Informe de Auditoría Interna

Sistema de Gestión de Seguridad de la Información – SGSI
Norma ISO 27001:2013

Vigencia 2024

Bogotá, D.C., 2/12/2024

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 Conformidad 43
5. Fortalezas y Recomendaciones: 45
5.1. Fortalezas 45
5.2. Recomendaciones 45
6. Conclusiones: 48
Anexo 1. Cuadro Consolidado de Hallazgos y/o No Conformidades 48

INTRODUCCIÓN

La Oficina de Control Interno, con base en el programa anual de auditorías año 2024 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, con el propósito de verificar el cumplimiento de los criterios de auditoría establecidos en el Plan de Auditoría.

Este informe presenta los resultados de la Auditoría Interna en cuanto al cumplimiento de la gestión realizada y los requisitos del Sistema de Gestión de Seguridad de la Información, que incluyen principalmente, fortalezas, recomendaciones, así como las desviaciones detectadas en relación con el incumplimiento 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, para el periodo con corte a diciembre de 2023 y septiembre año 2024.

3. Criterio(s) de la Auditoría:

- Normatividad legal Vigente.
- Normas y documentos al interior de la Personería de Bogotá D.C.
- Capítulos y numerales de las Norma ISO 27001:2013.
- Caracterización del Proceso Dirección de Tecnologías de la Información y las Comunicaciones.
- Requisitos de la organización, legales, cliente y las partes interesadas.
- Riesgos de Seguridad de la información.
- Documentación del Sistema de Gestión de Seguridad de la Información de la Personería de Bogotá.

4. Resultados de la Auditoría:

La Personería de Bogotá establece que la información es uno de los activos más importantes para las organizaciones y particularmente para la Personería de Bogotá D.C., en cumplimiento de su misión y sus objetivos, es indispensable establecer estrategias y mecanismos que contribuyan a la protección de la seguridad de la información institucional, independientemente del personal que interactúe con ella y del medio en que se trate, transporte o almacene.

Por lo anterior, se implementó, se mantiene y se mejora el Sistema de Gestión de Seguridad de la Información para todos los procesos de la Entidad, donde se establecen políticas, lineamientos acordes con los requisitos establecidos en la NTC ISO 27001:2013.

Metodología

La presente auditoría se desarrolló de manera presencial y a distancia, conforme al Plan de Auditoría allegado en su oportunidad.

A través del correo institucional se remitieron cuestionarios con solicitud de información y se realizaron entrevistas presenciales, por medio de los cuales se aportaron soportes y evidencias que corroboraron el cumplimiento de los criterios definidos para la auditoría, verificando los aspectos relacionados con la gestión realizada y la aplicación de los requisitos del Sistema de Gestión de Seguridad de la Información Norma ISO 27001:2013, en el periodo comprendido entre diciembre de 2023 y septiembre año 2024.

A continuación, se presentan los resultados obtenidos en el proceso de auditoría, las fortalezas, recomendaciones y conclusiones para la mejora continua del mismo.

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

Durante la Auditoría Interna al Sistema de Gestión de Seguridad de la Información, se verificaron los requisitos establecidos en la Norma ISO 27001:2013 y es así como en las listas de chequeo se revisaron los numerales detallados a continuación, evidenciando que se cumplen los requisitos legales, lineamientos y reglamentos de la Personería, las partes interesadas y los establecidos en las normas, así:

4. Resultados de la Auditoría:

CAPITULO NORMA ISO 27001:2013	NUMERALES DE LA NORMA ISO 27001:2013	TITULO GENERAL
4. Contexto de la Organización	Numeral 4.1	Conocimiento de la Organización y de su Contexto
	Numeral 4.2	Comprensión de las Necesidades y Expectativas de las Partes Interesadas.
	Numeral 4.3	Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información
	Numeral 4.4	Sistema de Gestión de Seguridad de la Información
5. Liderazgo	Numerales 5.1	Liderazgo y Compromiso
	Numerales 5.2	Política
	Numerales 5.3	Roles, Responsabilidades y Autoridades en la Organización
6. Planificación	Numeral 6.1 (6.1.1, 6.1.2, 6.1.3)	Acciones para Tratar Riesgos y Oportunidades
	Numeral 6.2	Objetivos de Seguridad de la Información y Planes para lograrlos
7. Soporte	Numeral 7.1	Recursos
	Numeral 7.2	Competencia
	Numeral 7.3	Toma de Conciencia
	Numeral 7.4	Comunicación
	Numeral 7.5 (7.5.1,7.5.2 y 7.5.3)	Información Documentada
8. Operación	Numeral 8.1	Planificación y Control Operacional
	Numeral 8.2	Valoración de Riesgos de la Seguridad de la Información
9. Evaluación del Desempeño	Numeral 9.1	Seguimiento, Medición, Análisis y Evaluación
	Numeral 9.3	Revisión por la Dirección
10. Mejora	Numeral 10.1	No Conformidades y Acciones Correctivas
	Numeral 10.2	Mejora Continua

Fuente: Oficina de Control Interno-OCI.

4. Resultados de la Auditoría:

CONTEXTO DE LA ORGANIZACIÓN

Conocimiento de la Organización y de su Contexto

El proceso DTIC informa que las cuestiones externas e internas se llevaron a cabo mediante un análisis del contexto interno y externo para identificar los factores que afectan la capacidad de su Sistema de Gestión de la Seguridad de la Información (SGSI) y cumplir con los resultados previstos. Este análisis incluyó:

Cuestiones Internas:

- Sector
- Estructura organizacional
- Objetivos estratégicos
- Servicios brindados
- Sistemas de información
- Ubicación
- Visión, misión
- Mapa de procesos
- Procesos e instancias para la toma de decisiones y modelos adoptados por la entidad
- Procesos y procedimientos
- Concientización y capacitación
- Normatividad (Regulación interna)

Cuestiones Externas:

- Marco Legal y Regulatorio
- Proveedores y Terceros
- Tecnología
- Grupos de interés

Así mismo, el proceso DTIC hace entrega como evidencia documento con el análisis del Contexto 2024; verificado el documento por parte del auditor se logró evidenciar que el documento se encuentra estructurado con los siguientes temas:

Introducción, comprensión de la organización y de su contexto, contextos interno y externo que influyen en la personería bajo la norma ISO 27001. Además, los contextos internos, externo y de riesgos, los grupos de interés, la definición del alcance del SGSI y la matriz DOFA.

4. Resultados de la Auditoría:

Una vez revisada la información se concluye que el documento es conforme, sin embargo, se precisan las siguientes recomendaciones:

"Incluir en la matriz DOFA con el cruce de las variables para determinar las estrategias adoptadas por la Entidad para el desarrollo del SGSI."

"Complementar el documento del contexto con el desarrollo de la metodología PESTAL en donde se incluya los entornos político, económico, social, tecnológico ambiental y legal."

"Desarrollar el entorno tecnológico frente a los requerimientos de la institución y en cumplimiento de la normatividad legal vigente."

"Incluir en el documento de contexto la matriz de comprensión de las necesidades y expectativas de las partes interesadas para la seguridad de la información."

"Unificar el documento del contexto del SGSI al documento contexto de la organización de los sistemas de gestión de calidad y seguridad y salud en el trabajo."

Comprensión de las Necesidades y Expectativas de las Partes Interesadas

La Entidad determinó las partes interesadas del Sistema de Gestión de Seguridad de la información a partir de la documentación existente en la entidad, se realizó un análisis del entorno interno y externo en el cual se identifican las personas o grupos que pueden verse afectados por la seguridad de la información en la Personería de Bogotá, D.C. y posteriormente se clasifican y documentan en la matriz *"COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS PARA SEGURIDAD DE LA INFORMACIÓN".*

ANALISIS INTERNO

- **Colaboradores**: Desde la alta dirección hasta los (las) empleados(as) contratistas, quienes tienen un papel clave en la gestión de la seguridad de la información.
- **Procesos institucionales**: las diferentes instancias y/o dependencias (oficinas, delegadas, personerías locales entre otras que deben cumplir con las políticas de seguridad, incluido el Comité Institucional de Gestión y Desempeño de la entidad) y que de una u otra forma se ven afectadas por la seguridad de la información.

4. Resultados de la Auditoría:

- **Responsables de la seguridad**: Personal encargado de la implementación y supervisión del SGSI, como los responsables de sistemas y el oficial de seguridad de la información.

ANALISIS EXTERNO

- **Proveedores y terceros**: Especialmente aquellos que tienen acceso a los sistemas o información de la organización y deben cumplir con los mismos estándares de seguridad.
- **Entidades reguladoras**: Entidades encargadas de emitir regulaciones y/o legislaciones relacionadas con la seguridad de la información.
- **Comunidad en general:** Quienes utilizan los servicios prestados por la Personería en cumplimiento de sus funciones.
- **Auditores externos**: Organismos que revisan el cumplimiento de la seguridad de la información y los controles implementados en el SGSI.

Por otra parte, los requisitos de las partes interesadas pertinentes a la seguridad de la información se definieron mediante un proceso que incluyó la identificación de las partes interesadas internas y externas que tienen un interés en la seguridad de la información, tales como:

- Comité Institucional de Gestión y Desempeño - Interna
- Procesos institucionales - Interna
- Colaboradores (funcionarios(as) y contratistas) - Interna
- Ciudadanía – Externa
- Empresas de Servicios – Externa
- Autoridades legislativas– Externa
- Contratistas (Proveedores) – Externa
- Colcert /Cisrt – Externa

Así mismo, se analizan las necesidades y expectativas de las partes interesadas teniendo en cuenta los requisitos legales y reglamentarios, tecnológicos, obligaciones contractuales cuando dé a lugar, políticas y procedimientos internos; estos requisitos fueron documentados en el sistema de gestión, a través de un documento de *"Comprensión de las necesidades y expectativas de las partes"*

La Dirección de Tecnologías de la Información y las Comunicaciones hace entrega de las siguientes evidencias: Matriz de comprensión de las necesidades y expectativas de las partes interesadas para seguridad de la información, matriz contactos con grupos de interés y autoridades SGSI y la matriz de requisitos legales.

4. Resultados de la Auditoría:

Se realizó la verificación del cumplimiento de los requisitos legales del sistema de gestión de seguridad de la información de acuerdo con la normatividad establecida en la matriz de requisitos legales donde se evidenció el cumplimento de algunas normas por muestreo como la ley 1266 de 2008, ley 415 de 2026 y la resolución 460 de 2022, en la revisión se logró establecer que hay algunas nomas que son de Tecnologías de la Información que aplican al proceso, pero no al SGSI.

Por lo anterior, se recomienda: *"Realizar actualización de la matriz de requisitos legales del proceso DTIC frente al SGSI"*

De la misma manera, el proceso informa que se realizará la depuración de la matriz de requisitos legales y se actualizará en la primera semana del mes de diciembre actividad que se encuentra programada en el plan de trabajo SGSI 2024-2025. Además, informan que como fuente de información de la normatividad vigente se cuenta en permanente contacto con el WhatsApp de la Alta Consejería Pública.

Verificada la documentación por parte del auditor se determina que esta es conforme y cumple con los requisitos establecidos por la norma ISO 27001:2013.

Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información

El alcance del SGSI de la Personería de Bogotá D.C. ha sido definido a partir de un análisis del contexto organizacional, identificando a las partes interesadas y sus respectivos requisitos; se incluyeron como partes interesadas los funcionarios, proveedores y terceros relevantes, además, se analizaron los procesos, sistemas y datos críticos de la organización, los requisitos de las partes interesadas se documentaron en el informe titulado *"Necesidades y expectativas de las partes interesadas – Personería".* El alcance del SGSI abarca todos los procesos de la entidad, clasificados en procesos estratégicos, misionales, de apoyo, y de evaluación, seguimiento y control.

Verificado el documento del alcance del SGSI se evidenció que este cumple con los requisitos de la norma ISO 27001:2013. Así mismo, revisado el alcance del SGSI que se encuentra publicado en la página web es diferente al que se describe en el documento del contexto del SGSI y diferente al documento entregado como soporte.

4. Resultados de la Auditoría:

De la misma manera, se evidencia que la información respecto al alcance del SGSI no es integra y confiable, incumpliendo los principios de integralidad y confidencialidad de la información que están enmarcados en el mismo alcance.

Por lo anterior, se recomienda: *"Mantener la integridad y confiabilidad de la información respecto al alcance del SGSI en los documentos y plataformas donde se públique esta información"*

Sistema de Gestión de la Seguridad de la Información

El SGSI de la Personería ha incluido en su alcance a todos los procesos de la entidad, estratégicos, misionales, de apoyo y de evaluación, seguimiento y control; adicionalmente, la política del SGSI aplica para todos los servidores de la entidad, contratistas, proveedores y demás partes interesadas, comprometiéndose en todos los niveles institucionales con la implementación mantenimiento y mejora continua del SGSI.

Por otra parte, mediante resolución 250 de 2023 se designan los responsables del Sistema de Gestión de Seguridad de la Información SGSI y la resolución 242 de 2023, adopta el *"Sistema de Gestión de la Seguridad de la Información SGSI bajo la NTC-ISO 27001 en la Personería de Bogotá, D.C."* y el Comité Institucional de Gestión y Desempeño aprueba el plan de implementación de seguridad y privacidad de la información.

LIDERAZGO

LIDERAZGO Y COMPROMISO

La alta dirección demuestra su liderazgo y compromiso con el sistema de gestión de la seguridad de la información mediante la creación y comunicación de una política de seguridad, la asignación de recursos, la definición y cumplimiento de los objetivos de seguridad de la información, la participación activa en revisiones y auditorías, el apoyo en la promoción de la cultura de seguridad en toda la organización, la inclusión de la gestión de los riesgos de seguridad de la información, el cumplimiento de la normatividad y la mejora continua del sistema.

Así mismo, mediante resolución 250 de 2023 se designa al responsable del *Sistema de Gestión de Seguridad de la Información SGSI y la resolución 242 de 2023,*

4. Resultados de la Auditoría:

"..adopta el Sistema de Gestión de la Seguridad de la Información SGSI bajo la NTC-ISO 27001 en la Personería de Bogotá, D.C."., la resolución 285 de 2023 que conforma el Comité de Gobierno Digital y el Comité Institucional de Gestión y Desempeño aprueba el plan de implementación de seguridad y privacidad de la información.

Por otra parte, se evidenció la revisión permanente y la divulgación de políticas del SGSI, además la asignación de los recursos mediante el presupuesto y el plan anual de adquisiciones para cubrir las necesidades de DTIC y el SGSI.

POLÍTICA

La Personería de Bogotá establece su política de seguridad de la información teniendo en cuenta las funciones de la entidad, la alineación de sus objetivos con los objetivos estratégicos, el cumplimiento de los requisitos legales, y la mejora continua; se tienen en cuenta aspectos básicos como la gestión de los riesgos, los principios de confidencialidad, integridad y disponibilidad de la información. La política de seguridad de la información fue comunicada al interior de la organización y se encuentra documentada y disponible para todas las partes interesadas.

Así mismo, la política de seguridad de la información de la Personería de Bogotá D.C. está disponible para todas las partes interesadas y se encuentra debidamente documentada. La política ha sido publicada y está accesible a través del repositorio documental de la entidad, así como en la página web institucional, también se encuentra documentada en el manual de políticas y lineamientos de seguridad de la información en ISOLUCIÓN.

Por otra parte, la política de seguridad de la información se comunica a través de la sensibilización permanente a los funcionarios(as) y contratistas de la entidad por los medios de comunicación institucionales, mediante actividades que son incluidas en el plan de sensibilización, comunicación, inducción y capacitación del SGSI.

Se verificaron los documentos soporte de la política de seguridad de la información de la Personería de Bogotá, el acta de aprobación de la política, la publicación de la política se verificó en el portal web, la intranet, el manual de políticas y lineamientos de seguridad de la información y el plan de sensibilización, comunicación y capacitación del SGSI.

4. Resultados de la Auditoría:

Por lo anterior, el auditor determina que los soportes entregados por el auditado son conformes con los requisitos establecidos en la norma ISO 27001:2013.

ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

La alta dirección ha designado y comunicado las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información, designando a la Dirección de Tecnologías de la información y las Comunicaciones DTIC como responsable del Sistema de Gestión de seguridad de la información SGSI, la adopción del Sistema de Gestión de seguridad de la información SGSI bajo la norma NTC-ISO 27001 y la definición de responsabilidades y forma de designación del Oficial de Seguridad de la Información; así mismo la Dirección DTIC es la encargada de informar sobre el desempeño del SGSI durante la actividad de revisión por la dirección.

Al interior del proceso Direccionamiento TIC, se designó el equipo de Seguridad de la Información, el cual tiene distribuidos los roles y responsabilidades para la implementación, mantenimiento y mejora continua del SGSI.

Se verificaron los documentos donde se establecen los roles y responsabilidades del SGSI mediante las Resoluciones 250, 242 de 2023 y 81 de 2024. Así mismo, los documentos de roles y responsabilidades del SGSI del 10 de agosto de 2023 y del equipo del SGSI.

No obstante, lo anterior se evidencio la siguiente NC: *Verificada la normatividad en la Resolución 500 de marzo 10 de 2021, "señala que se debe designar dentro de la Entidad los responsables de gestionar y dar respuesta a los incidentes de seguridad digital, liderado por el responsable de seguridad digital." Así mismo, la Entidad mediante la Resolución 81 del 22 de febrero de 2024 estableció la designación del Oficial de Seguridad de la Información y sus responsabilidades, sin que a la fecha se haya nombrado a un asesor o profesional de la plata global que cumpla con los requisitos y ejerza las responsabilidades de este rol, incumpliendo los requisitos legales y reglamentarios de la Entidad y el numeral 4.2 literal b) de la Norma ISO 27001:2013.*

Con respecto a la comunicación de los roles y responsabilidades del Sistema de Gestión de Seguridad de la Información, el auditado no presentó evidencias al respecto.

Por lo anterior, el auditor estableció la siguiente NC: *Verificados los roles, responsabilidades y autoridades del SGSI, se evidenció la asignación de estos, sin embargo, no se evidenció la comunicación del documento roles y responsabilidades del*

4. Resultados de la Auditoría:

Sistema de Gestión de Seguridad de la Información SGSI del 10 de agosto de 2023, incumpliendo el numeral 5.3 literal a) de la Norma ISO 27001:2013.

En relación con informar a la alta dirección sobre el desempeño del sistema de gestión de seguridad de la información se presenta documento con el informe de la revisión del Sistema de Gestión de Seguridad de la Información vigencia 2023.

PLANIFICACIÓN

ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES

- **Generalidades**

La Personería de Bogotá al planificar su sistema de gestión de seguridad de la información ha considerado el conocimiento y contexto de la organización, los requisitos de necesidades y expectativas de las partes interesadas, el alcance del Sistema de Gestión de la Información (SGSI), la aplicación de la metodología para la planificación de los riesgos y oportunidades.

Los riesgos de seguridad de la información se identificaron y se registran en la matriz de riesgos institucional, así mismo, se realiza la revisión periódica por cada proceso, para la valoración y tratamiento de estos y alcanzar los resultados previstos.

Además, para reducir los efectos indeseados se realiza el tratamiento de los riesgos aplicando la metodología de gestión de riesgos de la entidad, determinando las acciones que se requieran y seleccionando los controles de seguridad de la información que sean necesarios para mitigar los riesgos identificados a través de la declaración de aplicabilidad y el cumplimiento de las políticas, lineamientos y procedimientos de seguridad de la información, la adecuada gestión de eventos e incidentes de seguridad y el seguimiento y monitoreo continuo.

Para lograr la mejora continua del SGSI se realiza la evaluación periódica de los riesgos de seguridad de la información, el monitoreo y revisión de los controles de seguridad realizado con el instrumento de evaluación del Modelo de Seguridad y Privacidad de la información MSPI, la capacitación y/o sensibilización periódica sobre la importancia de la seguridad de la información para mitigar los riesgos, las auditorías internas periódicas, la documentación y aprendizaje en la gestión de

4. Resultados de la Auditoría:

incidentes, la revisión y/o actualización de políticas y procedimientos y la participación de la alta dirección en la revisión del SGSI y la definición y seguimiento de los objetivos de seguridad de la información.

La gestión de riesgos de seguridad de la información se encuentra integrada en la metodología de gestión de riesgos institucional, mediante la cual se planifican las acciones para tratar los riesgos y oportunidades y se evalúa la eficacia de las acciones de tratamiento de los riesgos mediante el seguimiento continuo a los controles establecidos.

- **Valoración de Riesgos de la Seguridad de la Información**

La evaluación de riesgos de seguridad de la información se encuentra en la metodología de gestión de riesgos institucional, mediante la cual se realiza la identificación, valoración y tratamiento de los riesgos de seguridad de la información.

Los criterios, para la gestión de riesgos de seguridad de la información, se establecieron en la metodología de gestión de riesgos institucional, mediante la cual se realiza la identificación, valoración y tratamiento de los riesgos de seguridad de la información, y en la cual se incluye la referencia para la aplicación de lo establecido en el documento "*Anexo 4 Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas"*, de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas, del Departamento Administrativo de la Función Pública- DAFP (2020) con el fin de garantizar la correcta gestión de los riesgos de seguridad de la información.

Así mismo, la identificación, evaluación y análisis de los riesgos de seguridad de la información se encuentran en el desarrollo de la matriz de riesgos institucionales, el seguimiento de manera cuatrimestral, además del desarrollo del plan de tratamiento de riesgos de seguridad y privacidad de la información

De la misma manera, la información correspondiente al proceso de valoración de riesgos de seguridad de la información se encuentra documentada en portal de intranet, los repositorios del sistema de Gestión de Seguridad de la Información SGSI de la DTIC y en la oficina de planeación quien es la encargada de consolidar y documentar la información correspondiente a la gestión del riesgo para todos los procesos de la entidad, incluidos los riesgos de seguridad de la información.

4. Resultados de la Auditoría:

Por otra parte, el proceso entrega como evidencia de la gestión de riesgos los documentos guía de administración de riesgos, matriz de riesgos institucional, plan de tratamiento de riesgos de seguridad de la información y el informe de gestión de riesgos de seguridad de la información.

- **Tratamiento de Riesgos de la Seguridad de la Información**

Las opciones de tratamiento de los riesgos de seguridad de la información se seleccionan mediante la aplicación de la metodología de gestión de riesgos institucional, y en la cual se incluye la referencia para la aplicación de lo establecido en el documento *"Anexo 4 Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas"*, de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas, del Departamento Administrativo de la Función Pública- DAFP (2020) con el fin de realizar la correcta gestión de los riesgos de seguridad de la información.

La Entidad estableció los controles necesarios para la implementación de las acciones de tratamiento y estos se encuentran registrados en la matriz de riesgos institucional el cual incluye los riesgos de seguridad de la información, acorde con lo establecido en la metodología de gestión de riesgos institucional.

Por otra parte, la Entidad cuenta con la Declaración de Aplicabilidad en el formato 03-FR-23 Versión 3 de fecha 14/04/2023. Documento que se encuentra actualizado y en el mismo se incluye la justificación y las razones de adopción de cada control.

Así mismo, la Declaración de Aplicabilidad contiene los controles aplicados para el tratamiento de los riesgos identificados en la entidad; y se realiza el monitoreo y revisión de dichos controles de seguridad con el instrumento de evaluación del Modelo de Seguridad y Privacidad de la información MSPI.

Además, se formuló el Plan de Tratamiento de Riesgos de la Seguridad de la información, documento que a través del Comité Institucional de Gestión y Desempeño se aprobó la actualización general del documento Versión 4 de fecha 25/01/2024.

Por otro lado, la aprobación del plan de tratamiento de riesgos por parte de los dueños de los riesgos, se logró mediante la aplicación de la metodología de gestión de riesgos institucional y la aprobación del plan de tratamiento de riesgos por el Comité Institucional de Gestión y Desempeño.

4. Resultados de la Auditoría:

Con respecto a la información documentada del proceso de tratamiento de riesgos de seguridad de la información, la Dirección de Tecnologías de la Información y las Comunicaciones informa que la información correspondiente al tratamiento de riesgos de seguridad de la información se encuentra documentada en los repositorios del sistema de Gestión de Seguridad de la Información SGSI de la DTIC, en la intranet y en la oficina de planeación quien es la encargada de consolidar y documentar la información correspondiente a la gestión del riesgo para todos los procesos de la entidad, incluidos los riesgos de seguridad de la información.

Durante la auditoría al proceso DTIC, se preguntó si la Entidad en el presente año había realizado un estudio de vulnerabilidades del sistema a lo cual el auditado respondió que el último estudio se había realizado en el año 2023 y posteriormente se establecieron las acciones pertinentes para cerrar las brechas y garantizar la seguridad de la información. Verificado el seguimiento de las vulnerabilidades se observa que algunas de ellas no se encuentran cerradas.

Teniendo en cuenta lo anterior, se establecen las siguientes recomendaciones:

"Realizar la actualización del estudio de vulnerabilidades del sistema de información de la Entidad."

"Identificar los riesgos de seguridad de la información teniendo en cuenta la criticidad de los activos de información.

"Establecer una matriz de riesgos del SGSI en donde se evidencie los riesgos identificados de las vulnerabilidades del sistema de información y los riesgos que se establecen respecto a los controles implementados del documento Declaración de Aplicabilidad en cumplimiento del anexo A de la norma ISO 27001:2022"

"Actualizar el documento Declaración de Aplicabilidad de acuerdo con los controles establecidos en el Anexo A de la norma ISO 27001:2022"

Finalmente, las evidencias entregadas por el proceso auditado, se puede establecer que estos cumplen con los criterios establecidos en la norma ISO 27001:2013.

4. Resultados de la Auditoría:

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS

Los objetivos de seguridad de la información fueron actualizados en reunión del Comité Institucional de Gestión y Desempeño según acta del 20/07/2023.

- Objetivo 1. Identificar e implementar mecanismos para lograr el cumplimiento de la normatividad y estándares en seguridad de la información
- Objetivo 2: Fortalecer la cultura y apropiación en seguridad de la información para los(as) servidores (as) y terceros(as) de la Personería de Bogotá D.C.
- Objetivo 3. Realizar una adecuada gestión de riesgos e incidentes de Seguridad de la Información
- Objetivo 4. Implementar los controles establecidos en la declaración de aplicabilidad de la Norma ISO 27001.
- Objetivo 5. Proteger los activos de información mediante la implementación de políticas, procedimientos y controles

Los objetivos del SGSI permiten evidenciar la coherencia con la Política de Seguridad de la Información a través de su alineación con los objetivos estratégicos de la entidad, en ellos se hace referencia a una adecuada gestión del riesgo, el cumplimiento de los requisitos normativos en materia de seguridad de la información, el fortalecimiento de la cultura y apropiación en seguridad y la comunicación constante con la alta dirección y los procesos institucionales.

Por otra parte, los objetivos del SGSI, permiten ser medibles y alcanzables, mediante la aplicación de la *"Matriz de seguimiento de objetivos del SGSI"* donde se encuentran registradas las mediciones de los objetivos, así mismo se encuentran alineados con la norma ISO 27001:2013 ya que contemplan aspectos relacionados con normatividad, uso y apropiación, gestión de riesgos, controles y la gestión de activos de información.

Así mismo, la información correspondiente a los objetivos de seguridad de la información se encuentra documentada en los repositorios del sistema de Gestión de Seguridad de la Información SGSI de la DTIC y en la intranet institucional.

Verificados los objetivos del SGSI, se observó que el Objetivo 4. Implementar los controles establecidos en la declaración de aplicabilidad de la Norma ISO 27001, es una obligatoriedad de la norma y por lo tanto es una actividad que ya se realizó

4. Resultados de la Auditoría:

en el proceso de implementación del SGSI, situación por la cual no amerita tener este objetivo como parte del SGSI.

Por lo anterior, se recomienda: *"Actualizar el objetivo No 4 en la Revisión por la Dirección y plantear otro objetivo si así lo determina la alta dirección."*

"Realizar seguimiento a los planes del SGSI, mediante la utilización de códigos de colores para distinguir cada tema"

SOPORTE

- **RECURSOS**

El proceso DTIC informa que: La entidad realiza las actividades necesarias para determinar y proporcionar los recursos necesarios para establecer, implementar, mantener y mejorar el SGSI, a través de:

Determinación de recursos*:* Mediante la identificación del estado actual de la entidad y sus necesidades frente a los requisitos de la NTC-ISO-IEC 27001:2013 lo que proporciona un punto de partida para establecer el SGSI; la evaluación y tratamiento de riesgos de seguridad de la información, permite identificar los activos de información que deben ser protegidos de las diferentes amenazas y vulnerabilidades y contribuye a la determinación de los recursos necesarios para mitigar los riesgos identificados, y la definición de los objetivos de seguridad de la información alineados a los objetivos estratégicos de la entidad, facilita la correcta asignación de los recursos.

Asignación de recursos*:* A través de la designación de responsables del SGSI y del recurso humano capacitado, así como la definición de los roles necesarios para la conformación del equipo que atenderá las actividades requeridas por el SGSI; la adquisición de herramientas tecnológicas como software y equipos de seguridad y protección de datos; la asignación de rubro presupuestal para cubrir las necesidades de mantenimiento y mejora continua del SGSI, incluido adquisición y capacitación de personal, consultorías, adquisición de herramientas tecnológicas, software y servicios de seguridad, etc.; la definición de políticas, procedimientos y documentación requerida para el cumplimiento de los requisitos de seguridad y la información NTC-ISO-IEC 27001:2013, y la inclusión del SGSI en los planes de auditoría y revisiones por la dirección para garantizar el proceso de evaluación, revisión periódica y mejora continua del sistema.

4. Resultados de la Auditoría:

Verificada la información por parte del auditor, se logó evidenciar que el Sistema de Gestión de Seguridad de la Información cuenta con 3 profesionales en ingeniería de sistemas y especialización, todos certificados en norma ISO 27001:2022.

Los ingenieros que son responsables de varios temas entre los cuales se encuentran, la ciberseguridad e incidentes, uso y apropiación, gobierno de seguridad, inventario de activos y partes interesadas.

No obstante, se recomienda: *"Continuar fortaleciendo el SGSI y la DTIC con personal."*

"Continuar fortaleciendo la infraestructura tecnológica hardware y software para la seguridad de la información."

Se puede establecer que la Entidad determinó y proporciono los recursos en su presupuesto para el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.

- **COMPETENCIA**

La Entidad realiza el análisis de competencias para el personal que realiza actividades relacionadas con seguridad de la información, de acuerdo con las necesidades y tareas que serán ejecutadas por ellos; se cuenta con un procedimiento de vinculación de servidores y manual específico de funciones para funcionarios de planta y requisitos de formación y experiencia para personal contratista. De igual manera, la resolución 81 de 2024 establece los requisitos de formación académica y experiencia para el oficial de seguridad de la información.

Por otra parte, la Entidad asegura que el personal de seguridad de la información sea competente en la realización de sus labores por lo cual se solicitan las certificaciones de formación según las actividades a realizar, para esto se tienen en cuenta los títulos de educación formal, estándares internacionales y certificaciones de experiencia.

Así mismo, la Entidad capacita al personal en asuntos relacionados con seguridad de la información; para esto se tienen en cuenta aspectos como la programación del plan institucional de capacitación y las obligaciones específicas de los contratos.

De igual manera, la Entidad cuenta con la conservación de documentación relacionada con las competencias de los funcionarios y contratistas que realizan

4. Resultados de la Auditoría:

labores en seguridad de la información, estos documentos se encuentran en las carpetas de historia laboral en el archivo de la Subdirección de Gestión del Talento Humano, expedientes contractuales para los contratos de consultoría y prestación de servicios en la Subdirección de Gestión Contractual y las carpetas de la ejecución contractual ubicadas en los repositorios de la Dirección DTIC.

- **TOMA DE CONCIENCIA**

La política de seguridad de la información se divulga y socializa al interior de la Entidad a través de diferentes actividades y medios de comunicación, como las jornadas de inducción de nuevos funcionarios, publicación en portales web e intranet institucional y actividades programadas en el plan de comunicación, sensibilización y capacitación del SGSI; de igual manera, los formatos de compromiso de confidencialidad y no divulgación de información para proveedores, funcionarios y contratistas, establecen el compromiso de conocer y acatar las políticas del SGSI.

Desde la Dirección de Tecnologías de la Información se han realizado actividades de comunicación y sensibilización permanente para generar una cultura organizacional y conciencia en los colaboradores de la entidad para los asuntos relacionados con la seguridad de la información y su importancia para el cumplimiento de los objetivos del SGSI; para esto se cuenta con el procedimiento de atención de eventos e incidentes de seguridad de la información y se programan actividades de capacitación y sensibilización a través del plan de comunicación, sensibilización y capacitación del SGSI, y sus resultados se ven reflejados en la participación de las actividades de capacitación y sensibilización programadas, en los reportes de eventos y/o incidentes de seguridad recibidos a través de los diferentes medios dispuestos y en la no materialización de riesgos de seguridad de información atribuibles a la falta de conciencia de las personas.

Respecto a la toma de conciencia de las implicaciones de las No Conformidades, la Dirección de Tecnologías de la Información y las Comunicaciones ha realizado la divulgación de las políticas y lineamientos de seguridad de la información, el manual de políticas y lineamientos de seguridad de la información, con el propósito de informar sobre las posibles consecuencias por el incumplimiento de las políticas establecidas por la entidad, también se han realizado encuestas con la participación de funcionarios y contratistas para determinar el compromiso respecto a la seguridad de la información. Así mismo, el compromiso de la entidad en la atención de las auditorías programadas del SGSI, y la definición y desarrollo

4. Resultados de la Auditoría:

de los planes de mejoramiento acordados que contribuyen a la mejora continua del sistema.

No obstante, se recomienda: *"Continuar fortaleciendo la toma de conciencia del SGSI."*

- **COMUNICACIÓN**

La Personería ha determinado la necesidad de las comunicaciones internas y externas, mediante la definición de la matriz de comunicaciones del SGSI, el plan de comunicación, sensibilización y capacitación del SGSI, la identificación de contactos con grupo de interés y durante al análisis del contexto se realizó la identificación y análisis de las partes interesadas internas y externas con quienes la Entidad debe permanecer en constante comunicación.

Los procesos de comunicación se llevan a cabo mediante la aplicación de la matriz de comunicaciones del SGSI, el plan de comunicación, sensibilización y capacitación del SGSI y el cumplimiento de la guía de comunicaciones de la entidad.

Verificadas las evidencias y realizados los muestreos para determinar la aplicabilidad de los instrumentos de comunicación establecidos por la Entidad, el auditor determina que es conforme con los requisitos de la norma ISO 27001:2013.

INFORMACIÓN DOCUMENTADA

Generalidades

La Dirección de Tecnologías de la Información y las Comunicaciones ha identificado los documentos que hacen parte de los requisitos de NTC-ISO-IEC 27001, y los demás que la entidad considera necesarios para garantizar la correcta implementación y eficacia del SGSI; para esto, se cuenta con el documento *"Inventario documental del SGSI"*, en el cual se registran los documentos que hacen parte del sistema de Gestión de Seguridad de la Información SGSI. Teniendo en cuenta lo anterior, se determinó documentar los planes, procedimientos, manuales, guías y formatos del SGSI.

Con respecto a la información documentada el auditor evidenció que el Proceso Direccionamiento de Tecnologías de la Información y las Comunicaciones cuenta con la siguiente documentación: 26 Formatos, 15 Procedimientos, 1

4. Resultados de la Auditoría:

Caracterización del Proceso, 8 Planes, 1 Manual, 1 Instructivo y 20 Guías para un total de 68 documentos controlados.

La información anterior fue verificada por el auditor en el aplicativo ISOLUCION encontrando consistencia en la información reportada por el proceso en donde los documentos tienen la siguiente participación:

DOCUMENTOS DTIC	TOTAL	% Participación
PROCEDIMIENTOS	15	21%
PLANES	8	11%
MANUALES	1	1%
INSTRUCTIVOS	1	1%
GUIAS	20	28%
FORMATOS	26	36%
CARACTERIZACIÓN	1	1%
TOTAL	**72**	**100%**

Fuente: Documentos DTIC Aplicativo ISOLUCION.

El Sistema de Gestión de Seguridad de la información cuenta con información documentada la cual se encuentra relacionada en el *"Inventario documental del SGSI"* y los documentos se encuentran almacenados en un repositorio del OneDrive institucional debidamente organizados según los requisitos y controles de la NTC-ISO-IEC 27001:2013. Así mismo, la documentación del SGSI que requieren ser controlados como parte del Sistema de Gestión de Calidad se encuentran publicados en el aplicativo ISOLUCION.

La socialización de los documentos del SGSI se encuentra programada en el Plan de comunicación, sensibilización y capacitación del SGSI y los documentos del SGSI se publican en los portales web e intranet.

- **Creación y Actualización**

La información documentada del SGSI se estructura de acuerdo con los lineamientos establecidos por el Sistema de Gestión de Calidad de la entidad, a través del "P*rocedimiento para la creación, actualización, eliminación y control de documentos controlados"* y la *"Guía para la elaboración de documentos controlados",* lo

4. Resultados de la Auditoría:

cual garantiza que los documentos cumplan con los requisitos de estandarización, codificación, versión, estructura y diseño corporativo.

Por otra parte, la información documentada del SGSI se gestiona de acuerdo a los lineamientos establecidos por el Sistema de Gestión de Calidad de la entidad, a través del *"Procedimiento para la creación, actualización, eliminación y control de documentos controlados"* y la *"Guía para la elaboración de documentos controlados",* lo cual garantiza que la creación de los documentos cumplan con los requisitos procedimentales de calidad como son la revisión metodológica y la aprobación por el Comité Institucional de Gestión y Desempeño.

Verificada la documentación frente a los lineamientos internos respecto a la información documentada se puede observar que los documentos se encuentran identificados, cuentan con un título, fecha, autor y numero de referencia.

Además, todos e encuentran en idioma español y versionados, tienen medios de soporte físico en papel y electrónicos, también están revisados y aprobados por lo cual se puede establecer que son idóneos y adecuados para el SGSI.

- **Control de la Información Documentada**

La información documentada del SGSI se controla de acuerdo a los lineamientos establecidos por el Sistema de Gestión de Calidad de la entidad, a través del *"Procedimiento para la creación, actualización, eliminación y control de documentos controlados",* se encuentra ubicada para su consulta en el sistema de información ISOLUCION el cual es administrado funcionalmente por el proceso Direccionamiento Estratégico y para el almacenamiento de la información de gestión institucional los procesos cuentan con el servicio de ONEDRIVE de Microsoft. Los de gestión del SGSI por parte de la dirección DTIC se encuentran almacenados en un repositorio del OneDrive institucional debidamente organizados según los requisitos y controles de la NTC-ISO-IEC 27001:2013.

Respecto a la disponibilidad, idoneidad y uso cuando se requiera la información documentada se encuentra en el aplicativo ISOLUCION, así mismo, la información documentada se encuentra ubicada en los servidores administrados por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, y cuentan con la realización de Backups de seguridad que garantizan su disponibilidad y con acuerdos de niveles de servicio para el caso de contratación de servicio ONEDRIVE de Office 365; respecto de la idoneidad para su uso donde y cuando se requiera, el acceso al aplicativo ISOLUCION y al ONEDRIVE institucional de

4. Resultados de la Auditoría:

Office 365 se encuentran publicados en el portal de intranet y web de la Personería, a los cuales se puede acceder desde cualquier navegador de internet mediante autenticación por usuario y contraseña del directorio activo de la entidad.

Por otra parte, la información documentada del aplicativo ISOLUCION y ONEDRIVE institucional de Office 365 se encuentra protegida en los servidores de la entidad a los cuales se realizan los correspondientes Backups de seguridad, y con acuerdos de niveles de servicio para el caso de contratación de ONEDRIVE de Office 365. Su acceso se realiza mediante usuario y contraseña del directorio activo garantiza que la información sea accesible únicamente por las personas autorizadas y adicionalmente, el protocolo https cifra la comunicación entre el servidor y el navegador de internet del usuario, garantizando la confidencialidad e integridad de la información.

Así mismo, la información institucional se conserva de acuerdo con los lineamientos y procedimientos establecidos por el proceso Gestión Documental, alineados a la normatividad legal vigente en lo relacionado con la organización, control, transferencia y conservación de documentos; la información y documentos controlados del Sistema de Gestión de calidad cuenta con su respectivo control de cambios y versión.

Respecto al control de la información externa se establecen los correspondientes compromisos de confidencialidad y no divulgación de información para proveedores de bienes y/o servicios, se cuenta con políticas de control a la red de datos y transferencia de la información y la implementación de VPN para garantizar la comunicación segura desde el exterior.

Durante la auditoria se realiza muestreo para la revisión del control de documentos encontrando la siguiente NC: "*Verificada la documentación del SGSI para el control de documentos, se evidenció que el formato de compromiso de confidencialidad y no divulgación de la información para funcionarios y vinculados temporalmente a la entidad código 03-FR-22 versión 2 vigente desde el 26/05/2020 de la contratista Stefany Cabrales Madrid, no se encuentra controlado respecto al formato oficial publicado en el aplicativo Isolución que tiene fecha de vigencia 13/02/2024, incumpliendo el numeral 7.5.3 literal b) de la norma ISO 2700:2013".*

Además, se recomienda: "*Actualizar el formato autorización para acceso permanente a centros de cómputo y cableado código 03-FR-19 versión 1 vigente desde el 14/08/2019, en la medida que el formato se encuentra con un logo de una administración anterior y la autorización corresponde al Director de TIC de unas administraciones anteriores."*

4. Resultados de la Auditoría:

OPERACIÓN

- **PLANIFICACIÓN Y CONTROL OPERACIONAL**

El SGSI se implementa a través de un enfoque estructurado y sistemático, teniendo en cuenta las fases del ciclo PHVA (Planificar, hacer, verificar y actuar), para garantizar que los procesos se planifiquen, implementen y controlen efectivamente.

Así mismo, la planificación se establece a partir del compromiso de la alta dirección y la elaboración de un diagnóstico inicial identificando los requisitos para la implementación del SGSI y el estado actual de la entidad frente a estos requisitos (Análisis de brechas), se elabora el plan para la implementación del SGSI (Plan de seguridad y privacidad de la información) que define las actividades programadas para dar cumplimiento a los objetivos de seguridad de la información y los requisitos de la Política de gobierno digital de MINTIC y la norma NTC-ISO-IEC 27001.

De la misma manera, la planificación y control operacional se logra mediante el cumplimiento de las políticas, lineamientos y procedimientos de seguridad, la ejecución de los controles aplicables y la implementación de planes para lograr los objetivos de seguridad de la información.

Así mismo, la entidad cuenta con procedimiento de gestión de cambios para controlar los cambios planificados; en caso de presentarse cambios no previstos se analizan las consecuencias de estos y se documentan las lecciones aprendidas para prevenir que se presenten situaciones recurrentes, esto se incluye en el procedimiento de gestión de incidentes de seguridad de la información y el procedimiento de monitoreo de eventos e incidentes informáticos.

Por otra parte, la entidad se asegura que los procesos contratados externamente estén controlados mediante la ejecución de procedimientos establecidos en el manual de contratación, a través de la evaluación de proveedores, el análisis de los riesgos, la inclusión en los contratos de obligaciones relacionadas con la seguridad de la información, el manejo de datos sensibles, el cumplimiento de las políticas y lineamientos de seguridad de la información, la suscripción de compromisos de confidencialidad y no divulgación de la información y el seguimiento continuo a través de la supervisión del contrato.

4. Resultados de la Auditoría:

Durante la auditoría se realizaron muestreos de la documentación que soporta el control operacional del SGSI, es así como se revisaron los siguientes procedimientos: Gestión de Incidentes de Seguridad de la Información código 03-PT-014 versión 1 vigente desde el 27/07/2023, en el mencionado procedimiento se establece como control a la gestión realizada la aplicación del formato Eventos y/o Incidentes Informáticos y de la Seguridad de la Información código 03-FR-07 versión 2 vigente desde el 21/07/2023.

Se observaron los seguimientos durante las vigencias 2023 y 2024, encontrando que los tiempos para solucionar un evento o un incidente de seguridad de la información son muy altos, teniendo en cuenta que se han definido variables de severidad e impacto para la atención del servicio.

Sin embargo, solo se hace seguimiento a los tiempos de solución del evento o incidente, por lo que se recomienda: "*Realizar seguimiento a los tiempos de atención de los eventos e incidentes."*

"Revisar el procedimiento para verificar los acuerdos de niveles de servicio para determinar los tiempos de solución de un evento o incidente teniendo en cuenta la severidad e impacto."

Cuando se presenta un evento que pueda afectar la prestación de los servicios, se aplica al interior de la institución el respectivo plan de contingencia de tecnologías de la información.

Por otra parte, se realizó la verificación del Procedimiento Gestión de Monitoreo de Eventos e Incidentes Informáticos código 03-PT-10 versión 1 vigente desde el 21/07/2023, encontrando que existe similitud con el procedimiento Gestión de Incidentes de Seguridad de la Información código 03-PT-014 versión 1 vigente desde el 27/07/2023 por lo que se recomienda:

"Revisar los procedimientos 03-PT-10 versión 1 y el procedimiento 03-PT-14 versión 1 para determinar si técnicamente es posible unificarlos en uno solo."

Así mismo, se realizó la verificación del Procedimiento Gestión de Cambio código 03-PT-04 versión 2 vigente desde el 12 de agosto de 2019, se observó que el procedimiento aplica los controles establecidos en los formatos solicitud de cambios código 03-FR-15, bitácora RFC cambio estándar y el formato código 03-FR-17 bitácora RFC cambio general, encontrándolos conformes sin embargo se recomienda lo siguiente: *"Revisar el procedimiento gestión de cambio y establecer la trazabilidad del cambio general y cambio estándar."*

4. Resultados de la Auditoría:

El auditor solicita el ingreso al centro de cómputo y cableado para observar el Procedimiento de Ingreso a Centro de Cómputo y Cableado con sus respectivos controles.

NC: *Verificado el Procedimiento de Ingreso a Centros de Cómputo y Cableado código 03-PT-05 versión 1 vigente desde el 14 de agosto de 2019, se ingresa al centro de cómputo y cableado se realiza recorrido y toma de fotografías sin ningún tipo de registro para su ingreso, así mismo se verificó el diligenciamiento del formato bitácora de acceso a centro de cómputo y cableado código 03-FR-20 versión 1, encontrándolo que faltaban espacios por diligenciar como las horas de salida, elementos ingresados, funcionario responsable de la actividad, firma del visitante, nombre y firma de quien autoriza, contraviniendo las políticas de operación 4.4,4.6 y 4.7 establecidas en el procedimiento e incumpliendo el control A.11.1.2 controles de acceso físico, los numerales 7.5.3 literal b) y 8.1 de la norma ISO 27001:2013.*

También, se realiza la verificación del Procedimiento Desarrollo y Personalización de Aplicaciones código 03-PT-003 versión 4 vigente desde el 8 de octubre de 2019.

NC: *Verificado el Procedimiento Desarrollo y Personalización de Aplicaciones código 03-PT-003 versión 4 vigente desde el 8 de octubre de 2019, se evidenció que respecto al proyecto de aplicación de antecedentes del año 2023, no se encontraron los registros de los formatos 03-FR-08 requerimientos TIC, 08-FR-32 registro de asistencia a capacitación, 08-FR-22 evaluación de capacitación y formato 03-FR-01 acta de entrega de requerimientos TIC, Así mismo, no hay registros del SINPROC de la gestión realizada para el proyecto de antecedentes, incumpliendo el procedimiento y los numerales 7.5.3 literal a) y 8.1 de la norma ISO 27001:2013.*

Finalmente, se verificaron los planes y estos están relacionados con los objetivos del SGSI, así mismo, los procesos contratados externamente se les hace seguimiento a las obligaciones contractuales por parte del supervisor del contrato y los cambios no previstos del sistema de información, se tratan mediante la activación del plan de contingencia para mitigar los efectos adversos en la prestación del servicio.

Se recomienda: "*Actualizar el Plan de Control Operacional y el Plan de Continuidad del Negocio 2018-2020."*

4. Resultados de la Auditoría:

- **VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN**

La entidad realiza la valoración de los riesgos de seguridad de la información a intervalos planificados en el cronograma del plan de tratamiento de riesgos del sistema para los meses de marzo y abril de 2024 mediante la aplicación de matriz de riesgos de la Entidad.

Así mismo, conserva la información documentada de los resultados de las valoraciones de riesgos, de acuerdo a la metodología de gestión de riesgos, mediante la cual los resultados de la valoración de riesgos se registran en el formato mapa de riesgos institucional, esta información se encuentra almacenada y disponible en un repositorio centralizado disponible en las carpetas de ONEDRIVE de Microsoft Office 365 y para su consulta en la intranet institucional, la Oficina de Planeación, es la encargada de consolidar y custodiar los mapas de riesgos incluidos los de seguridad de la información de todos los procesos.

- **TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN**

La entidad cuenta con un plan de tratamiento de riesgos de seguridad de la información, el cual incluye como elementos clave, la identificación, análisis, valoración y plan de acción con las medidas de tratamiento de los riesgos, los responsables y plazos para su ejecución.

Por otra parte, la entidad conserva la información documentada de los resultados de la valoración de riesgos de seguridad de la información, de acuerdo a la metodología de gestión de riesgos, mediante la cual los resultados se registran en el formato mapa de riesgos institucional, esta información se encuentra almacenada y disponible en un repositorio centralizado disponible en las carpetas de ONEDRIVE de Microsoft Office 365 y para su consulta en la intranet institucional, La Oficina de Planeación, es la encargada de consolidar y custodiar los mapas de riesgos incluidos los de seguridad de la información de todos los procesos.

Se evidenció durante la auditoría que la Dirección de Tecnologías de la Información y las Comunicaciones, estaba realizando un informe del análisis de vulnerabilidades de servicios institucionales publicados en la internet.

Así mismo, el proceso cuenta con un informe de vulnerabilidades de la infraestructura tecnológica del año 2023. Además, este cuenta con las respectivas

4. Resultados de la Auditoría:

recomendaciones y seguimientos a 2023, sin embargo, se observa que los estados de algunas vulnerabilidades se encuentran abiertas.

Por lo anterior, se recomienda: "*Realizar seguimientos a las vulnerabilidades abiertas, identificar los riesgos de esas vulnerabilidades y llevarlos a la matriz de riesgos y plan de tratamiento de riesgos."*

"Elaborar por lo menos un informe al año de análisis de vulnerabilidades de la infraestructura tecnológica y hacer los respectivos tratamientos."

EVALUACIÓN DEL DESEMPEÑO

- **SEGUIMIENTO, MEDICIÓN, ANÁLISIS y EVALUACIÓN**

La gestión del SGSI se mide a través de la definición y diligenciamiento de indicadores de desempeño, auditorías internas y externas, la evaluación a la gestión de los riesgos, realización de encuestas, la medición de los controles aplicables, el seguimiento de cumplimiento de objetivos del SGSI, el análisis y gestión de incidentes de seguridad, el análisis de brechas existentes y la presentación de informes a la Alta dirección.

Además, la entidad evalúa la efectividad del SGSI a través de diferentes actividades: Auditorías internas, Indicadores de desempeño, Gestión de riesgos, Análisis de incidentes, Encuestas de seguridad y Revisión por la dirección.

Así mismo, la entidad determina las necesidades de monitoreo y medición de los objetivos de seguridad, la gestión de los riesgos, el uso y apropiación en seguridad, el monitoreo de eventos a través de la herramienta FORTISIEM, el procedimiento de gestión y monitoreo de eventos e incidentes de seguridad, la revisión de los controles aplicables y el estado del SGSI frente a los requisitos de la NTC-ISO-IEC 27001:2013.

Con respecto a los métodos para la medición, análisis y evaluación, se realiza a través de formatos de hoja de vida de indicadores, planes e informes de auditoría, informes de gestión, realización de encuestas, matrices de seguimiento y herramientas de monitoreo y análisis de datos.

En cuanto a la frecuencia, responsables y análisis de los resultados del monitoreo se determina para cada uno de los aspectos a tener en cuenta; estos se documentan en cada uno de los documentos o formatos diseñados para el registro

4. Resultados de la Auditoría:

de las actividades de monitoreo y medición del SGSI o en los diferentes planes establecidos como la revisión anual por la dirección, el plan anual de auditorías o el informe cuatrimestral de gestión de riesgos.

Por otro lado, la entidad conserva adecuadamente la información documentada de la evidencia de los resultados del monitoreo y la medición; esta información se encuentra almacenada y disponible en un repositorio centralizado en las carpetas de ONEDRIVE de Microsoft Office 365, organizada de acuerdo con las cláusulas de la NTC-ISO-IEC 27001:2013.

Por parte de la auditoría se establecen las siguientes recomendaciones: "*Realizar indicadores de disponibilidad del servicio de internet y uso de aplicativos."*

"Establecer indicadores para determinar la eficacia en la solución de eventos e incidentes del sistema de información."

"Reforzar los análisis cualitativos de los indicadores y en caso de incumplimiento realizar las correspondientes acciones correctivas."

"Establecer los indicadores para la medición de los planes y hacer seguimiento mensual en la matriz de planes de seguridad de la información."

- **REVISIÓN POR LA DIRECCIÓN**

La revisión por la dirección del SGSI se realiza anualmente y se encuentra planificada para el año 2024 en el plan de seguridad y privacidad de la información para los meses de noviembre y diciembre.

Así mismo, las entradas y salidas de la revisión por la dirección del año 2023 se encuentran relacionadas en el documento informe de revisión por la dirección, así mismo, se observó acta de reunión del comité institucional de gestión y desempeño del 12 de diciembre de 2023 donde fue presentada la revisión por la dirección.

Por otra parte, la entidad conserva la información documentada como evidencia de los resultados de las revisiones por parte de la dirección; esta información se encuentra almacenada y disponible en un repositorio centralizado en las carpetas de ONEDRIVE de Microsoft Office 365, organizada de acuerdo a los requisitos establecidos en la norma ISO 27001:2013.

4. Resultados de la Auditoría:

Esta auditoría recomienda: *"Presentar en la revisión por la dirección el seguimiento y medición de los indicadores del SGSI"*

"Complementar en la revisión por la dirección la retroalimentación de las partes interesadas."

MEJORA

- **NO CONFORMIDADES Y ACCIONES CORRECTIVAS**

La Entidad toma acciones cuando ocurren las No Conformidades y oportunidades de mejora derivadas de las auditorías internas y externas realizadas al SGSI, a través de la definición de los planes de mejoramiento donde se establecen las acciones correctivas y acciones de mejoramiento.

Por otra parte, se realiza análisis de causas identificadas para determinar las acciones correctivas y acciones de mejora que garanticen que no se vuelva a presentar las No Conformidades y a implementar las oportunidades de mejora y posteriormente se hace seguimiento trimestral a las acciones de mejora, registradas en los planes de mejoramiento,

Con respecto a la eficacia de las acciones correctivas tomadas se establece mediante el seguimiento y revisión de los documentos soporte y las evidencias de cumplimiento de las acciones correctivas programadas en los planes de mejoramiento, como consta en el *"formato de seguimiento plan de mejoramiento"* 16-FR-03, en el cual se refleja el análisis realizado por el equipo auditor, al desarrollo de las acciones de mejora implementadas y se determina si cumple o no con lo esperado.

Así mismo, la entidad conserva la información documentada pertinente a las acciones correctivas; esta información se encuentra almacenada y disponible en un repositorio centralizado en las carpetas de ONEDRIVE de Microsoft Office 365, organizada de acuerdo con los requisitos establecidos en la norma 27001:2013.

Durante la auditoria, el auditor reviso las evidencias de los planes de mejoramiento del SGSI y sus soportes en la actualidad estos planes se encuentran cerrados y son conformes respecto a los requisitos establecidos en la norma ISO 27001:2013.

4. Resultados de la Auditoría:

- **MEJORA CONTINUA**

La Entidad mejora continuamente a través de la definición de implementación de las acciones de mejora resultantes de los hallazgos de auditoría, la revisión periódica de los riesgos de seguridad de la información, la revisión y actualización periódica de los planes, procedimientos, políticas y lineamientos del SGSI, la revisión de la alta dirección, la sensibilización y capacitación permanente del personal en asuntos relacionados con el SGSI y la seguridad de la información y la adquisición y/o implementación de nuevas tecnologías y buenas prácticas de TI que fortalezcan la seguridad de la información.

Así mismo, la entidad verifica la efectividad del SGSI de manera programada a través los indicadores de desempeño, las auditorías internas y externas, la evaluación a la gestión de los riesgos, la realización de encuestas, el seguimiento de cumplimiento de objetivos del SGSI, el análisis y gestión de incidentes de seguridad y la presentación de informes a la Alta dirección.

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 mediante el documento Declaración de Aplicabilidad código 03-FR-23 versión 3 vigente desde el 14/04/2023, en el mencionado documento se identificaron 114 controles.

Por otra parte, de los 114 controles se han implementado 114 que corresponde al 100% de los controles establecidos en la referida Declaración de Aplicabilidad.

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).

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

4. Resultados de la Auditoría:

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 al Sistema de Gestión de Seguridad de la Información-Norma ISO 27001:2013, el equipo auditor seleccionó una muestra del 19% de los controles implementados del Anexo A que equivalen a 22 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 y A13 Seguridad de las Comunicaciones.

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

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.6.1.1	**Roles y Responsabilidades para la Seguridad de la Información**
4	A.6.1.4	**Contacto con grupos de interés**
5	A.6.1.5	**Seguridad de la información en la gestión de proyectos**
6	A.8.1.1	**Inventario de activos**
7	A.8.1.2	**Propiedad de los activos**
8	A.8.2.3	**Manejo de activos**
9	A.8.3.1	**Gestión de medios removibles**
10	A.8.3.3	**Transferencia de medios físicos**
11	A.9.1.2	**Acceso a redes y a servicios en red**
12	A.9.2.3	**Gestión de derechos de acceso privilegiado**
13	A.9.2.6	**Retiro o ajuste de los derechos de acceso**
14	A.9.4.4	**Uso de programas utilitarios privilegiados**
15	A.11.1.2	**Controles de acceso físico**
16	A.11.2.1	**Ubicación y protección de equipos**
17	A.11.2.3	**Seguridad del cableado**
18	A.11.2.8	**Equipos de usuario desatendido**

4. Resultados de la Auditoría:

19	A.11.2.9	**Política de escritorio limpio y pantalla limpia**
20	A.12.1.1	**Procedimientos de operación documentados**
21	A.12.2.1	**Controles contra códigos maliciosos**
22	A.13.1.1	**Controles de redes**

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

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

A.5.1.1 Políticas para la Seguridad de la Información

La política de seguridad de la información y el conjunto de políticas específicas han sido definidas y aprobadas por la alta dirección; para que los colaboradores de la entidad reconozcan y acepten las políticas de seguridad de la información, al ingresar a la entidad se suscriben los compromisos de confidencialidad y no divulgación de la información en los cuales se comprometen a conocer, acatar y consultar permanentemente los lineamientos y políticas establecidas en el manual de políticas de seguridad de la información de la Personería; se implementan estrategias de publicación y comunicación a través de medios institucionales como el correo electrónico, la intranet, el portal web, papel tapiz de equipos de cómputo, en jornadas de inducción a funcionarios y contratistas y mediante charlas de sensibilización programadas.

A.5.1.2 Revisión de las Políticas para la Seguridad de la Información

Las políticas de seguridad de la información son revisadas anualmente o cuando ocurran cambios significativos y se encuentran consolidadas en el documento *"Manual de políticas de seguridad de la información"* en el cual se evidencia la última revisión el 25/01/2024 con actualización de la normatividad y lineamientos relacionados con los numerales 6,1, 6,2, 7,5,2, 7,11,1, 7,12,1 y 7,15,2. Mediante la ejecución de auditorías internas al SGSI, se evalúa la conformidad de las políticas con la norma ISO 27001.

A.6.1.1 Roles y Responsabilidades para la Seguridad de la Información

La entidad ha designado y comunicado los roles y responsabilidades pertinentes a la seguridad de la información, designando a la Dirección de Tecnologías de la Información y las Comunicaciones DTIC como responsable del Sistema de Gestión de seguridad de la información SGSI mediante la resolución 250 de 2023,

4. Resultados de la Auditoría:

la adopción del Sistema de Gestión de seguridad de la información SGSI bajo la norma NTC-ISO 27001 mediante la resolución 242 de 2023 y la definición de responsabilidades y forma de designación del Oficial de seguridad de la información con la resolución 81 de 2024, al interior del proceso Direccionamiento TIC, se designó el equipo de Seguridad de la Información, el cual tiene distribuidos los roles y responsabilidades para la implementación, mantenimiento y mejora continua del SGSI. Para los (las) Funcionarios(as) de la Personería, al ingresar a la entidad se suscriben los compromisos de confidencialidad y no divulgación de la información en los cuales se comprometen a conocer, acatar y consultar permanentemente los lineamientos y políticas establecidas en el manual de políticas de seguridad de la información de la Personería; y en los contratos de prestación de servicios con contratistas y proveedores, se incluyen obligaciones relacionadas con el cumplimiento de políticas y procedimientos de seguridad de la información y se suscriben los correspondientes acuerdos de confidencialidad y no divulgación de la información.

A.6.1.4 Contacto con Grupos de Interés

La Personería de Bogotá, D.C. mantiene contacto con grupos y personas de interés en asuntos de seguridad de la información como CSIRT gobierno, CSIRT Policía Nacional, COLCERT, Fiscalía General de la Nación, Alta Consejería de Bogotá para las TIC, proveedores y comunidades relacionadas con asuntos de seguridad a través de las cuales se obtiene información de valor como boletines y alertas tempranas sobre nuevos ataques o vulnerabilidades, capacitación y participación en eventos de interés; adicionalmente, la Personería se encuentra incluida en un grupo de seguridad digital DC, administrado por la Alta Consejería para las TIC del Distrito, a través del cual se presta apoyo en asuntos relacionados con seguridad de la información y se comparte información de interés para la comunidad; esta información de contactos se consolida en el documento 03-FR-04- CONTACTOS CON GRUPOS DE INTERES Y AUTORIDADES-SGSI. A.6.2.2 Teletrabajo.

A.8.1.1 Inventario de Activos

Mediante el documento 03-GU-13 *"GUÍA PARA LA IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN" y el formato 03-FR-21 "INVENTARIO DE ACTIVOS DE INFORMACIÓN",* la Personería implementa la metodología para la identificación y valoración de los activos de información, acorde con los requisitos y lineamientos establecidos en el documento del Departamento Administrativo de

4. Resultados de la Auditoría:

la Función Pública DAFP, *"Guía para la administración del riesgo y el diseño de controles en Entidades públicas".*

A.8.1.2 Propiedad de los Activos

En el documento 03-FR-21 *"INVENTARIO DE ACTIVOS DE INFORMACIÓN"* se identifican los procesos responsables, el custodio y los roles que tienen a cargo los activos de información; adicionalmente para los activos físicos la entidad cuenta con procedimientos y formatos para el control de bienes que estandarizan las actividades a seguir para la administración, control, custodia y protección de los bienes a cargo de los colaboradores de la entidad, desde la entrega del activo en el momento de ingreso hasta la devolución de los mismos en caso de retiro del servicio en el cual se incluye control para la entrega de los elementos devolutivos a cargo de los funcionarios en el formato acta de entrega de puesto de trabajo.

A.8.2.3 Manejo de Activos

A través de procedimientos, manuales y formatos implementados para garantizar la seguridad de los activos durante el manejo, procesamiento, almacenamiento y comunicación de la información, que son aplicables a los colaboradores de la entidad que tengan a cargo los activos de información. La información institucional se conserva de acuerdo con los lineamientos y procedimientos establecidos por el proceso Gestión Documental, alineados a la normatividad legal vigente en lo relacionado con la organización, control, transferencia y conservación de documentos. Para los activos físicos la entidad cuenta con procedimientos y formatos para el control de bienes que estandarizan las actividades a seguir para la administración, control, custodia y protección de los bienes a cargo de los colaboradores de la entidad, desde la entrega del activo en el momento de ingreso hasta la devolución de los mismos en caso de retiro del servicio en el cual se incluye control para la entrega de los elementos devolutivos a cargo de los funcionarios en el formato acta de entrega de puesto de trabajo. El proceso direccionamiento TIC, cuenta con procedimientos, políticas y lineamientos de seguridad para el manejo de los activos de información tecnológicos que contribuyen a preservar la seguridad de la información institucional a su cargo.

A.8.3.1 Gestión de Medios Removibles

La entidad cuenta con procedimientos de gestión de medios removibles y procedimiento de borrado seguro de la información, que contribuyen a prevenir la

4. Resultados de la Auditoría:

divulgación, modificación y/o destrucción no autorizada de la información almacenada en los medios.

A.8.3.3 Transferencia de Medios Físicos

El manual de gestión documental y el procedimiento de ingreso, egreso y traslado de bienes, establecen lineamientos para la protección de los bienes físicos que contengan información de la entidad en el momento de ser trasladados.

A.9.1.2 Acceso Redes y a Servicios en Red

Se tienen implementados controles para el acceso seguros a la red basados en roles mediante servicios como el de VPN para ingreso desde fuera de la entidad y la autenticación a los servicios de red mediante directorio activo con usuario y contraseña. El Manual de Políticas de Seguridad de la Información establece políticas y lineamientos generales relacionados con el acceso seguro a las redes por parte de los colaboradores de la entidad.

Así mismo, mediante el procedimiento de gestión de usuarios se definen y ejecutan los lineamientos para la gestión de creación, modificación y retiro de las cuentas de usuario a los Sistemas de Información, carpetas compartidas en servidores y accesos especiales a internet, en el cual los derechos de acceso se asignan de acuerdo a las funciones y necesidades del usuario que son determinadas por el líder de cada proceso y se gestiona mediante solicitud de mesa de ayuda, asegurando que los usuarios tengan acceso únicamente a la información necesaria para el ejercicio de sus funciones.

A.9.2.3 Gestión de Derechos de Acceso Privilegiado

Los privilegios de acceso a los servicios tecnológicos son controlados conforme al procedimiento de gestión de usuarios, en el cual se realiza la solicitud formal de creación, modificación y retiro de las cuentas de usuario a los Sistemas de Información, carpetas compartidas en servidores y accesos especiales a internet, contribuyendo a que los derechos de acceso se asignen de acuerdo a las funciones y necesidades del usuario que son determinadas por el líder de cada proceso y se gestiona mediante solicitud de mesa de ayuda, asegurando que los usuarios tengan acceso únicamente a la información necesaria para el ejercicio de sus funciones.

4. Resultados de la Auditoría:

Por otra parte, el Manual de Políticas de Seguridad de la Información establece políticas y lineamientos generales relacionados con el acceso seguro a las redes por parte de los colaboradores de la entidad.

A.9.2.6 Retiro o Ajuste de los Derechos de Acceso

Los privilegios de acceso de los colaboradores y contratistas se retiran o suspenden según sea el caso, al terminar la vinculación laboral o contractual o se modifican según las solicitudes recibidas por la DTIC mediante procesos formales, como el procedimiento de gestión de usuarios y el procedimiento de retiro de talento humano, adicionalmente para el personal contratista, se garantiza la restricción de acceso a la red, registrando la fecha de finalización del contrato como fecha de expiración de la cuenta al momento de crear el usuario en el directorio activo, de tal manera que el usuario se inactiva automáticamente en la fecha indicada.
Por otra parte, el Manual de Políticas de Seguridad de la Información establece políticas y lineamientos generales relacionados con el acceso seguro a las redes por parte de los colaboradores de la entidad.

A.9.4.4 Uso de Programas Utilitarios Privilegiados

La Personería de Bogotá D.C., establece controles, políticas y lineamientos sobre el uso de software no autorizado. Se restringen los privilegios de administrador para instalar software mediante políticas de directorio activo y las cuentas de usuarios administradores de los equipos de cómputo están restringidas para uso exclusivo del personal de soporte de la DTIC, con lo cual se evita que los usuarios puedan instalar software o realizar cambios en las configuraciones de seguridad de los equipos.

Así mismo, mediante el Manual de Políticas de Seguridad de la Información en el numeral 7.5.4 *"Control de acceso a sistemas y aplicaciones"* establece lineamientos relacionados con la prohibición de uso de software o programas utilitarios que puedan violar o evadir los controles de seguridad para el acceso seguro a los sistemas y aplicaciones, adicionalmente la política de derechos de propiedad intelectual prohíbe el uso o instalación de software no licenciado.

Las solicitudes de instalación de software se realizan mediante procedimiento formal de mesa de ayuda.

4. Resultados de la Auditoría:

A.11.1.2 Controles de Acceso Físico

El acceso a las áreas seguras se controla mediante diferentes medios; se cuenta con protección de acceso físico por la empresa de vigilancia quien solicita presentar el carné de la entidad para el control de ingreso y salida del personal interno y el registro de accesos como control de ingreso y salida para personal externo, así como el registro de ingreso y salida de equipos mediante la planilla física

Por otra parte, las áreas de procesamiento de datos se encuentran protegidas de acceso no autorizado a través de un sistema de control de acceso con tarjeta de proximidad, a la cual se le pueden asignar los permisos dependiendo el rol del funcionario.

Además, se cuenta con instalación de sistemas de videovigilancia mediante cámaras y avisos de *"Área restringida"* para personal no autorizado.

Para el ingreso al centro de cómputo se implementó el procedimiento de ingreso a centros de cómputo y cableado, y se diligencia una bitácora física con los registros de accesos al centro de cómputo de la entidad, para controlar el acceso temporal de visitantes como contratistas o proveedores.

Por otro lado, el Manual de Políticas de Seguridad de la Información en el numeral 7.7. *"SEGURIDAD FÍSICA Y DEL ENTORNO"*, establece lineamientos relacionados con el acceso a las áreas seguras.

A.11.2.1 Ubicación y Protección de Equipos

Para proteger los equipos de los riesgos y amenazas y peligros del entorno y del acceso no autorizado, se han implementado una serie de medidas como:

Definición de políticas y lineamientos de seguridad estableciendo directrices sobre la ubicación y protección de equipos y las buenas prácticas en los puestos de trabajo.

Los equipos se encuentran ubicados de forma segura según la distribución de puestos de trabajo de cada dependencia, los que procesan información sensible y las instalaciones de almacenamiento de datos se ubican en áreas seguras, alejadas de personal externo y/o interno no autorizado y controladas mediante sistema de control de acceso con sensores de proximidad, y se implementó el

4. Resultados de la Auditoría:

procedimiento de ingreso a centros de cómputo y cableado, llevando un registro de los ingresos realizados para controlar el acceso temporal de visitantes como contratistas o proveedores.

Se han implementado medidas de protección ambientales, como sensores de humo y sistema de alerta contra incendios, ubicación de extintores y sistema de aire acondicionado, sistema eléctrico con acometida de puesta a tierra y energía regulada por sistema de UPS (Sistema de alimentación ininterrumpida) y planta eléctrica, para protección contra fallas electromagnéticas y problemas de voltaje o de suministro de energía).

Así mismo, se cuenta con protección de acceso físico por la empresa de vigilancia para el control de ingreso y salida de equipos mediante el registro de planilla física y la instalación de cámaras de videovigilancia.

A.11.2.3 Seguridad del Cableado

Para el control de interceptaciones y separar el cableado de corriente eléctrica del cableado de datos para evitar interferencias, el cableado se encuentra instalado en canaleta metálica y los cables de datos UTP cuentan con blindaje electromagnético.

Por otra parte, el acceso a los paneles de conexión y las instalaciones de cableado se encuentra restringido a personal no autorizado y controlado mediante sistema de control de acceso con sensor de proximidad.

Además, se han definido políticas y lineamientos de seguridad estableciendo directrices para la protección del cableado de energía eléctrica y de datos contra interceptación, interferencia o daño.

A.11.2.8 Equipos de Usuario Desatendido

Se implementan medidas como: Bloqueo automático de sesión mediante política de directorio activo, para que los equipos de cómputo se bloqueen automáticamente después de un periodo de tiempo de inactividad.

Desbloqueo de las sesiones de usuario de los equipos de cómputo mediante usuario y contraseña de directorio activo con características de complejidad de contraseñas.

4. Resultados de la Auditoría:

Así mismo, el Manual de Políticas de Seguridad de la Información en el numeral 7.7.2.1. *"Política de escritorio y pantalla limpia"* establece lineamientos relacionados con la seguridad de los equipos desatendidos.

Además, se realiza sensibilización permanente a través de medios de comunicación institucionales y en jornadas de inducción y charlas de seguridad de la información programadas, en las cuales se dan a conocer las políticas y lineamientos de seguridad implementados.

A.11.2.9 Política de Escritorio Limpio y Pantalla Limpia

Se encuentra definida una Política de escritorio y pantalla limpia. Se realiza sensibilización permanente a través de medios de comunicación institucionales y en jornadas de inducción y charlas de seguridad de la información programadas, en las cuales se dan a conocer las políticas y lineamientos de seguridad implementados.

Así mismo, se implementan medidas como el bloqueo automático de sesión mediante política de directorio activo y el desbloqueo de las sesiones de usuario de los equipos de cómputo mediante usuario y contraseña de directorio activo con características de complejidad de contraseñas.

A.12.1.1 Procedimientos de Operación Documentados

Los procedimientos, manuales, guías, y demás documentación que hace parte del SGSI, se encuentran registrados en el formato *"Inventario documental del SGSI"* y los documentos se encuentran almacenados en un repositorio del OneDrive institucional debidamente organizados según los requisitos y controles de la NTC-ISO-IEC 27001:2013. La documentación del SGSI que requiere ser controlada como parte del Sistema de Gestión de Calidad se encuentran publicados en el aplicativo ISOLUCION.

A.12.2.1 Controles Contra Códigos Maliciosos

Los equipos de cómputo se encuentran protegidos mediante la instalación de software de antivirus el cual cuenta con características de detección de virus en tiempo real, escaneo de equipos programado y automático y actualización automática de las bases de datos que contienen las firmas de malware con las últimas amenazas que se presenten.

4. Resultados de la Auditoría:

Por otra parte, el filtrado de correos electrónicos realizado por la plataforma de office 365 Defender y la gestión de instalación de parches y actualizaciones de software programados y automáticos a través del servicio WSUS.

Además, el Manual de Políticas de Seguridad de la Información en el numeral 7.8.2. *"Protección contra códigos maliciosos"* establece lineamientos relacionados con este control de seguridad.

Así mismo, se realiza sensibilización permanente a través de medios de comunicación institucionales y en jornadas de inducción y charlas de seguridad de la información programadas, en las cuales se dan a conocer las políticas y lineamientos de seguridad implementados con la prevención contra virus y códigos maliciosos.

A.13.1.1 Controles de Redes

Se han implementado medidas como la segmentación de redes utilizando la configuración de VLAN's que permite separar lógicamente las redes dependiendo la ubicación de los usuarios y recursos de red.

La instalación de equipos de seguridad de redes, FIREWALL para controlar el tráfico de red entrante y saliente, WAF (Web Aplication Firewall) para protección de aplicaciones web contra ataques maliciosos y tráfico no deseado, correlacionador de eventos fortisiem para identificar eventos de seguridad.

Medidas de hardening o endurecimiento de la seguridad a nivel de aplicaciones y sistemas operativos en servidores como selinux, firewall local (IPtable o firewalld), modsecurity, modevasive).

Por otra parte, la implementación de protocolo HTTPS en los aplicativos de la entidad para garantizar el cifrado de los datos transmitidos por la red protegiendo la confidencialidad e integridad de la información, la implementación de acceso remoto mediante servicio de VPN para acceso remoto a los recursos de red.

Las responsabilidades y procedimientos para la gestión de equipos de redes se encuentran a cargo del grupo de infraestructura y redes de la dirección DTIC.

Contratación servicio de monitoreo SOC (Centro de Operaciones de Seguridad) para el monitoreo, detección y atención de eventos de seguridad. (Contrato 412

4. Resultados de la Auditoría:

de 2024). Además, se define la política de controles en la red de datos y transferencia de información que establece los lineamientos de seguridad relacionados con las redes de datos.

Revisados los controles del anexo A de la norma ISO 27001:2013 de acuerdo con la muestra seleccionada por el auditor, estableció que 20 de ellos se encontraron conformes; sin embargo, se presentaron incumplimiento del control A.11.1.2 controles de acceso físico y el control A.11.2.9 política de escritorio limpio y pantalla limpia.

Respecto al control A.11.1.2 controles de acceso físico, este se unifico con una No Conformidad establecida en la planificación y control operacional, por lo tanto, se establece la siguiente No Conformidad para el control A.11.2.9.

NC: *Efectuada la revisión del control de política de escritorio limpio y pantalla limpia mediante muestreo de verificación de pantallas de computador en la Dirección de Tecnologías de la Información y las Comunicaciones, se evidenciaron 4 pantallas de computador con varios archivos expuestos en los equipos, situación que incumple el control A.11.2.9 de la norma ISO 27001:2013.*

Se recomienda: "*Realizar la comunicación y sensibilización de los controles establecidos en el anexo A de la norma ISO 27001:2022 a los procesos de la Entidad."*

4.1. Hallazgos y/o No Conformidad

- Verificada la normatividad en la Resolución 500 de marzo 10 de 2021, *"señala que se debe designar dentro de la Entidad los responsables de gestionar y dar respuesta a los incidentes de seguridad digital, liderado por el responsable de seguridad digital."* Así mismo, la Entidad mediante la Resolución 81 del 22 de febrero de 2024 estableció la designación del Oficial de Seguridad de la Información y sus responsabilidades, sin que a la fecha se haya nombrado a un asesor o profesional de la planta global que cumpla con los requisitos y ejerza las responsabilidades de este rol, incumpliendo los requisitos legales y reglamentarios de la Entidad y el numeral 4.2 literal b) de la Norma ISO 27001:2013.

- Verificados los roles, responsabilidades y autoridades del SGSI, se evidenció la asignación de estos, sin embargo, no se observó la comunicación del documento roles y responsabilidades del Sistema de

4. Resultados de la Auditoría:

Gestión de Seguridad de la Información SGSI del 10 de agosto de 2023, incumpliendo el numeral 5.3 literal a) de la Norma ISO 27001:2013.

- Verificada la documentación del SGSI para el control de documentos, se evidenció que el formato de compromiso de confidencialidad y no divulgación de la información para funcionarios y vinculados temporalmente a la entidad código 03-FR-22 versión 2 vigente desde el 26/05/2020 de la contratista Stefany Cabrales Madrid, no se encuentra controlado respecto al formato oficial publicado en el aplicativo Isolución que tiene fecha de vigencia 13/02/2024, incumpliendo el numeral 7.5.3 literal b) de la norma ISO 27001:2013.

- Verificado el Procedimiento de Ingreso a Centros de Cómputo y Cableado código 03-PT-05 versión 1 vigente desde el 14 de agosto de 2019, se ingresa al centro de cómputo y cableado se realiza recorrido y toma de fotografías sin ningún tipo de registro para su ingreso, así mismo se verificó el diligenciamiento del formato bitácora de acceso a centro de cómputo y cableado código 03-FR-20 versión 1, encontrándolo que faltaban espacios por diligenciar como las horas de salida, elementos ingresados, funcionario responsable de la actividad, firma del visitante, nombre y firma de quien autoriza, contraviniendo las políticas de operación 4.4,4.6 y 4.7 establecidas en el procedimiento e incumpliendo el control A.11.1.2 controles de acceso físico, los numerales 7.5.3 literal b) y 8.1 de la norma ISO 27001:2013.

- Verificado el Procedimiento Desarrollo y Personalización de Aplicaciones código 03-PT-003 versión 4 vigente desde el 8 de octubre de 2019, se evidenció que respecto al proyecto de aplicación de antecedentes del año 2023, no se encontraron los registros de los formatos 03-FR-08 requerimientos TIC, 08-FR-32 registro de asistencia a capacitación, 08-FR-22 evaluación de capacitación y formato 03-FR-01 acta de entrega de requerimientos TIC, Así mismo, no hay registros del SINPROC de la gestión realizada para el proyecto de antecedentes, incumpliendo el procedimiento y los numerales 7.5.3 literal a) y 8.1 de la norma ISO 27001:2013.

- Efectuada la revisión del control de política de escritorio y pantalla limpios mediante muestreo de verificación de pantallas de computador en la Dirección de Tecnologías de la Información y las Comunicaciones, se evidenciaron 4 pantallas de computador con varios archivos expuestos en los equipos, situación que incumple el control A.11.2.9 de la norma ISO 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 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 planificación, ejecución y seguimiento del SGSI.
- Ejecución de acciones de mejora de las auditorías internas, externas y autoevaluaciones.
- El sistema cuenta con acciones adecuadas que le permiten cumplir los requisitos en la normatividad aplicable.

5.2. Recomendaciones

- Incluir en la matriz DOFA con el cruce de las variables para determinar las estrategias adoptadas por la Entidad para el desarrollo del SGSI.
- Complementar el documento del contexto con el desarrollo de la metodología PESTAL en donde se incluya los entornos político, económico, social, tecnológico ambiental y legal.
- Desarrollar el entorno tecnológico frente a los requerimientos de la institución y en cumplimiento de la normatividad legal vigente.
- Incluir en el documento de contexto la matriz de comprensión de las necesidades y expectativas de las partes interesadas para la seguridad de la información.

5. Fortalezas y Recomendaciones:

- Unificar el documento del contexto del SGSI al documento contexto de la organización de los sistemas de gestión de calidad y seguridad y salud en el trabajo.
- Realizar actualización de la matriz de requisitos legales del proceso DTIC frente al SGSI.
- Mantener la integridad y confiabilidad de la información respecto al alcance del SGSI en los documentos y plataformas donde se publique esta información.
- Realizar la actualización del estudio de vulnerabilidades del sistema de información de la Entidad.
- Identificar los riesgos de seguridad de la información teniendo en cuenta la criticidad de los activos de información.
- Establecer una matriz de riesgos del SGSI en donde se evidencie los riesgos identificados de las vulnerabilidades del sistema de información y los riesgos que se establecen respecto a los controles implementados del documento Declaración de Aplicabilidad en cumplimiento del anexo A de la norma ISO 27001:2022.
- Actualizar el documento Declaración de Aplicabilidad de acuerdo con los controles establecidos en el Anexo A de la norma ISO 27001:2022.
- Actualizar el objetivo No 4 en la Revisión por la Dirección y plantear otro objetivo si así lo determina la alta dirección.
- Realizar seguimiento a los planes del SGSI, mediante la utilización de códigos de colores para distinguir cada tema.
- Continuar fortaleciendo el SGSI y la DTIC con personal.
- Continuar fortaleciendo la infraestructura tecnológica hardware y software para la seguridad de la información.
- Continuar fortaleciendo la toma de conciencia del SGSI.

5. Fortalezas y Recomendaciones:

- Actualizar el formato autorización para acceso permanente a centros de cómputo y cableado código 03-FR-19 versión 1 vigente desde el 14/08/2019, en la medida que el formato se encuentra con un logo de una administración anterior y la autorización corresponde al Director de TIC de unas administraciones anteriores.

- Realizar seguimiento a los tiempos de atención de los eventos e incidentes.

- Revisar el procedimiento para verificar los acuerdos de niveles de servicio para determinar los tiempos de solución de un evento o incidente teniendo en cuenta la severidad e impacto.

- Revisar los procedimientos 03-PT-10 versión 1 y el procedimiento 03-PT-14 versión 1 para determinar si técnicamente es posible unificarlos en uno solo.

- Revisar el procedimiento y gestionar la trazabilidad del cambio general y cambio estándar.

- Actualizar el Plan de Control Operacional y el Plan de Continuidad del Negocio 2018-2020.

- Realizar indicadores de disponibilidad del servicio de internet y uso de aplicativos.

- Establecer indicadores para determinar la eficacia en la solución de eventos e incidentes del sistema de gestión de seguridad de la información.

- Reforzar los análisis cualitativos de los indicadores y en caso de incumplimiento realizar las correspondientes acciones correctivas.

- Establecer los indicadores para la medición de los planes y hacer seguimiento mensual en la matriz de planes de seguridad de la información.

- Presentar en la revisión por la dirección el seguimiento y medición de los indicadores del SGSI.

- Complementar en la revisión por la dirección la retroalimentación de las partes interesadas.

5. Fortalezas y Recomendaciones:

- Realizar la transición del SGSI a la norma ISO 27001:2022.
- Realizar la comunicación y sensibilización de los controles establecidos en el anexo A de la norma ISO 27001:2022 a los procesos de la Entidad.

6. Conclusiones:

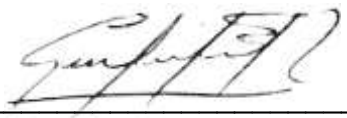
- El Sistema de Gestión de Seguridad de la Información, cumplió con los requisitos establecidos en la Norma ISO 27001: 2013.

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

Ítem	CRITERIO DE AUDITORÍA	HALLAZGO Y/O NO CONFORMIDAD	RIESGO IDENTIFICADO
1	Numeral 4.2 Norma ISO 27001:2013	Verificada la normatividad en la Resolución 500 de marzo 10 de 2021, *"señala que se debe designar dentro de la Entidad los responsables de gestionar y dar respuesta a los incidentes de seguridad digital, liderado por el responsable de seguridad digital."* Así mismo, la Entidad mediante la Resolución 81 del 22 de febrero de 2024 estableció la designación del Oficial de Seguridad de la Información y sus responsabilidades, sin que a la fecha se haya nombrado a un asesor o profesional de la planta global que cumpla con los requisitos y ejerza las responsabilidades de este rol, incumpliendo los requisitos legales y reglamentarios de la Entidad y el numeral 4.2 literal b) de la Norma ISO 27001:2013.	Incumplimiento legal y lineamientos interno de la Entidad

2	Numeral 5.3 Norma ISO 27001:2013	Verificados los roles, responsabilidades y autoridades del SGSI, se evidenció la asignación de estos, sin embargo, no se evidenció la comunicación del documento roles y responsabilidades del Sistema de Gestión de Seguridad de la Información SGSI del 10 de agosto de 2023, incumpliendo el numeral 5.3 literal a) de la Norma ISO 27001:2013.	Incumplimiento de la comunicación de los roles y responsabilidades del SGSI
3	Numeral 7.5 Norma ISO 27001:2013	Verificada la documentación del SGSI para el control de documentos, se evidenció que el formato de compromiso de confidencialidad y no divulgación de la información para funcionarios y vinculados temporalmente a la entidad código 03-FR-22 versión 2 vigente desde el 26/05/2020 de la contratista Stefany Cabrales Madrid, no se encuentra controlado respecto al formato oficial publicado en el aplicativo Isolución que tiene fecha de vigencia 13/02/2024, incumpliendo el numeral 7.5.3 literal b) de la norma ISO 27001:2013.	Incumplimiento del control de documentos
4	Control A.11.1.2 y Numeral 8.1 Norma ISO 27001:2013	Verificado el Procedimiento de Ingreso a Centros de Cómputo y Cableado código 03-PT-05 versión 1 vigente desde el 14 de agosto de 2019, se ingresa al centro de cómputo y cableado se realiza recorrido y toma de fotografías sin ningún tipo de registro para su ingreso, así mismo se verifico el diligenciamiento del formato bitácora de acceso a centro de cómputo y cableado código 03-FR-20 versión 1, encontrándolo que faltaban espacios por diligenciar como las horas de salida, elementos ingresados,	Incumplimiento del procedimiento y control de acceso físico

		funcionario responsable de la actividad, firma del visitante, nombre y firma de quien autoriza, contraviniendo las políticas de operación 4.4, 4.6 y 4.7 establecidas en el procedimiento e incumpliendo el control A.11.1.2 controles de acceso físico, los numerales 7.5.3 literal b) y 8.1 de la norma ISO 27001:2013.	
5	Numerales 7.5.3 y 8.1 Norma ISO 27001:2013	Verificado el Procedimiento Desarrollo y Personalización de Aplicaciones código 03-PT-003 versión 4 vigente desde el 8 de octubre de 2019, se evidenció que respecto al proyecto de aplicación de antecedentes del año 2023, no se encontraron los registros de los formatos 03-FR-08 requerimientos TIC, 08-FR-32 registro de asistencia a capacitación, 08-FR-22 evaluación de capacitación y formato 03-FR-01 acta de entrega de requerimientos TIC, Así mismo, no hay registros del SINPROC de la gestión realizada para el proyecto de antecedentes, incumpliendo el procedimiento y los numerales 7.5.3 literal a) y 8.1 de la norma ISO 27001:2013.	Incumplimiento del procedimiento y control de documentos
6	Control A.11.2.9 Norma ISO 27001:2013	Efectuada la revisión del control de política de escritorio limpio y pantalla limpia mediante muestreo de verificación de pantallas de computador en la Dirección de Tecnologías de la Información y las Comunicaciones, se evidenciaron 4 pantallas de computador con varios archivos expuestos en los equipos, situación que incumple el control A.11.2.9 de la norma ISO 27001:2013.	Incumplimiento del control de escritorio limpio y pantalla limpia.

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

APROBÓ
Firma:  **Nombre: William Ospina Giraldo** **Empleo: Jefe Oficina de Control Interno**