Informe de Auditoría Interna

Proceso Direccionamiento Tecnologías de la Información y las Comunicaciones-DTIC
Sistema de Gestión de Seguridad de la Información de la Información-SGSI
Norma ISO 27001:2013

Vigencia 2022

Bogotá, D.C., 16/09/2022

Nota: Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

TABLA DE CONTENIDO

INTRODUCCIÓN 3
1. Objetivo de la Auditoría: 3
2. Alcance de la Auditoría: 3
3. Criterio(s) de la Auditoría: 3
4. Resultados de la Auditoría: 4
4.1. Hallazgos y/o No Conformidades 20
5. Fortalezas y Recomendaciones: 23
5.1. Fortalezas 23
5.2. Recomendaciones 23
6. Conclusiones: 26
Anexo 1. Cuadro Consolidado de Hallazgos y/o No Conformidades 27

Nota: Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

INTRODUCCIÓN

La Oficina de Control Interno, con base en el programa anual de auditorías año 2022 aprobado por el Comité Institucional de Coordinación del Sistema de Control Interno, determinó realizar la Auditoría Interna al Sistema de Gestión de Seguridad de la Información-SGSI, Norma ISO 27001:2013. Con el propósito de verificar el cumplimiento de los criterios de auditoría establecidos en el plan de auditoría.

Este informe presenta los resultados de dicha auditoría interna en cuanto al cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información en el proceso DTIC, los resultados que incluyen principalmente, fortalezas, recomendaciones, así como las desviaciones detectadas en relación con el cumplimiento de los requisitos de la norma ISO 27001:2013 y con base en lo anterior, el proceso realizará el plan de mejoramiento.

1. Objetivo de la Auditoría:

Verificar el cumplimiento de requisitos del Sistema de Gestión de Seguridad de la Información-SGSI bajo la norma ISO 27001: 2013.

2. Alcance de la Auditoría:

Determinar el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información-SGSI de la Personería de Bogotá D.C, bajo la norma ISO 27001: 2013 en el Proceso Direccionamiento Tecnologías de la Información y la Comunicación, y aquellos que por muestreo defina el equipo auditor para el primer semestre del año 2022.

3. Criterio(s) de la Auditoría:

- Normatividad legal Vigente.
- Normas y documentos al interior de la Personería de Bogotá D.C.
- Capítulos y numerales Norma ISO 27001:2013.

3. Criterio(s) de la Auditoría:

- Caracterización del Proceso Dirección de Tecnologías de la Información y las Comunicaciones.
- Requisitos de la organización, legales, cliente y las partes interesadas.
- Documentación del Sistema de Gestión de Seguridad de la Información de la Personería de Bogotá

4. Resultados de la Auditoría:

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
NORMA ISO 27001:2013

Durante la auditoría Interna del Sistema de Gestión de Seguridad de la Información-SGSI de la Personería de Bogotá D.C, se verificaron los requisitos establecidos en la Norma ISO 27001:2013.

Es así como en la lista de chequeo de la auditoría se dejó evidencia de la revisión, verificación y evaluación los siguientes capítulos:

Capítulo 4 Contexto de la Organización: 4.1,4.2,4.3,4.4.
Capítulo 5 Liderazgo: 5.1, 5.2,5.3.
Capítulo 6 Planificación: 6.1, 6.2.
Capítulo 7 Soporte: 7.1,7.2, 7.3, 7.4, 7.5.
Capítulo 8 Operación: 8.1, 8.2, 8.3.
Capítulo 9 Evaluación del Desempeño: 9.1, 9.3.
Capítulo 10 Mejora: 10.1, 10.2.

En desarrollo de la auditoría se verificaron los requisitos legales, lineamientos y reglamentos establecidos en la Personería, las partes interesadas y los establecidos para el Sistema de Gestión de Seguridad de la Información Norma ISO 27001:2013.

Para el Capítulo 4 Contexto de la Organización se realizó la verificación del numeral 4.1 conocimiento de la organización y su contexto, respecto a este tema el proceso hace entrega de documento Contexto ISO/IEC 27001:2013; encontrando que es importante mejorar el documento con la metodología PESTEL, con énfasis en el análisis del Entorno tecnológico, también es importante

4. Resultados de la Auditoría:

complementar la matriz DOFA con información del Proceso Gestión Documental y Recursos Físicos frente a los temas de seguridad de la información y el manejo de aspectos comunes a los 2 procesos. Así mismo, es importante que se realice la codificación del documento para incluirlo en el listado maestro de documentos del SGSI.

Por otra parte, en el numeral 4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas, el proceso hace entrega como soporte a este numeral las matrices de contactos con grupos de interés y de partes interesadas (actores y responsabilidades en datos personales), encontrando por parte del equipo auditor que el contenido de las matrices entregadas no soporta los requerimientos establecidos en el numeral de la norma. Posteriormente el proceso hace entrega del documento soporte denominado “contexto de la organización” el cual presenta las partes interesadas de manera general. Así mismo, entrega la matriz de partes interesadas, sin embargo, se observó solo la descripción de partes interesadas internas; por lo que se recomienda incluir las partes interesadas externas al igual que complementar con estas el documento del contexto de la organización.

Para el numeral 4.3 respecto a la determinación del alcance del sistema de gestión de la seguridad de la información, se evidenció que el Sistema de Gestión de Seguridad de la Información-SGSI cuenta con un alcance definido por la Alta Dirección, sin embargo, es importante que en el alcance se incluyan otras partes interesadas porque en el documento solo hacen referencia a los ciudadanos.

Finalmente, se evidenció el cumplimiento del numeral 4.4 Sistema de Gestión de Seguridad de la Información en donde la Entidad ha establecido su SGSI, se implementó se mantiene y se trabaja en la mejora continua.

En el Capítulo 5 Liderazgo se evidenció cumplimiento de los numerales 5.1 liderazgo y compromiso y 5.2 política; sin embargo, para el numeral 5.3 Roles, Responsabilidades y Autoridades de la Organización el proceso entrega como evidencia la Resolución 406 de 2020; el mencionado documento hace referencia a la adopción del Modelo Integrado de Planeación y Gestión-MIPG, Así mismo designa los responsables del MIPG, hace referencia a la inclusión de los sistemas de gestión de calidad, seguridad de la información y seguridad y salud en el trabajo y tan solo designa como responsable del SGSI al Director de Tecnologías de la información y las Comunicaciones. Por lo anterior, no se evidenció los roles, responsabilidades y autoridades en la organización frente al Sistema de Gestión de Seguridad de la Información.

4. Resultados de la Auditoría:

Respecto al Capítulo 6 Planificación en su numeral 6.1 se evidenciaron la matriz de riesgos del sistema de información, la matriz de oportunidades y plan de tratamiento de riesgos del SGSI. Por otra parte, se tuvieron en cuenta los controles que están establecidos en el Anexo A de la Norma ISO 27001:2013 los cuales son aplicables en su totalidad. Sin embargo, de un total de 114 controles de la norma, la entidad clasificó 38 controles como *"Control seleccionado, pero aún no está implementado"*, los cuales corresponden a un 33% de los controles del Anexo A situación que incumple el numeral 6.1.3 Tratamiento de Riesgos de Seguridad de la Información.

Para el numeral 6.2 Objetivos de Seguridad de la Información y Planes para Lograrlos, se solicitó al proceso DTIC informar como realizan la medición los Objetivos del SGSI y el proceso entrego como evidencia el documento Diagnóstico Actual y Brechas ISO 27001- MSPI - Personería de Bogotá; así mismo se solicito la entrega de los planes para el logro de los objetivos de seguridad de la información entregando los siguientes documentos: Plan Comunicación Sensibilización y Capacitación, Plan de Seguridad y Privacidad de la Información SGSI, Plan de Control Operacional, Plan de Seguimiento al SGSI, Plan de Tratamiento de Riesgos del SGSI, Plan de Continuidad del Negocio (en actualización), Plan de Contingencia (en Actualización). Revisados los documentos se puede establecer que los documentos no guardan relación con los objetivos del SGSI, aspecto que se tratara en detalle en el desarrollo de este informe.

En el Capítulo 7 Soporte se evidenció cumplimiento de los numerales 7.1 Recursos, 7.2 Competencia, 7.3 Toma de Conciencia y 7.5 Información Documentada. Sin embargo, en la verificación de la comunicación del SGSI en la pagina web y en la intranet de la Entidad se evidenció inconsistencias en la información del Alcance del SGSI, situación que presenta falta de integridad y claridad en la información que se comunica a los funcionarios, ciudadanos y otras partes interesadas evidenciando un incumplimiento del numeral 7.4 comunicación.

Por otra parte, en el Capítulo 8 Operación se evidenció cumplimiento de los numerales 8.1 Planificación y Control Operacional, 8.2 Valoración de Riesgos de la Seguridad de la Información y 8.3 Tratamiento de Riesgos de la Seguridad de la Información.

Para el Capítulo 9 Evaluación del Desempeño se solicitó al proceso DTC informar cómo se realizaba la medición del SGSI, el proceso hace entrega de formatos de seguimiento a los eventos e incidentes de seguridad de la información del año 2021 y año 2022, fichas de indicadores del año 2021 con mediciones hasta el mes de septiembre y 2022 con mediciones hasta el mes de junio y agosto; los

4. Resultados de la Auditoría:

indicadores están enfocados a objetivos y metas que no están relacionados con los objetivos del SGSI. Así mismo, presentaron documento Plan de Seguimiento y Revisión del SGSI, pero no hay evidencia de su aplicación por lo que se evidencia un incumplimiento del numeral 9.1, aspecto que se tratara en detalle en el desarrollo de este informe.

Así mismo, se solicito información acerca de la Revisión por la Dirección y el proceso entrego como soporte los siguientes documentos: Plan de Seguridad y Privacidad de la Información, cumplimiento de objetivos del SGSI, Plan de Comunicación Sensibilización y Capacitación del SGSI, Formato Plan de Auditoría 2021, Formato Informe Auditoria, Informe Auditoría Externa, Plan de Mejoramiento Proceso, estado actual de la seguridad y privacidad de la información PETI arquitectura empresarial y Plan de Seguimiento y Revisión del SGSI.
Los documentos presentados contienen algunos insumos para realizar la Revisión por la Dirección, pero no corresponde a la Revisión por la Dirección del año 2021. Por lo que se evidencia un incumplimiento del numeral 9.3 que se detalla más adelante.

Finalmente, en el capítulo 10 mejora, se evidenció el cumplimiento de los numerales 10.1 No Conformidades y Acciones Correctivas y 10.2 mejora Continua. Lo anterior soportado en el plan de mejoramiento del SGSI producto de la auditoría interna y la gestión realizada frente al plan de mejoramiento de la auditoría externa del año 2021.

Riesgos del Sistema de Gestión de Seguridad de la Información

Los lineamientos establecidos por el SGSI, y de conformidad con el plan de tratamiento de riesgos, cada proceso registró los riesgos de seguridad de la información en la matriz de Riesgos Institucionales los cuales fueron identificados y valorados de conformidad con la Guía para la Administración del Riesgo código 01-GU-04 versión 5 en el marco de los lineamientos establecidos por el DAFP.

En el mapa de riesgos se observaron las etapas de identificación del riesgo, análisis del riesgo inherente, evaluación del riesgo y valoración de controles; posterior a los controles realizaron nuevamente evaluación del riesgo-nivel del riesgo residual.

Para el Proceso Direccionamiento Estratégico de Tecnologías de la Información y las Comunicaciones, en su Sistema de Gestión de Seguridad de la Información cuenta con una matriz del mapa de riesgos institucionales en donde se identifican 6 riesgos de seguridad de la información.

4. Resultados de la Auditoría:

Revisado el mapa de riesgos se puede observar que 4 de los riesgos tienen que ver con fallas tecnológicas que generan la perdida de disponibilidad de la información en: (base de datos Oracle, información institucional procesada en actividades de trabajo en casa, teletrabajo, aplicativos misionales, plataforma virtual de servidores, SINPROC, SIRIUS, ISOLUCIÓN, portales web e intranet.)

Además, se evidenciaron 2 riesgos que tienen que ver con los usuarios, productos y prácticas organizacionales que generan la perdida de confidencialidad en: (información institucional procesada durante el trabajo en casa o teletrabajo). Así mismo, se pierde confidencialidad en la información sensible de la infraestructura tecnológica a cargo del proceso, como direcciones IP, hardening de los sistemas y redes, nombre de servidores y BD, contraseñas entre otros.

Todos los riesgos identificados cuentan con un plan de acción al que posteriormente le realizan monitoreo y revisión, durante la auditoría se observó que se realizó seguimiento a los riesgos para el primer cuatrimestre del año 2022 y a la fecha no se habían materializado riesgos.

Finalmente, se revisó el Plan de Tratamiento de Riesgos y se observó que ejecutan 3 actividades durante el año como son: La identificación y valoración de riesgos, la implementación del plan con los controles a los riesgos y el seguimiento a los riesgos de SGSI.

ANEXO A NORMA ISO 27001:2013
OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA

Se realizó seguimiento al Anexo A de la norma ISO 27001:2013 Objetivos de Control y Controles de Referencia, los cuales fueron acogidos por la Entidad; se identificaron 114 controles en el documento Declaración de Aplicabilidad código 03-FR-23 versión 2 vigente desde el 26/06/2020.

Así mismo, se identificó la implementación de 76 controles que corresponde al 67% de los mismos. De la misma manera, se encuentran seleccionados 38 controles que corresponde al 33% de los controles del Anexo A, pero aún no se han implementado.

Las convenciones descritas en el documento de aplicabilidad son: (I: Control esta Implementado, S: control se ha seleccionado, pero aún no se está implementando, E: el control ha sido excluido, BP: Buena Práctica, LE: Obligación Legal, OC: Obligación Contractual, TR: Tratamiento de Riesgo)

4. Resultados de la Auditoría:

En el Anexo A, se establecieron 18 dominios con los siguiente temas: A5 Políticas de la Seguridad de la Información, A6 Organización de la Seguridad de la Información, A7 Seguridad de los Recursos Humanos, A8 Gestión de Activos, A9 Control de Acceso, A10 Criptografía, A11 Seguridad Física y del Entorno, A12 Seguridad de las Operaciones, A13 Seguridad de las Comunicaciones, A14 Adquisición, Desarrollo y Mantenimiento de Sistemas, A15 Relaciones con los Proveedores, A16 Gestión de Incidentes de Seguridad de la Información, A17 Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio y A18 Cumplimiento.

Para efecto de la auditoría del Sistema de Gestión de Seguridad de la Información-Norma ISO 27001:2013 el equipo auditor selecciono una muestra del 30% de los controles implementados que equivale a 23 controles en los siguientes dominios A5 Políticas de Seguridad de la Información, A6 Organización de la Seguridad de la Información, A8 Gestión de Activos, A9 Control de Acceso, A11 Seguridad Física y del Entorno, A12 Seguridad de las Operaciones.

En el siguiente cuadro se pueden observar los controles que fueron revisados y que hacen parte de la muestra de auditoría:

Cuadro No. 1 controles

Numero	Numeral Controles	Tema
1	A.5.1.1	Políticas para la Seguridad de la Información
2	A.5.1.2	Revisión de las Políticas para la Seguridad de la Información
3	A.6.1.5	Seguridad de la Información en la Gestión de Proyectos
4	A.6.2.1	Política para dispositivos móviles
5	A.6.2.2	Teletrabajo
6	A.8.1.4	Devolución de activos
7	A.9.1.1	Política de Control de acceso
8	A.9.1.2	Acceso redes y a servicios en red
9	A.9.2.1	Registro y cancelación del registro de usuarios
10	A.9.2.2	Suministro de acceso de usuarios
11	A.9.2.3	Gestión de derechos de acceso privilegiado
12	A.9.4.2	Procedimiento de ingreso seguro
13	A.11.1.1	Perímetro de seguridad física
14	A.11.1.2	Controles de acceso físico
15	A.11.2.3	Seguridad del cableado

4. Resultados de la Auditoría:

16	A.11.2.4	Mantenimiento de equipos
17	A.11.2.8	Equipos de usuario desatendido
18	A.11.2.9	Política de escritorio limpio y pantalla limpia
19	A.12.1.2	Gestión de cambios
20	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación
21	A.12.2.1	Controles contra códigos maliciosos
22	A.12.3.1	Respaldo de la información
23	A.12.4.4	Sincronización de relojes

Fuente: Papel de Trabajo Muestreo Controles SGSI-ISO 27001:2013

La verificación de los controles se realizó mediante entrevista in situ y verificación de los soportes y análisis de los mismos se registraron en papel de trabajo de la auditoría, algunos resultados se observan a continuación:

A.9.4.2 Procedimiento de Ingreso Seguro

Para el ingreso a las instalaciones de la Dirección de Tecnologías de la Información y las Comunicaciones, existe un control de acceso o ingreso seguro por medio de la utilización de una tarjeta de proximidad, que cada funcionario utiliza para su acceso. Sin embargo, como se evidencia en el registro fotográfico, la puerta de acceso a la oficina se encontraba abierta, y no siempre permanece cerrada. Situación que evidencia debilidades en el ingreso a las referidas instalaciones.

Imagen Puerta y control de acceso a la Dirección de TIC abierta

4. Resultados de la Auditoría:

La seguridad física es importante y el acceso del personal al Centro de Cómputo está restringido a unos pocos. Sin embargo, el formato 03-FR-20 Versión 1 "Bitácora de Acceso a Centro de Cómputo y Cableado", utilizado para ejercer el control de acceso, no se está diligenciando completamente, haciendo que se pierda la efectividad del control. Esta situación se puede evidenciar en la siguiente imagen:

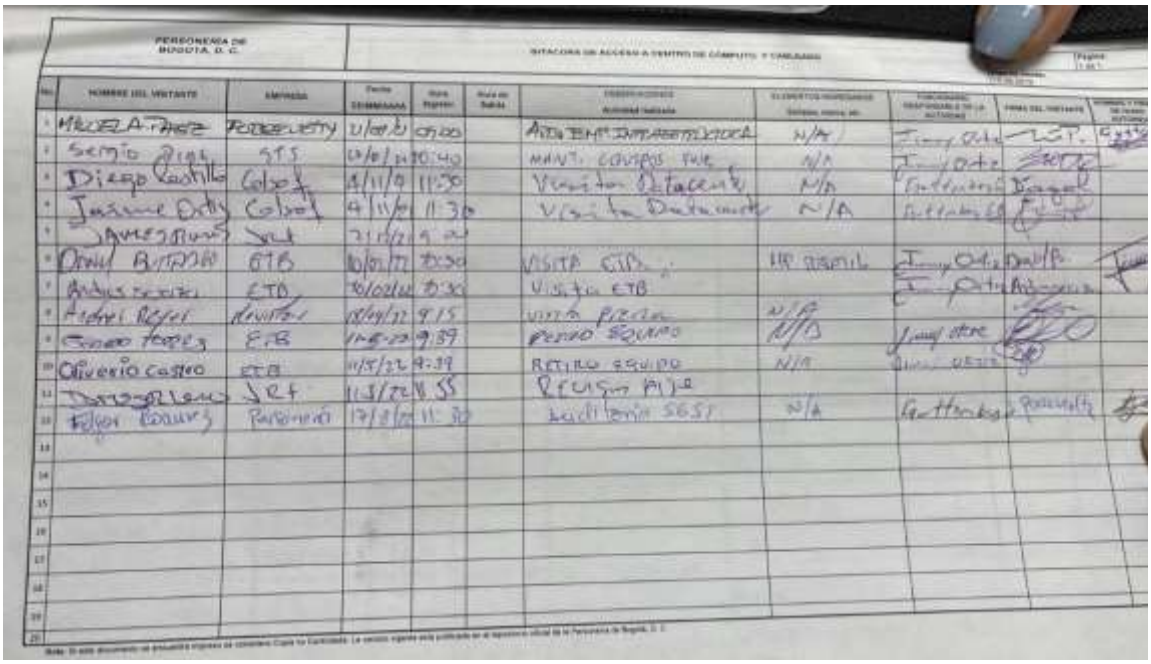


Imagen Bitácora de Acceso al Centro de Cómputo y Cableado diligenciada de manera incompleta

El formato registra el diligenciamiento de doce (12) filas, de las cuales cinco (5) contienen información de las visitas realizadas al centro de cómputo durante la vigencia 2021 y las siete (7) restantes corresponden a la vigencia 2022, evidenciando lo siguiente:

a) Para las doce (12) visitas, la columna "HORA DE SALIDA", no registra ninguna información.
b) En la columna "NOMBRE Y FIRMA DE QUIEN AUTORIZA", solamente tres (3) visitas registran la firma del funcionario que autorizó el ingreso.
c) El registro identificado como fila No. 5, del 21 de diciembre de 2021, no registra información en las siguientes columnas de "HORA DE SALIDA", "OBSERVACIONES Actividad Realizada", "ELEMENTOS INGRESADOS Seriales, marca, etc", "FUNCIONARIO RESPONSABLE DE LA ACTIVIDAD", "FIRMA DEL VISITANTE", y "NOMBRE Y FIRMA DE QUIEN AUTORIZA".

4. Resultados de la Auditoría:

d) En la fila 11, fechada el 11 de mayo de 2022, se registra una visita para "Revisar Aire", sin el diligenciamiento de cinco (5) de las diez (10) columnas.

A pesar de que se evidenció la aplicación del formato, se recomienda al proceso realizar el diligenciamiento completo del mismo.

A.11.2.3 Seguridad del Cableado

En las imágenes que se presentan a continuación, se observa que el piso falso utilizado para pasar y ocultar instalaciones eléctricas de voz y datos presenta deterioro; una de sus placas modulares se encuentra rota, situación que genera riesgos para los funcionarios y las personas visitantes que ingresan al Centro de Cómputo. Así mismo, en el techo se observa que faltan piezas que dejan al descubierto el cableado.

Imagen Piso falso roto

Imagen Faltan piezas del techo

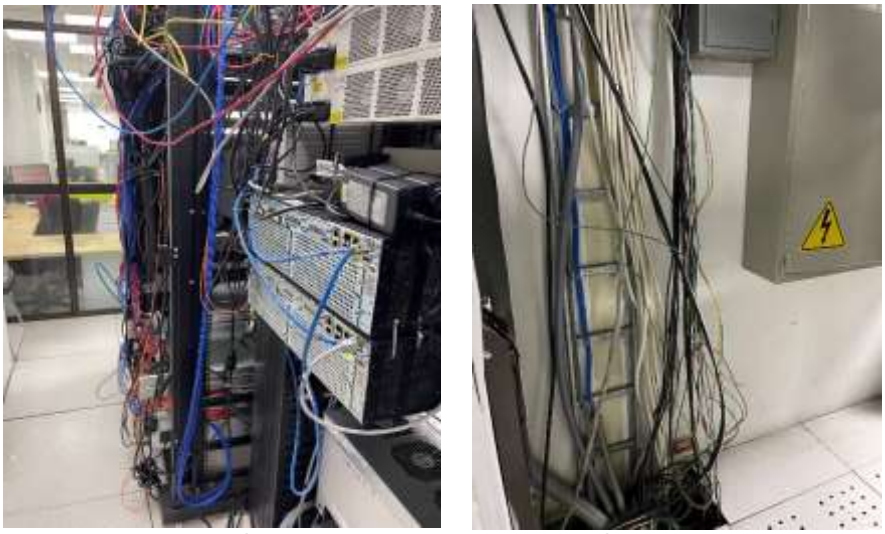
Igualmente, dentro del centro de cómputo y los cuartos de cableado estructurado ubicados en el Edificio viejo, Edificio nuevo y Edificio Centro de Atención a la Comunidad – CAC, se encontraron elementos como cajas, escalera, pintura, laminas, zorra de carga, proyector y otros elementos que no deben estar ubicados en estos sitios que por su importancia deben permanecer limpios, organizados y brindar la seguridad que requieren todos sus componentes.

4. Resultados de la Auditoría:

Imágenes Elementos encontrados en el Centro de Cómputo (Cajas, láminas de metal, placa modular)

En el centro de cómputo, se encontraron elementos como cajas y elementos que no deberían estar en este sitio, hecho que genera riesgos físicos.

A continuación, se presenta las imágenes donde se observó el estado de conexión y organización del cableado estructurado en las tres sedes visitadas por el equipo auditor:



Imágenes Estado Cableado Centro de Cómputo

4. Resultados de la Auditoría:

Piso 6 Edificio Viejo

Imágenes Estado Cableado Piso 6 Edificio Viejo

Piso 5 Edificio Viejo

Imágenes Estado Cableado Piso 5 Edificio Viejo

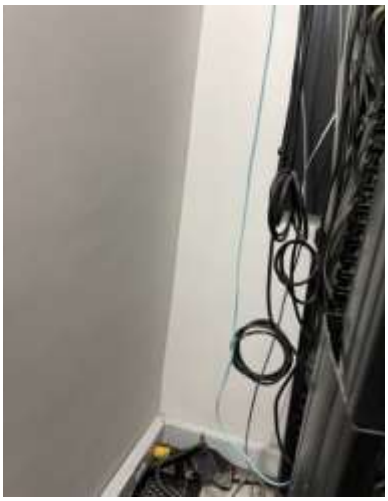
Nota: Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

4. Resultados de la Auditoría:

Piso 2 Edificio Viejo

Imágenes Estado Cableado Piso 2 Edificio Viejo (Láminas en el piso y faltan piezas del techo)

Piso 5 y Piso 4 Edificio Nuevo



Imágenes Estado Cableado Piso 5 Edificio Nuevo

Imagen Estado Cableado Piso 4 Edificio Nuevo

Nota: Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en el repositorio oficial de la Personería de Bogotá, D. C.

4. Resultados de la Auditoría:

Piso 3 Edificio Nuevo

Imágenes Estado Cableado Piso 3 Edificio Nuevo

Piso 2 Edificio Nuevo

Imagen Estado Cableado Piso 2 Edificio Nuevo

4. Resultados de la Auditoría:

Piso 1 Edificio Centro de Atención a la Comunidad - CAC

Imágenes Estado Cableado Piso 1 Edificio Centro de Atención a la Comunidad - CAC

Piso 9 Edificio Centro de Atención a la Comunidad - CAC

Imágenes Estado Cableado Piso 9 Edificio Centro de Atención a la Comunidad - CAC

4. Resultados de la Auditoría:

Piso 10 Edificio Centro de Atención a la Comunidad - CAC

Imágenes Estado Cableado Piso 10 Edificio Centro de Atención a la Comunidad - CAC

Las anteriores imágenes de los centros de cableado, permite observar que los componentes de red no están anclados dentro del rack y/o armario y no se usan adecuadamente los organizadores de cable y se acumulan elementos que no deben estar en estos sitios.

En general en las tres edificaciones visitadas, se observa que, en algunos centros de cableado, los cables no están totalmente canalizados ni organizados. Un cableado técnicamente conectado facilita tareas de soporte, modificación, mantenimiento de la red y reduce problemas de red para los usuarios.

A.11.2.8 Equipos de usuario desatendido

La Personería de Bogotá cuenta con una política de seguridad física y del entorno y el control “Equipo de usuario desatendido”. Sin embargo, se observó que algunos al retirarse de su puesto de trabajo, dejan sus equipos desatendidos sin cerrar la sesión. Por lo tanto, se recomienda sensibilizar, concientizar y entrenar a los servidores para que respondan de forma adecuada y apropiada a la protección de la información y los recursos tecnológicos.

4. Resultados de la Auditoría:

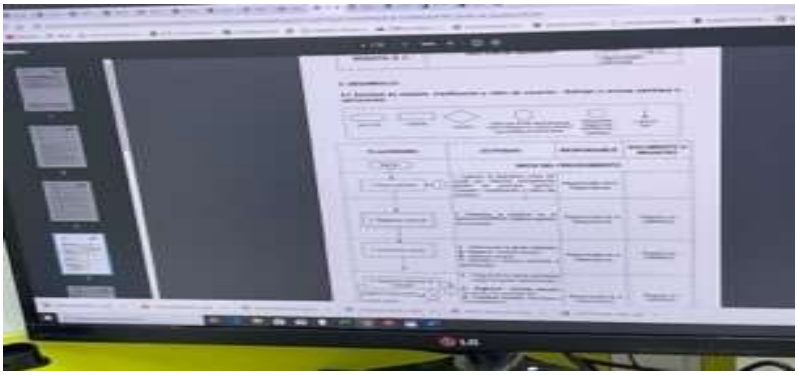
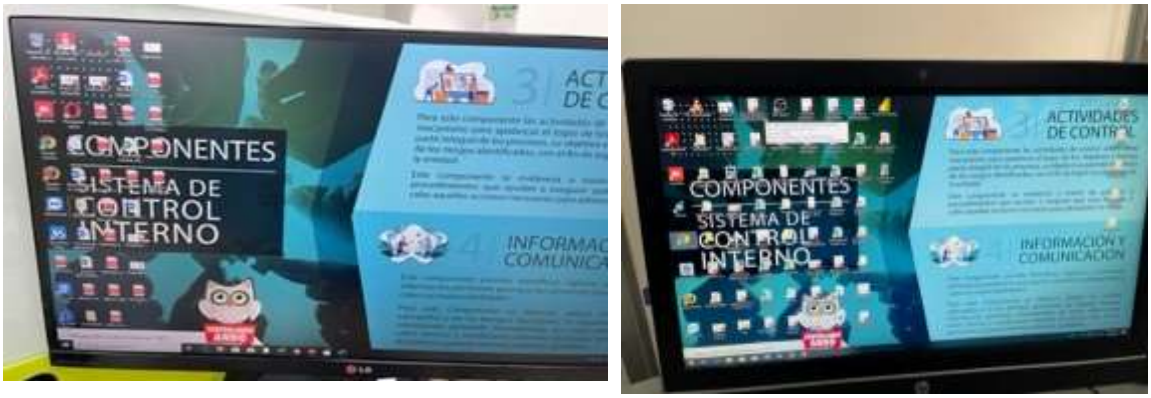


Imagen Equipo Desatendido

A.11.2.9 Política de escritorio limpio y pantalla limpia.

La Personería de Bogotá cuenta con una Política de Seguridad Física y del Entorno y el control “Política de escritorio limpio y pantalla limpia”, que se encuentra incluida en el Manual de Políticas de Seguridad de la Información Cód. 03-MN-01 V.7. Sin embargo, se observó que, en algunos puestos de trabajo, tanto los escritorios físicos como los escritorios de sus pantallas contienen documentos físicos como archivos digitales. Por lo tanto, se recomienda fortalecer la apropiación por parte de los funcionarios sobre la aplicación de la política de escritorio y pantalla limpia, teniendo en cuenta que esto reduce los riesgos de acceso no autorizado, pérdida y daño de información. Así mismo, es recomendable que en áreas con información sensible, reservada o crítica se fomente el uso de impresora con función de código PIN, para garantizar el control de quién, cuando y que se imprime.



Imágenes Escritorio limpio y pantalla limpia

4. Resultados de la Auditoría:

Imagen Escritorio limpio y pantalla limpia

A continuación, se establecen los Hallazgos y/o No Conformidades, las Fortalezas y las Recomendaciones que se encontraron durante del proceso de auditoría al Sistema de Gestión de Seguridad de la Información-Norma ISO 27001:2013.

4.1. Hallazgos y/o No Conformidades

1. La Dirección de las Tecnologías de la Información y las comunicaciones-DTIC informa que los roles y responsabilidades y autoridades del SGSI se encuentran en la Resolución 406 de 2020, revisada la mencionada Resolución se evidencia las responsabilidades de los procesos frente a las Dimensiones Operativas del MIPG, el Comité de Gestión y Desempeño, el Modelo Integrado de Planeación y Gestión-MIPG, los responsables de los sistemas de gestión y frente al SGSI solo relaciona la responsabilidad del Director de Tecnologías de Información y Comunicaciones, pero no se relacionan las responsabilidades y autoridades respecto a otros niveles de la organización que hacen parte del SGSI, tampoco se evidenció algún otro documento que presentará los roles y responsabilidades el SGSI en el listado maestro de documentos del Sistema, incumpliendo con el numeral 5.3 Roles, Responsabilidades y Autoridades en la Organización literales a) y b) de la norma ISO 27001:2013.

2. La DTIC entrega como medición de los objetivos del SGSI el instrumento llamado "Diagnóstico Actual y Brechas ISO 27001- MSPI - Personería de Bogotá", verificado el documento Diagnóstico Actual y Brechas se evidenció que este instrumento realiza mediciones del Anexo A Objetivos de Control y Controles de Referencia Norma ISO 27001:2013, también evalúa el grado de avance del Modelo de Seguridad de la Información-MSPI, pero no hace seguimiento y medición de los objetivos del SGSI.

4. Resultados de la Auditoría:

Así mismo, verificados los planes que se encuentran en el listado maestro de documentos del SGSI y los planes presentados por DTIC, se evidenció que estos planes tienen objetivos diferentes a los del SGSI y tampoco existe evidencia de su medición y seguimiento. Por lo anterior, no se realiza el seguimiento de los objetivos del Sistema de Gestión de Seguridad de la Información, como tampoco se evidenciaron los planes para lograrlos, incumpliendo con el numeral 6.2 Objetivos de Seguridad de la Información y Planes para Lograrlos literales f), g), h), i) y j) de la norma ISO 27001:2013.

3. Verificados los documentos del SGSI en la página web de la Entidad en el link MIPG (https://www.personeriabogota.gov.co/sistemas-de-gestion/sistema-de-seguridad-y-gestion-de-la-informacion-sgsi), Sistemas de Gestión, Sistema de Gestión de Seguridad de la Información, se evidenció publicado el alcance el SGSI con un enfoque a los activos de información, plataformas tecnológicas y procesos; posteriormente verificado el documento Política General de Seguridad de la Información y del cual hace parte también la publicación del alcance del SGSI mostrando el alcance aprobado por la Alta Dirección y que difiere en su contenido de la publicación del alcance que hace la presentación del sistema de gestión.

   Así mismo, se revisa el contenido de la intranet de la Entidad por el enlace MIPG (https://intranet.personeriabogota.gov.co/mipg/sistemas-de-gestion/sistema-de-seguridad-y-gestion-de-la-informacion), Sistemas de Gestión, Sistema de Gestión de Seguridad de la Información en el cual se presenta nuevamente el alcance del SGSI con una información que complementa las informaciones anteriores del alcance y que no fue aprobada por la Alta Dirección. Por lo anterior, la comunicación es confusa y se pierde la integridad de la información, incumpliendo con el numeral 7.4 Comunicación literal a) de la norma ISO 27001:2013.

4. Se evidenció documento formato de acta de reunión código 01-FR-06 versión 4 del 18/07/2019 donde se revisaron y aprobaron los indicadores del SGSI. Por otra parte, se evidenciaron formatos de seguimiento a los eventos e incidentes de seguridad de la información del año 2021 y año 2022; el formato de seguimiento del año 2022 no cuenta con codificación del SGSI. Así mismo, se observaron hojas de vida de los indicadores Tratamiento de Eventos de la Seguridad de la Información y Plan de Comunicación, Sensibilización y Capacitación del SGSI con mediciones hasta el mes de septiembre de 2021, pero en las fichas del indicador aparece el año 2020 y para el año 2022 con mediciones hasta los meses

4. Resultados de la Auditoría:

de junio y agosto, no obstante, lo anterior los indicadores están enfocados a objetivos y metas que no están relacionados con los objetivos del SGSI.

Finalmente, se evidenció documento Plan de Seguimiento y Revisión del SGSI código 03-PL-012 versión 1 vigente desde el 01/10/2021; sin embargo, no se evidencia documento de revisión y seguimiento del mencionado plan que den cuenta de los responsables del seguimiento, medición, análisis y evaluación de los planes y objetivos del SGSI y demás insumos de información requeridos para determinar la eficacia del Sistema. Incumpliendo lo establecido en el numeral 9.1 Seguimiento, Medición, Análisis y Evaluación literales a), b), c), d), e) y f) de la norma ISO 27001:2013.

5. Respecto a la Revisión por la Dirección, el Proceso DTIC entrega como evidencias los siguientes documentos Plan de Seguridad y Privacidad de la Información, cumplimiento de objetivos del SGSI, Plan de Comunicación Sensibilización y Capacitación del SGSI, Formato Plan de Auditoría 2021, Formato Informe Auditoria, Informe Auditoría Externa, Plan de Mejoramiento Proceso y Plan de Seguimiento y Revisión del SGSI.

   Así mismo, el proceso mediante correo electrónico de fecha 26/08/2022 ratifica los documentos y entrega nuevo documento denominado estado actual de la seguridad y privacidad de la información PETI arquitectura empresarial. Los documentos presentados contienen algunos insumos para realizar la Revisión por la Dirección, pero no corresponde a la Revisión por la Dirección del año 2021. Por lo anterior, no se evidenció documento o acta de la Revisión por la Dirección con los elementos de entrada y salida establecidos en la norma ISO para el SGSI; incumpliendo el numeral 9.3 Revisión por la Dirección literales a). b), c), d), e) y f) de la Norma ISO 27001:2013.

6. En concordancia con el Alcance del SGSI y la Declaración de Aplicabilidad código 03-FR-23, versión 2; adoptada por la entidad, se incluyen todos los procesos de la Entidad, y se indica que los requisitos como los controles del anexo A de la norma NTC/ISO 27001:2013 son aplicables en su totalidad. Sin embargo, de un total de 114 controles de la norma, la entidad clasificó 38 controles como *"Control seleccionado, pero aún no está implementado"*, por lo tanto, llama la atención de esta auditoría como se emite una certificación del SGSI, sin implementar la totalidad de los controles del *Anexo A. Objetivos de Control y Controles de Referencia*, en la medida en que se deben usar en contexto con el tratamiento de riesgos de

4. Resultados de la Auditoría:

la seguridad de la información. Incumpliendo el numeral 6.1.3. literal c) y d) de la norma NTC-ISO-IEC 27001:2013.

5. Fortalezas y Recomendaciones:

5.1. Fortalezas

- Disposición del responsable del SGSI y su equipo de trabajo frente a la auditoría del SGSI.
- En la implementación del Sistema de Gestión de Seguridad de la Información-SGSI, se resalta el liderazgo y compromiso por parte de la Dirección de TIC, trabajo que garantiza la seguridad de la información en la Entidad.
- Competencias del Talento Humano para el desarrollo de las funciones establecidas por el proceso DTIC y el SGSI.
- Realización de diversas actividades orientadas a la mitigación de riesgos del SGSI.
- Desarrollo de aplicativos para mejorar la gestión de los procesos misionales.
- Estructuración de los lineamientos establecidos por la Alta Dirección en el Manual de Políticas de Seguridad de la Información para la aplicación de controles.

5.2. Recomendaciones

- Es importante que se defina la adopción la Norma ISO 27001:2013, mediante acto administrativo para que esta norma internacional este como lineamiento interno por parte de la Entidad.
- Se recomienda complementar el documento Contexto ISO/IEC 27001:2013 mediante la metodología PESTEL haciendo un mayor énfasis en los factores tecnológicos, así mismo se debe terminar de revisar el documento, aprobarlo, codificarlo y anexarlo al listado maestro de documentos del SGSI. Igualmente, revisar los hechos que se evidenciaron en el análisis DOFA relacionados con la seguridad de la información, especialmente en

5. Fortalezas y Recomendaciones:

los procesos de Direccionamiento TIC y la Subdirección de Gestión Documental y Recursos Físicos, de tal forma que se alcancen los resultados previstos en el SGSI.

- Revisado el documento alcance del SGSI, solo se evidenció como parte interesada a los ciudadanos, es importante describir las otras partes interesadas, así mismo, sus necesidades y expectativas para que hagan parte del alcance en el SGSI.

- Se recomienda hacer un análisis detallado de los incidentes de seguridad y las vulnerabilidades del sistema de información para la identificación de riesgos, llevarlos a la matriz de riesgos y establecer controles.

- Revisar dentro de los documentos, el compendio de las normas externas aplicables al Sistema de Gestión de Seguridad de la Información - SGSI establecidas en la *"Matriz de requisitos legales"*, con el fin de verificar la vigencia y actualización de las normas incluidas en la referida matriz.

- En el Manual de Políticas de Seguridad de la Información código 03-MN-01 Versión 7, existe la política *"7.2.2.1 Política de dispositivos móviles"*, y siete (7) *"Lineamientos generales"*. Sin embargo, para proteger la información y crear conciencia sobre el uso de estos dispositivos, es importante impulsar el uso de controles y aplicar lo relacionado con el lineamiento que señala: ***"(…) tener configurada la aplicación para el borrado remoto de la información (…)"***, para los casos cuando estos dispositivos móviles sean hurtados o extraviados.

- Se hace necesario gestionar con Talento Humano las capacitaciones para mejorar las competencias de los funcionarios de DTIC.

- Es importante, como consecuencia de la implementación y certificación del Sistema de Gestión de Seguridad de la Información, que la entidad revise y actualice la caracterización del proceso de Direccionamiento TIC Código 03-PR-001, versión 8 y los diferentes documentos del SGSI, teniendo en cuenta que, en dicho documento, no se incluyen los requisitos y controles aplicables de la norma NTC ISO-IEC 27001:2013 y su anexo.

- De acuerdo con las disposiciones generales para la protección de datos personales, solo puede ejercerse con el consentimiento previo, expreso e informado del titular, por lo tanto, se recomienda como mecanismos para obtención de la autorización de los titulares que se encuentran dentro de

5. Fortalezas y Recomendaciones:

las diferentes instalaciones de la entidad objeto de un área de videovigilancia, se utilicen señales o avisos distintivos en estas zonas que incluyan: Información de quién es el responsable del tratamiento, sus datos de contacto, indicar el tratamiento que se dará a los datos y la finalidad de los mismos, incluir los derechos de los titulares e indicar dónde está publicada la política de tratamiento de datos.

- Gestionar la aprobación de los siguientes documentos: Procedimiento Gestión de Incidentes, formato informe de incidentes y Plan de Contingencia de TI.

- Considerando que corresponde al rol de Oficial de Seguridad la responsabilidad de planificar, desarrollar, controlar y gestionar las políticas, lineamientos, procedimientos y acciones a seguir para mejorar la seguridad de la información, es recomendable que la Alta Dirección defina la creación y empoderamiento de este rol dentro de la entidad.

- Se recomienda que la Alta Dirección defina la creación de una instancia donde se definan las políticas y lineamientos respecto a la seguridad de la información.

- A pesar de contar con la política de seguridad física y de entorno, en la visita realizada se observó que algunos funcionarios dejan abiertas las sesiones de sus equipos cuando se retiran de su puesto de trabajo. Por lo tanto, se recomienda generar conciencia y conocimiento de los requisitos y procedimientos de seguridad, a los funcionarios, contratistas y terceras partes, para proteger los equipos desatendidos.

- La entidad debe garantizar que se cumplan las directrices y controles establecidos para restringir el acceso a la información como se establece en el Anexo A, Control 9.4.2 de la Norma ISO 27001:2013, toda vez para ingresar a la Dirección de TIC se cuenta con un control que desasegura la puerta con el uso de una tarjeta de proximidad para los funcionarios de dicha dependencia. Sin embargo, durante la vista se observó que en ocasiones la puerta permanece abierta permitiendo el ingreso a personal no autorizado.

- Se recomienda realizar de manera completa y correcta el diligenciamiento de la Bitácora de Acceso a Centro de Cómputo y Cableado código 03-FR-20 Versión 1.

5. Fortalezas y Recomendaciones:

- Respecto del Cableado Estructurado de las tres edificaciones visitadas, se recomienda limpiar y retirar todos los elementos que no pertenecen a estos espacios y anclar y organizar de manera adecuada el trenzado del cable.

- La entidad cuenta con una política de seguridad física y del entorno y el control, *Política de escritorio limpio y pantalla limpia*, Sin embargo, se observó que, en algunos puestos de trabajo, tanto los escritorios físicos como los escritorios de sus pantallas contiene tanto documentos físicos como archivos digitales. Por lo tanto, se recomienda fortalecer la apropiación por parte de los funcionarios sobre la aplicación de la política de escritorio y pantalla limpia, teniendo en cuenta que esto reduce los riesgos de acceso no autorizado, pérdida y daño de información. Así mismo, es recomendable que en áreas con información sensible, reservada o crítica se fomente el uso de impresora con función de código PIN, para garantizar el control de quién, cuando y que se imprime.

- Se hace necesario fortalecer el compromiso de los responsables de proceso, para apropiar el conocimiento del SGSI en toda la organización con énfasis en la aplicación y uso de los controles, lineamiento y políticas.

- Se recomienda la inclusión de las partes interesadas externas con sus necesidades y expectativas en la matriz de partes interesadas y posteriormente incluirlas en el documento contexto de la organización.

6. Conclusiones:

- El Proceso Direccionamiento de las Tecnologías de la Información y las Comunicaciones, cuenta con un Sistema de Gestión de Seguridad de la Información fundamentado en los requisitos de la norma ISO 27001:2013, sin embargo, es importante gestionar algunos temas para el mejoramiento continuo del mismo.

- El Sistema de Gestión de Seguridad de la Información contribuye a la mejora de los procesos misionales mediante el desarrollo tecnológico de los aplicativos para prestación de los servicios ofrecidos a la ciudadanía.

6. Conclusiones:

- Para el tratamiento de riesgos de la seguridad de la información es necesario implementar los objetivos de control y controles de referencia del Anexo A que fueron asumidos en su totalidad por la Entidad.

Anexo 1. Cuadro Consolidado de Hallazgos y/o No Conformidades

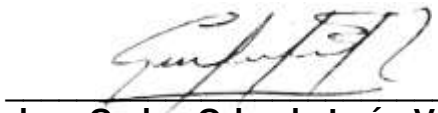
Ítem	CRITERIO DE AUDITORÍA	HALLAZGO Y/O NO CONFORMIDAD	RIESGO IDENTIFICADO
1	**Norma ISO 27001:2013** Capítulo 5 Liderazgo, Numeral 5.3 Roles, Responsabilidades y Autoridades en la Organización	La Dirección de las Tecnologías de la Información y las comunicaciones-DTIC informa que los roles y responsabilidades y autoridades del SGSI se encuentran en la Resolución 406 de 2020, revisada la mencionada Resolución se evidencia las responsabilidades de los procesos frente a las Dimensiones Operativas del MIPG, el Comité de Gestión y Desempeño, el Modelo Integrado de Planeación y Gestión-MIPG, los responsables de los sistemas de gestión y frente al SGSI solo relaciona la responsabilidad del Director de Tecnologías de Información y Comunicaciones, pero no se relacionan las responsabilidades y autoridades respecto a otros niveles de la organización que hacen parte del SGSI, tampoco se evidenció algún otro documento que presentará los roles y responsabilidades el SGSI en el listado maestro de documentos del Sistema, incumpliendo con el numeral 5.3 Roles, Responsabilidades y Autoridades en la Organización literales a) y b) de la norma ISO 27001:2013.	Desconocimiento de los roles, responsabilidades y autoridad en la Entidad respecto al SGSI
2	**Norma ISO 27001:2013** Capitulo 6 Planificación, Numeral 6.2 Objetivos de	La DTIC entrega como medición de los objetivos del SGSI el instrumento llamado "Diagnóstico Actual y Brechas ISO 27001-MSPI - Personería de Bogotá", verificado el documento Diagnóstico Actual y Brechas se evidenció que este instrumento realiza	Incumplimiento de los objetivos del SGSI por falta de seguimiento y medición.

Ítem	CRITERIO DE AUDITORÍA	HALLAZGO Y/O NO CONFORMIDAD	RIESGO IDENTIFICADO
	Seguridad de la Información y Planes para Lograrlos	mediciones del Anexo A Objetivos de Control y Controles de Referencia Norma ISO 27001:2013, también evalúa el grado de avance del Modelo de Seguridad de la Información-MSPI, pero no hace seguimiento y medición de los objetivos del SGSI. Así mismo, verificados los planes que se encuentran en el listado maestro de documentos del SGSI y los planes presentados por DTIC, se evidenció que estos planes tienen objetivos diferentes a los del SGSI y tampoco existe evidencia de su medición y seguimiento. Por lo anterior, no se realiza el seguimiento de los objetivos del Sistema de Gestión de Seguridad de la Información, como tampoco se evidenciaron los planes para lograrlos, incumpliendo con el numeral 6.2 Objetivos de Seguridad de la Información y Planes para Lograrlos literales f), g), h), i) y j) de la norma ISO 27001:2013.	
3	**Norma ISO 27001:2013** Capitulo 7 Soporte, Numeral 7.4 Comunicación	Verificados los documentos del SGSI en la página web de la Entidad en el link MIPG (https://www.personeriabogota.gov.co/sistemas-de-gestion/sistema-de-seguridad-y-gestion-de-la-informacion-sgsi), Sistemas de Gestión, Sistema de Gestión de Seguridad de la Información, se evidenció publicado el alcance el SGSI con un enfoque a los activos de información, plataformas tecnológicas y procesos; posteriormente verificado el documento Política General de Seguridad de la Información y del cual hace parte también la publicación del alcance del SGSI mostrando el alcance aprobado por la Alta Dirección y que difiere en su contenido de la publicación del alcance que hace la presentación del sistema de gestión. Así mismo, se revisa el contenido de la intranet de la Entidad por el enlace MIPG (https://intranet.personeriabogota.gov.co/mipg/sistemas-	Perdida de integridad de la información comunicada del SGSI.

Ítem	CRITERIO DE AUDITORÍA	HALLAZGO Y/O NO CONFORMIDAD	RIESGO IDENTIFICADO
		de-gestion/sistema-de-seguridad-y-gestion-de-la-informacion), Sistemas de Gestión, Sistema de Gestión de Seguridad de la Información en el cual se presenta nuevamente el alcance del SGSI con una información que complementa las informaciones anteriores del alcance y que no fue aprobada por la Alta Dirección. Por lo anterior, la comunicación es confusa y se pierde la integridad de la información, incumpliendo con el numeral 7.4 Comunicación literal a) de la norma ISO 27001:2013.	
4	**Norma ISO 27001:2013** Capitulo 9 Evaluación del Desempeño, Numeral 9.1. Seguimiento, medición y análisis y evaluación	Se evidenció documento formato de acta de reunión código 01-FR-06 versión 4 del 18/07/2019 donde se revisaron y aprobaron los indicadores del SGSI. Por otra parte, se evidenciaron formatos de seguimiento a los eventos e incidentes de seguridad de la información del año 2021 y año 2022; el formato de seguimiento del año 2022 no cuenta con codificación del SGSI. Así mismo, se observaron hojas de vida de los indicadores Tratamiento de Eventos de la Seguridad de la Información y Plan de Comunicación, Sensibilización y Capacitación del SGSI con mediciones hasta el mes de septiembre de 2021, pero en las fichas del indicador aparece el año 2020 y para el año 2022 con mediciones hasta los meses de junio y agosto, no obstante, lo anterior los indicadores están enfocados a objetivos y metas que no están relacionados con los objetivos del SGSI. Finalmente, se evidenció documento Plan de Seguimiento y Revisión del SGSI código 03-PL-012 versión 1 vigente desde el 01/10/2021; sin embargo, no se evidencia documento de revisión y seguimiento del mencionado plan que den cuenta de los responsables del seguimiento, medición, análisis y evaluación de los planes y objetivos del SGSI y demás insumos de información requeridos para	Falta de medición para evaluar el desempeño y eficacia del Sistema de Gestión de Seguridad de la información

Ítem	CRITERIO DE AUDITORÍA	HALLAZGO Y/O NO CONFORMIDAD	RIESGO IDENTIFICADO
		determinar la eficacia del Sistema. Incumpliendo lo establecido en el numeral 9.1 Seguimiento, Medición, Análisis y Evaluación literales a), b), c), d), e) y f) de la norma ISO 27001:2013.	
5	**Norma ISO 27001:2013** Capitulo 9 Evaluación del Desempeño, Numeral 9.3 Revisión por la Dirección	Respecto a la Revisión por la Dirección, el Proceso DTIC entrega como evidencias los siguientes documentos Plan de Seguridad y Privacidad de la Información, cumplimiento de objetivos del SGSI, Plan de Comunicación Sensibilización y Capacitación del SGSI, Formato Plan de Auditoría 2021, Formato Informe Auditoria, Informe Auditoría Externa, Plan de Mejoramiento Proceso y Plan de Seguimiento y Revisión del SGSI. Así mismo, el proceso mediante correo electrónico de fecha 26/08/2022 ratifica los documentos y entrega nuevo documento denominado estado actual de la seguridad y privacidad de la información PETI arquitectura empresarial. Los documentos presentados contienen algunos insumos para realizar la Revisión por la Dirección, pero no corresponde a la Revisión por la Dirección del año 2021. Por lo anterior, no se evidenció documento o acta de la Revisión por la Dirección con los elementos de entrada y salida establecidos en la norma ISO para el SGSI; incumpliendo el numeral 9.3 Revisión por la Dirección literales a). b), c), d), e) y f) de la Norma ISO 27001:2013.	Falta de Revisión por la Dirección del Sistema de Gestión de Seguridad de Información.
6	**Anexo A Norma ISO 27001:2013** Objetivos de Control y Controles de Referencia	En concordancia con el Alcance del SGSI y la Declaración de Aplicabilidad código 03-FR-23, versión 2; adoptada por la entidad, se incluyen todos los procesos de la Entidad, y se indica que los requisitos como los controles del anexo A de la norma NTC/ISO 27001:2013 son aplicables en su totalidad. Sin embargo, de un	Incumplimiento de los Objetivos de Control y Controles de Referencia establecidos para el Tratamiento de

Ítem	CRITERIO DE AUDITORÍA	HALLAZGO Y/O NO CONFORMIDAD	RIESGO IDENTIFICADO
		total de 114 controles de la norma, la entidad clasificó 38 controles como *"Control seleccionado, pero aún no está implementado"*, por lo tanto, llama la atención de esta auditoría como se emite una certificación del SGSI, sin implementar la totalidad de los controles del *Anexo A. Objetivos de Control y Controles de Referencia*, en la medida en que se deben usar en contexto con el tratamiento de riesgos de la seguridad de la información. Incumpliendo el numeral 6.1.3. literal c) y d) de la norma NTC-ISO-IEC 27001:2013.	Riesgos de la Seguridad de la Información.

EQUIPO AUDITOR
Firma:  **Nombre: Carlos Orlando León Valenzuela** **Empleo: Profesional Especializado 222-07**

APROBÓ
Firma: **Nombre: Nathalia Andrea Pineda Camelo** **Empleo: Jefe Oficina de Control Interno**