los activos de información que se encuentran en oficinas, salas e instalaciones no son suficientes para garantizar una protección adecuada frente al acceso no autorizado. Durante la auditoría se identificaron áreas donde se encuentran archivos documentales físicos (expedientes, historias laborales, entre otros), que no cuentan con controles físicos suficientes, el antecedente es que en el año 2025 hubo un incidente por perdida de 9 carpetas de expedientes en la Oficina de Asuntos Jurídicos, lo cual conllevó a la reconstrucción de dichas carpetas. A la fecha se desconoce el autor material o intelectual de los hechos señalados anteriormente. Lo anterior en términos del control de acceso físico, puede facilitar el acceso no autorizado, manipulación, daño, pérdida o sustracción de activos como equipos, documentos y medios que contienen información institucional, afectando la confidencialidad, integridad y disponibilidad de la información.

De acuerdo con lo anterior, se declara y ratifica la no-conformidad con respecto al control A7.3 y se deberá aplicar la acción correctiva que a haya lugar con miras a la obtención de la Certificación del SGSI.

Hallazgo 6	
Dominio	Controles Físicos
Controles	Control A 7.14 Eliminación o reutilización segura de equipos Asegurar que la información sensible y el software licenciado hayan sido eliminados o sobrescritos de manera segura antes de su disposición o reutilización. Cuando un equipo sea: Dado de baja. /Donado/Reasignado a otro usuario/Devuelto a un proveedor/ Enviado a reparación/Retirado definitivamente.
Dependencia Auditada:	Dirección TIC Subdirección de Bienes y Servicios Dirección de Planeación Institucional y Calidad
Resultado de la evaluación	Al particular, se informa que cuando un colaborador de la entidad se retira de la entidad ya sea por despido o decisión propia, se genera la solicitud que permite formalizar la entrega de equipos y la solicitud se procede a registrar en el Software Aranda. Por su parte el equipo de propiedad planta y equipo solicita a la Dirección TIC generar el concepto técnico de los equipos de cómputo que permitirá el traslado al ALMACEN. Por último, para dar de baja los equipos, se hace la solicitud a la Dirección TIC de llevar a cabo el borrado seguro de la información que permitirá la reutilización de los equipos. A la fecha de la presente evaluación, se cuenta con registros de "conceptos técnicos" emitidos por la Dirección TIC, sin embargo, registros de borrado seguro de la información mediante el formato SDS-BYS-FT-017 y aplicando la metodología, no se tiene en todos los casos. Si bien la entidad cuenta con un procedimiento formalmente establecido que permite garantizar la eliminación segura de la información contenida en los equipos y medios de almacenamiento antes de su reutilización, este no es aplicado continuamente, así mismo, durante la auditoría se identificaron equipos retirados o destinados a reutilización que cuentan con conceptos técnicos emitidos, pero a la fecha no se evidenció la aplicación de procedimientos de borrado seguro, sobre escritura o destrucción de los medios de almacenamiento, ni registros que permitan demostrar la eliminación efectiva de la información contenida en estos. Lo anterior genera el riesgo de recuperación y acceso no autorizado a información institucional, confidencial o sensible por parte de terceros

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos
--

afectando la confidencialidad de la información y pudiendo generar incumplimientos legales o contractuales.

Evidencias solicitadas en mesa de trabajo:

- Conceptos técnicos de reintegro al almacén generados
- Formato SDS-BYS-FT-017 de borrado seguro de información tramitados
- Inventario de equipos dados de baja a los cuales se les debe realizar el borrado seguro.
- Procedimiento de disposición y reutilización de equipos.
- Actas de baja de equipos.

Nota: Se consultó el caso de exfuncionaria Dra. Diana Acosta, frente a la cual se formalizó el retiro de la entidad hace 2 meses, sin embargo, el equipo de cómputo que tenía asignado sigue en la dependencia, no cuenta con concepto técnico emitido, y la información que se encuentra almacenada en dicho equipo sigue sin ser borrada de acuerdo con lo informado aportada.

De acuerdo con lo anterior y con base en reunión de cierre, se reclasifica y se emite una acción para abordar riesgo con respecto al control A7.14 del anexo A y se deberán aplicar las acciones de mejora que haya lugar.

Hallazgo 7	
Dominio	Controles Tecnológicos
Controles	Control A 8.6 Gestión de la capacidad El uso de los recursos debe ser monitoreado y ajustado de acuerdo con los requisitos de capacidad actuales y esperados. La entidad debe asegurarse de que sus servidores, almacenamiento, redes, aplicaciones y demás recursos tecnológicos tengan capacidad suficiente, tanto para las necesidades actuales como para el crecimiento futuro.
Dependencia Auditada:	Dirección TIC Dirección de Planeación Institucional y Calidad
Resultado de la evaluación	Al particular, se solicitó a los participantes evidencia o reportes de monitoreo continuo que permitiera conocer el uso de los recursos, sin embargo, se informa que dicha tarea es realizada por cada uno de los administradores de manera independiente pero no todos lo realizan. En el caso de los elementos de la Red LAN (Switches de Piso y Borde) se utilizan las herramientas de gestión propietarias, para el monitoreo de infraestructura on-premise, se hace uso de la herramienta libre ZABBIX y para servicios en la NUBE se utilizan las herramientas de gestión propietarias de AZURE Microsoft y en el caso de elementos de Seguridad perimetral, se hace uso de herramientas de gestión de Fortinet. Sin embargo, evidenciamos que buenas prácticas de gestión de la capacidad no se realizan con es el caso de: • Informe o reportes mensuales de capacidad general • Proyecciones futuras o Plan de capacidad para los próximos 6-12 meses • Análisis de tendencias de consumo. • Planificación de ampliaciones antes de que los recursos lleguen a niveles críticos. • No en todos los casos se realiza optimización de aplicaciones, bases de datos y procesos que consumen altos recursos. • Crecimiento esperado de los servicios que se prestan. • Así mismo, informe del dominio de servidores, no se realiza fue necesario solicitarlo en mesa.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos
--

Así mismo, el monitoreo actual no se mide:

- Crecimiento mensual de almacenamiento
- Capacidad disponible vs. capacidad requerida
- Número de servicios que superan los umbrales establecidos

Por último, no existe un lineamiento y procedimiento con enfoque a la gestión de la capacidad, es por eso que no todos los administradores o los responsables de recursos conocen lo que deben hacer y no existe un informe consolidado que debería proveer el coordinador de infraestructura.

De acuerdo con lo expuesto, es evidente que la entidad a través de los referentes encargados, no realizan de manera sistemática el monitoreo, análisis y gestión de la capacidad de los recursos tecnológicos que soportan los servicios y sistemas de información y durante la auditoría no se suministró información suficiente que permita demostrar el seguimiento periódico de la utilización de recursos y tampoco existen proyecciones de capacidad que permitan anticipar las necesidades futuras de los servicios tecnológicos. Dicha situación puede ocasionar que los recursos tecnológicos alcancen niveles críticos de utilización, saturación o insuficiencia, ocasionando degradación del rendimiento, interrupción de servicios, indisponibilidad de sistemas y afectación de la disponibilidad de la información.

De acuerdo con lo anterior y con base en reunión de cierre, se reclasifica y se emite una acción para abordar riesgo con respecto al control A8.6 del anexo A y se deberán aplicar las acciones de mejora que haya lugar con miras la obtención de la Certificación del SGSI.

Se precisa que el presente informe contiene la síntesis de todo el ejercicio realizado y es importante resaltar que la auditoría, implicó la revisión y evaluación de cada uno de los aspectos trazados de acuerdo con el cronograma establecido, las evidencias y soportes solicitados en cada una de las mesas, se especificara en el documento ANEXO denominado: Inventario_SOPORTES_EVIDENCIAS_SI2026.xlsx el cual es uno de los productos a entregar como resultado del ejercicio.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

7. ASPECTOS POSITIVOS (NIA 2410 A2)

- 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.
- Entre las principales fortalezas se destacan la disposición y el compromiso institucional de las diferentes partes interesadas en la seguridad de la información, la existencia de políticas y lineamientos relacionados, la implementación de mecanismos de control en los sistemas de información y los diferentes avances en la implementación del plan de seguridad y el fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI).
- La seguridad de la información es considerada como un tema transversal que impacta y afecta a todas las dependencias y operaciones de la entidad, más allá de ser una preocupación exclusiva de la Dirección TIC, la protección de datos e información es crucial para la Secretaría de Salud.
- Se reconoce que la seguridad es un tema transversal y crucial para definir y establecer las estrategias de seguridad, ya que el riesgo puede provenir de múltiples fuentes internas y externas.
- Se entiende que la seguridad de la información en los activos de información en salud, se centra en evitar el robo de identidad, fraudes, el daño a la reputación institucional y graves consecuencias económicas.
- Existe el compromiso firme de la Dirección de Planeación Institucional y de la Dirección de Talento Humano en 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 y gobierno digital.
- El recurso humano conoce las entradas y las salidas de cada uno de los procedimientos, instructivos que actualmente se encuentran implementados y determina de forma preventiva los recursos físicos, financieros y tecnológicos que son necesarios para la operación de la seguridad de la información en la entidad.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

8. NO CONFORMIDADES (NIA 2431)

8.1. Si bien la entidad cuenta con un Plan de Seguridad de la Información establecido para el año 2026 que permite orientar y ejecutar las actividades requeridas para la implementación y fortalecimiento del SGSI, durante la auditoría se identificaron actividades cuyo cumplimiento presenta atrasos frente a las fechas programadas y/o no cuentan con evidencia suficiente de avance o ejecución, así como tampoco se evidencian, productos o entregables específicos, situación que conlleva a que no está asegurando de manera eficaz la implementación y el seguimiento al cumplimiento de los compromisos, responsables, plazos y resultados definidos en el Plan de Seguridad de la Información; en consecuencia, se presenta una brecha entre la planificación establecida y la ejecución efectiva, lo que conlleva a decretar una no-conformidad del requisito numeral 8.1 de la norma ISO/IEC 27001:2022

Responsables: Dirección de Planeación Institucional

8.2. Se evidenció que la organización tiene definidos 11 indicadores asociados a la gestión de seguridad de la información; sin embargo, algunos de estos no han sido objeto de medición periódica, toda vez que no presentan resultados o evidencias de seguimiento y tampoco se encuentran claramente relacionados con los objetivos de seguridad de la información, si bien se reportan resultados de medición del POGD frente al cumplimiento de actividades del SGSI al 100%; se evidencia, de acuerdo con la revisión realizada, que el resultado no es del 100%, toda vez que existen atrasos de actividades. En consecuencia, los indicadores definidos no permiten, de manera integral, determinar si el SGSI está alcanzando los resultados previstos, lo anterior evidencia que el control de seguimiento, medición, análisis y evaluación del SGSI no se encuentra implementado de manera eficaz, incumpliendo lo establecido en el numeral 9.1 de la norma ISO/IEC 27001:2022.

Responsable: Dirección de Planeación Institucional

8.3. Se evidenció que la seguridad de la información no se encuentra integrada a la gestión de los proyectos institucionales, debido a que no todos los proyectos ejecutados al interior de la entidad incorporan de manera uniforme requisitos, criterios y actividades de seguridad de la información durante las diferentes etapas de su ciclo de vida, incluyendo la planificación, ejecución, control, y cierre de proyectos. Adicionalmente, no se evidencian registros de realización de evaluaciones de riesgos de seguridad de la información asociadas a los diferentes proyectos internos que permitan identificar y valorar oportunamente los riesgos, amenazas y posibles impactos sobre información y los activos involucrados en los proyectos en la entidad, y no se cuenta con un mecanismo formal impartido desde la PMO o desde la Dirección de Planeación institucional y Calidad, que permita determinar para cada proyecto, los requisitos de seguridad, los riesgos asociados, las medidas de tratamiento requeridas. En consecuencia, la entidad no puede demostrar que los requisitos o aspectos de

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

seguridad de la información sean considerados y gestionados de manera adecuada a lo largo del ciclo de vida de los proyectos, lo cual conlleva un incumplimiento del control A.5.8 del Anexo A de la norma ISO/IEC 27001:2022.

Responsables: Dirección de Planeación Institucional y Oficina de Proyectos

8.4. Como resultado de la auditoría se evidenciaron debilidades en la implementación y aplicación efectiva de los controles establecidos para restringir y controlar el acceso físico a oficinas, dependencias y áreas sensibles de la entidad. En particular, se identificaron las siguientes situaciones: 1. Asignación y validación inadecuada de permisos de acceso: Si bien la entidad dispone de mecanismos de control de acceso biométrico mediante huella dactilar y/o tarjeta de proximidad en las puertas de acceso a las dependencias o áreas sensibles, durante las pruebas de acceso realizadas en el edificio del DUES, pisos 5, 6 y 7, se logró demostrar que funcionarios y contratistas que no tienen relación con estas áreas o dependencias hicieron uso de la tarjeta de proximidad y/o huella dactilar registrada y pudieron ingresar. 2. Puertas de acceso permanecen abiertas, aunque las puertas cuentan con dispositivos biométricos instalados, estas permanecen abiertas de manera permanente, permitiendo el ingreso y circulación de personas sin que medie la autenticación o validación correspondiente, situación que hace que el control biométrico instalado pierda efectividad. Dichas situaciones ponen en riesgo los activos de información, equipos tecnológicos, documentación, carpetas físicas, expedientes y demás recursos institucionales, pudiendo afectar su confidencialidad, integridad y disponibilidad. En consecuencia, se determina el incumplimiento del control A.7.3 del Anexo A de la norma ISO/IEC 27001:2022.

Responsable: Subdirección de Bienes y Servicios/Seguridad y Control / Planeación Institucional

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

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

9.1 Si bien se cuenta con una matriz de identificación de partes interesadas, durante la auditoría se evidenció que existen actores relevantes para el SGSI que no se encuentran incorporados en el inventario y en el análisis como es el caso de las dependencias: Subdirección de Bienes y servicios, Talento Humano, Oficina de Asuntos Jurídicos, Asuntos Disciplinarios y Planeación Institucional y Calidad, así como requisitos aplicables o pertinentes relacionados con la seguridad de la información que no han sido determinados, documentados y evaluados para establecer su incidencia en el SGSI, en consecuencia, varias de las partes interesadas relacionadas y relevantes no han sido considerados como elementos de entrada para la planificación, implementación, mantenimiento y mejora del SGSI, lo que deriva en una acción para abordar riesgo de cara al requisito 4.2 de la norma ISO/IEC 27001:2022 por cuanto no ha determinado de manera integral las partes interesadas pertinentes al SGSI.

Responsable: Dirección de Planeación Institucional y Calidad

9.2. Se cuenta con lineamiento y manual que define los roles, responsabilidades y autoridades frente a la seguridad de la información; sin embargo, se evidencia que dichos roles no se encuentran claramente asignados a responsables específicos y no han sido comunicados o divulgados de manera individual, roles que tienen relación para la ejecución, seguimiento y control de las actividades del SGSI, se identificó que los colaboradores que ejercen dichos roles, desconocen las responsabilidades que tienen frente al sistema, lo anterior evidencia una implementación parcial de los requisitos establecidos en el numeral 5.3 de la norma ISO/IEC 27001:2022 y del control A.5.2 del Anexo A, al no garantizarse que las responsabilidades y autoridades pertinentes para la seguridad de la información deben estar definidas, asignadas y comunicadas, lo que deriva en una acción para abordar riesgo de cara al requisito y control.

Responsable: Dirección de Planeación Institucional y Calidad

9.3. La entidad dispone de un inventario/normograma de requisitos legales, estatutarios, reglamentarios y contractuales aplicables, este no contempla de manera integral los requisitos relacionados con la seguridad de la información, ya que requisitos tales como la Decisión Andina 351 de 1993, el Decreto 1360 de 1989 y la Ley 565 de 2000, relacionados con derechos de autor y protección de programas de computador, no se encuentran incorporados en dicho inventario, adicionalmente, no se evidenciaron registros que demuestren la comunicación de los requisitos aplicables a las dependencias responsables de su cumplimiento, ni registros suficientes que permitan demostrar el seguimiento, verificación y evaluación del cumplimiento de dichos requisitos. Lo anterior, evidencia que el mecanismo establecido por la entidad para identificar, mantener, comunicar y verificar los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la seguridad de la información no se

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

encuentra implementado de manera integral, lo que deriva en una acción para abordar riesgo de cara al cumplimiento del control A.5.31 del Anexo A de la norma ISO/IEC 27001:2022.

Responsables: Dirección de Planeación Institucional

- 9.4. Se evidenció que la entidad no ha establecido e implementado de manera transversal los mecanismos necesarios para identificar, controlar, proteger y realizar seguimiento a los derechos de propiedad intelectual asociados con la información y los activos, teniendo en cuenta que durante la auditoría se identificaron las siguientes situaciones:
1. No se cuenta con un inventario de activos sujetos a derechos de propiedad intelectual, que permita identificar y controlar de manera sistemática los activos protegidos y los derechos, licencias, autorizaciones o restricciones de uso asociados,
 2. No se encuentra establecido y formalizado un lineamiento o procedimiento que defina el flujo que deben surtir las dependencias para identificar, gestionar, proteger y dar cumplimiento a las directrices relacionadas con derechos de propiedad intelectual.
 3. La entidad no cuenta con mecanismos para identificar, controlar y proteger los derechos de propiedad intelectual asociados a diferentes activos de información, tales como documentos, diseños, bases de datos, videos, contenidos digitales y otros materiales sujetos a protección; así mismo, existe insuficiencia de registros que permitan demostrar el seguimiento periódico al cumplimiento de las obligaciones relacionadas con derechos de propiedad intelectual, en consecuencia, se deriva en una acción para abordar riesgo de cara al cumplimiento del control A.5.32 del Anexo A de la norma ISO/IEC 27001:2022.

Responsables: Dirección de Planeación Institucional

- 9.5. Durante la auditoría se evidenció que la entidad cuenta con diferentes mecanismos establecidos para el control de acceso físico a sus instalaciones como es el caso de los dispositivos biométricos, cámaras de vigilancia 7X24 y cuenta además con guardas de seguridad y monitoreo continuo, sin embargo, estos controles no son del todo eficientes ya que presentan debilidades en su operación, seguimiento y gestión, situación que afecta la eficacia para prevenir y detectar accesos físicos no autorizados. Como resultado de las actividades de auditoría se identificaron las siguientes situaciones:
- a) Debilidades en los registros de ingreso y salida de equipos y personal visitantes, ya que, en las bitácoras o libros utilizados para registrar el ingreso y salida de equipos, se evidenció que no todos los equipos que ingresan o salen de las instalaciones son registrados y se identifican registros con información incompleta, de igual manera se identificó que, en la bitácora alterna para el control de visitantes, no se evidencia de manera consistente el registro de la salida.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

- b) Evasión de los mecanismos de autenticación para el ingreso físico, se evidenció que algunos colaboradores y visitantes evaden el mecanismo de autenticación individual, ingresando inmediatamente detrás de otra persona que previamente realizó la validación de acceso.
- c) Permanencia de permisos de acceso físico de personas que ya no tienen vínculo con la entidad, ya que la consulta realizada al aplicativo BIOSTAR y tomando como muestra tres usuarios, se evidenció que las personas que se retiraron de la entidad, mantienen activos los mecanismos de acceso físico asociados a tarjeta y/o huella dactilar. Todo lo anterior, evidencia debilidades en la gestión y depuración de los usuarios con permisos de acceso físico, particularmente en la actualización y deshabilitación oportuna de las credenciales como consecuencia de las novedades administrativas. Para lo cual, se deriva en una acción para abordar riesgo de cara al cumplimiento del control A.7.2 de la norma ISO/IEC 27001:2022.

Responsables: Subdirección de Bienes y Servicios/Seguridad y Control

9.6. Pese a que la entidad cuenta con un procedimiento formalmente establecido para garantizar la eliminación o borrado seguro de la información contenida en equipos y medios de almacenamiento antes de su reutilización o baja, durante la auditoría se evidenció que dicho procedimiento no se aplica de manera consistente y sistemática. En particular, se identificaron equipos retirados o destinados a reutilización que cuentan con conceptos técnicos emitidos; sin embargo, a la fecha de la auditoría no se evidenció la ejecución de actividades de borrado seguro para garantizar la eliminación de la información contenida en los medios de almacenamiento, no se cuenta con registros, actas, u otros soportes que permitan demostrar que la información almacenada en dichos equipos y medios haya sido efectivamente eliminada. Por lo anterior, se evidencia una brecha entre el procedimiento formalmente establecido y su aplicación efectiva, generando debilidades en la trazabilidad y en la capacidad de la entidad para demostrar el cumplimiento total del control A.7.14. de la norma ISO/IEC 27001:2022.

Responsables: Dirección TIC, Dirección de Planeación Institucional

9.7. Durante la auditoría se evidenció que la gestión de la capacidad de los recursos tecnológicos no se realiza de manera sistemática, documentada y preventiva, presentándose debilidades en el monitoreo, análisis, proyección y planificación de la capacidad requerida para soportar adecuadamente los servicios de tecnología y los servicios prestados por la entidad. En general, no se evidenciaron los siguientes elementos: Proyecciones futuras o un plan de capacidad que permita estimar las necesidades de recursos para los siguientes 6 a 12 meses, análisis de tendencias de consumo y utilización de recursos, que permitan identificar comportamientos crecientes, decrecientes o anómalos, planificación anticipada de ampliaciones o ajustes de capacidad, actividades de optimización de aplicaciones, bases de datos y

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

procesos que presentan un consumo elevado de recursos, evidenciándose que estas acciones no se realizan en todos los casos de manera sistemática. Lo anterior evidencia que, el seguimiento de la capacidad se encuentra principalmente orientado a la atención de necesidades puntuales y requerimientos específicos, sin que se evidencie un esquema integral de monitoreo, análisis de tendencias, proyección y planificación preventiva de la capacidad. En consecuencia, se deriva una acción para abordar riesgo de cara al cumplimiento del control A.8.6 del Anexo A de la norma ISO/IEC 27001:2022.

Responsable: Dirección TIC y Dirección de Planeación Institucional y Calidad

10. CONCLUSIONES (NIA 2410-A1)

- La entidad entiende que la seguridad de la información no es un sistema aislado, sino un proceso complejo que debe ser constante y que abarca diferentes aspectos entre ellos la seguridad física, lógica, la aplicación de programas de seguridad (antivirus, cortafuegos), la concientización, y la aplicación de políticas y procedimientos, todo esto con el fin de protegerse contra diferentes amenazas naturales o provocadas por el ser humano.
- La Dirección de Planeación Institucional, ejerce el liderazgo y lleva a cabo la gobernanza y define la implementación institucional del sistema de seguridad de la información a partir de las buenas prácticas de seguridad en donde todos los procesos y las dependencias son actores fundamentales y ejercen un rol en su estricto cumplimiento.
- La Dirección de Planeación Institucional, se encuentra comprometida con la gestión de riesgos de seguridad de la Información, la implementación de políticas de operación de seguridad de la información y ha dispuesto los recursos necesarios para la implementación y mejora del SGSI.
- Si bien el SGSI se viene implementado gradualmente y se cuenta con diferentes repositorios documentales, se evidencia que, existen enlaces de publicación en el portal WEB de la entidad, que referencian a documentos de política y planes de seguridad no vigentes, lo cual se puede constatar a partir de los siguientes enlaces: <https://n9.cl/pqwlgw>, <https://n9.cl/csg7c>, <https://n9.cl/hq5186>, en virtud de lo anterior, se hace necesario realizar las actualizaciones que haya lugar.
- Se logró verificar el cumplimiento de varias actividades trazadas en el plan de seguridad año 2026 en concordancia con la implementación del Sistema de Gestión de Seguridad de la Información, que hacen parte de los requisitos establecidos de la Norma ISO/IEC 27001:2022 y el ANEXO-A, sin embargo, existen atrasos tal cómo

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

se describió en el hallazgo presentado en el informe, lo cual no coinciden con el reporte de desempeño de actividades del POGD año 2026

- El SGSI se encuentra en un proceso de implementación y adecuación de cara a la obtención de la certificación internacional, dicha implementación contempla todos los requisitos de la norma ISO 27001:2022, los 93 controles del ANEXO-A y en cumplimiento de la Resolución 500 de 2021 expedida por MinTIC.
- La estructura de roles y responsabilidades definida frente a la seguridad de información en la entidad, debe ser dada a conocer a cada una de las partes interesadas y debe ponerse en práctica, ya que es una debilidad existente.
- La entidad cuenta con un proceso y metodología estructurada que permite identificar, evaluar y mitigar las amenazas y vulnerabilidades permitiendo identificar de manera oportuna posibles exposiciones y evitar daños a la reputación, interrupciones en las operaciones, sanciones legales y pérdidas financieras.
- En el caso de violaciones o incidentes de seguridad que lleguen a materializarse y en la que pueden verse comprometidos colaboradores o funcionarios de la entidad, el proceso de control disciplinario establecido en la actualidad, está en la capacidad de recibir de diferentes fuentes o canales las quejas o reclamaciones que son recepcionadas y llevar a cabo las investigaciones del caso y determinar las casuísticas. Se enfatiza en la importancia de crear campañas de concientización, para que los colaboradores de la entidad reporten situaciones o casos que atenten contra la confidencialidad e integridad de la información, ya que hasta el momento solo existe un caso registrado.
- En la visita e inspección realizada en los diferentes edificios de la SDS, identificamos dispositivos de acceso físico Biométricos que son administrados por el aplicativo BIOSTAR, y que por razones de labores de mantenimiento se encuentran fuera de funcionamiento, como es el caso del dispositivo ubicado en el sótano del ARCHIVO CENTRAL y en otras áreas sensibles de los diferentes pisos del DUES.
- La falta de medición de los objetivos de seguridad definidos mediante política general bajo la Resolución 705 del 2025, conlleva a una no-conformidad, ya que la ausencia de seguimiento, significa que no se está verificando el cumplimiento de dichos objetivos y actividades del plan, por lo que se evidencia falta de seguimiento y control, para lo cual es indispensable implementar las acciones correctivas y asegurar la medición.
- Es pertinente continuar fomentando la cultura de seguridad y el empleo de un lenguaje común a todos los colaboradores de la entidad que permita minimizar las amenazas del internet, para ello es indispensable definir estrategias de sensibilización y formación aplicada a todos los colaboradores, dicha estrategia es

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

continúa en el tiempo debido a su importancia y relevancia. Las estrategias sugeridas apuntan a: cursos virtuales, intranet, correo electrónico, posters ubicados en sitios estratégicos, pantallas digitales, sesiones presenciales entre otros.

- Es conveniente y preventivo robustecer la arquitectura de seguridad, con servidores de detección de intrusos - IDS de tipo host o red, así como servidores de prevención de intrusos – IPS, analizadores de tráfico y SIEM, permitiendo detectar actividades sospechosas y no autorizadas, como los ataques de suplantación de identidad (phishing), la infección de virus, 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.
- La gestión de Incidentes de Seguridad y Privacidad de la Información define el procedimiento y la guía para la identificación, atención y respuesta a los incidentes y eventos de seguridad y privacidad de la información y seguridad digital, lo cual permite actuar de manera rápida y eficiente frente a los incidentes de seguridad que atenten contra la pérdida de la confidencialidad, integridad y disponibilidad de la información de la Secretaría de Salud
- Ampliar y continuar el contacto con autoridades en materia de seguridad de la información, ya que es crucial para recibir información sobre amenazas de ámbito mundial e incentivar la gestión proactiva de incidentes de seguridad en la entidad y permite además solicitar asesoramiento experto, lo que fortalece el sistema de gestión de seguridad de la información y la capacidad de respuesta ante vulnerabilidades.
- El control de acceso en las entradas principales mediante control biométrico de tarjetas de proximidad y huella dactilar, no es del todo efectivo, ya que el personal evade o evita el control, la persona que está por delante de la otra, realiza autenticación debida y las personas que están detrás de esta, se ponen en cola o van en fila accediendo a las instalaciones, y los guardas de seguridad no están verificando o no ponen ningún tipo de restricción, situación que pone en riesgo las áreas que manejan activos de información sensible.
- Se cuenta con el documento de declaración de aplicabilidad – SOA, el cual define los controles necesarios enumerados para gestión de riesgos, se justifica cada uno de los controles aplicables y se comprueba que no existen exclusiones.
- En lo correspondiente a las verificaciones realizadas por los referentes encargados frente a los requisitos de selección del personal establecido mediante lista de verificación, existe constancia o evidencia de la verificación realizada por el profesional de las consultas realizadas con las instituciones educativas garantizando la legalidad de la información aportada.

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	

Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos
--

- El control de préstamos de carpetas físicas de historias laborales, que se lleva mediante bitácora o libro físico, cuenta con la trazabilidad o registro completo de los préstamos y la entrega de carpetas a la dependencia.
- Se lleva el control de préstamos de expedientes de procesos jurídicos o carpetas físicas al grupo de abogados, dicho control se realiza mediante archivo Excel y cuenta con la trazabilidad o registro completo de los préstamos y la entrega de carpetas a la dependencia.

RECOMENDACIONES:

- Considerando que el propósito de la entidad es obtener la certificación de su Sistema de Gestión de Seguridad de la Información (SGSI) en el corto plazo, se deberá definir y ejecutar el plan de preparación para la certificación, priorizando el cierre de las brechas identificadas frente a los requisitos de ISO/IEC 27001:2022 y los controles aplicables del Anexo A, se deberá contar con un cronograma de cierre de brechas con responsables, fechas, recursos, indicadores y criterios de aceptación, realizando seguimiento periódico hasta alcanzar un nivel de preparación adecuado para enfrentar la auditoría de certificación en el mes de octubre del año 2026.
- Se evidenciaron acciones orientadas a la concientización y sensibilización de los colaboradores en todos los niveles de la entidad; no obstante, al realizar preguntas a los referentes de seguridad y profesionales en diferentes áreas que participaron, la percepción es generalizada en cuanto a que se desconoce la política, los objetivos y donde esta publicada, al igual que las políticas operativas, si bien es cierto, se han realizado varias actividades de concientización y sensibilización al personal, dicho ejercicio seguirá siendo susceptible de mejora y fortalecimiento.
- El almacenamiento de archivos físicos de la OAJ en el piso 6 del edificio administrativo en el ala occidental, cuenta con un espacio o habitación que, al observar, no cuenta con medidas de protección contra incendios o inundación, situación que podría poner en riesgo la información física de carpetas con información sensible y confidencial que se almacena en dicho lugar, para lo cual se sugiere tomar las medidas requeridas y preventivas que permitan la protección contra amenazas ambientales.
- Priorizar la implementación de las acciones correctivas para subsanar las no-conformidades detectadas producto de la preauditoría realizada por ICONTEC y aquellas que la auditoría interna actual determine, clasificándolas según su criticidad y posible impacto sobre el cumplimiento de los requisitos de la norma ISO/IEC 27001:2022 y los controles aplicables del Anexo A, ya que no al contar con evidencia del cumplimiento, pueden afectar directamente la conformidad del SGSI. Se deberá asegurar que, antes de la auditoría de certificación del SGSI, se encuentren

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

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

debidamente analizadas, con causa raíz determinada, acciones correctivas definidas, responsables, recursos y fechas de ejecución, así como evidencias objetivas de su implementación y de la evaluación de su eficacia.

- Existen planes de recuperación ante desastres - DRPs que permiten dar respuesta ante una crisis, se definieron y aprobaron 18 planes, se realizaron pruebas sobre algunos sistemas de información y en efecto se guarda trazabilidad y resultados de algunos ejercicios realizados, de igual forma existen documentos de BIA técnicos y las variables RPO y RTO definidos para los 18 activos de información críticos. Se recomienda aunar esfuerzos para programar y llevar a cabo las pruebas reales sobre todos los activos de información críticos identificados.
- El proceso de Gestión TIC, debe fortalecer el modelo de gobernanza sobre los activos de información de la entidad, definiendo claramente las responsabilidades y niveles de autoridad de los propietarios, custodios y demás actores involucrados, de manera que se garantice una administración integral durante todo su ciclo de vida, lo anterior permitirá reducir el riesgo de pérdida, acceso no autorizado, divulgación, modificación o indisponibilidad de la información y demostrar el cumplimiento de los requisitos del SGSI y de los controles aplicables de la norma ISO/IEC 27001:2022, ya que en la actualidad una de las debilidades es que la Gestión TIC no tiene autoridad y control integral sobre todos los activos de información.
- Se recomienda fortalecer y formalizar los controles físicos de seguridad implementados en las áreas donde se custodian archivos documentales físicos, tales como expedientes, historias laborales y demás documentos que contengan información institucional, personal o de carácter reservado, con el fin de evitar o prevenir su pérdida, sustracción, alteración o acceso no autorizado. Lo anterior, considerando que durante la auditoría y adquiere especial relevancia, ya que se identificó que en el piso 6 del edificio administrativo Oficina de Asuntos Jurídicos durante el año 2025, se presentó un incidente relacionado con la pérdida de nueve (9) carpetas de expedientes, situación que requirió la reconstrucción de la documentación. A la fecha, no se cuenta con evidencia que permita establecer de manera concluyente el autor material o intelectual de los hechos. En consecuencia, se recomienda implementar medidas de control preventivo y de trazabilidad, entre ellas: restricción de acceso a las áreas de archivo únicamente al personal autorizado, mecanismos de identificación y registro de ingreso y salida, control y seguimiento de préstamo o consulta de expedientes, inventarios periódicos, sistemas de custodia y cierre de dependencias, monitoreo mediante cámaras de seguridad, y revisión periódica de la efectividad de dichos controles. El fortalecimiento de lo anterior, permitirá reducir la probabilidad de recurrencia de incidentes, mejorar la trazabilidad sobre la documentación bajo custodia y contribuir a preservar la confidencialidad, integridad y disponibilidad de la información contenida en los archivos físicos de la entidad.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	EVALUACIÓN, INDEPENDIENTE A LA GESTIÓN INSTITUCIONAL OFICINA DE CONTROL INTERNO SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	INFORME FINAL TRABAJO DE AUDITORIA (NIA 2410)				
	Código:	SDS- EIG -FT-002	Versión:	1	
Elaborado por: Mónica Ulloa Maz /Revisado por: Olga Lucia Vargas Cobos / Aprobado por: Olga Lucia Vargas Cobos					

- Continuar 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 entidad para la obtención de la certificación internacional en el corto plazo.

11. PLAN DE MEJORAMIENTO (NIA 2500)

Como resultado de la auditoría, los procesos deberán 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 las acciones para abordar los riesgos involucren otros procesos o dependencias. Nota: Sera responsabilidad de los referentes elaborar el plan de mejoramiento adecuado que responda a las no-conformidades identificadas.

12. ANEXOS.

- Corresponde a los papeles de trabajo utilizados de cada una de mesas de trabajo realizadas. LISTADEVERIFICACION AUDITORIA-SI2026.xlsx
- Inventario_SOPORTES_EVIDENCIAS_SI2026.xlsx, los cuales fueron solicitados para cada de las mesas de trabajo realizadas.

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


 Firmado digitalmente por
 Francisco Javier
 Pinto Gonzalez

Francisco Javier Pinto González

APRUEBA JEFE OFICINA DE CONTROL INTERNO.


 Firmado digitalmente
 por Saira Adelina
 Guzman Marmolejo

Saira Adelina Guzmán Marmolejo