	PROCESO GESTION AUDITORIA	Código: FT-GAUD-020
		Serie:100-1.3-18
	INFORME FINAL DE AUDITORÍA INTERNA DE GESTIÓN	Versión: 03
		Página **1** de **14**

FECHA DE EMISIÓN DEL INFORME FINAL: DÍA 17 MES 06 AÑO 2022

Proceso/Dependencia Auditada:	Gestión TIC
Líder de Proceso:	Antonio José Rodríguez Linares Jefe oficina asesora sistemas
Objetivo de la Auditoría:	*Evaluar el modelo de seguridad y privacidad de la información de la Dirección de Tránsito de Bucaramanga, basado en las directrices impartidas por el MINTIC".*
Alcance de la Auditoría:	*Verificar la aplicación y el cumplimiento de las directrices impartidas por le MINTIC para el periodo comprendido entre el primero de Enero de 2021 al 31 de marzo de 2022*
Criterios de la Auditoría:	• Normatividad legal vigente a nivel nacional y territorial • Procedimeintos y formatos internos • Entrevistas realizadas • Trabajo de campo • Muestreo aleatorio • Resoluciones internas • Metodologia de auditoria basada en riesgos
Equipo Auditor	OMAIRA JEREZ TAMI - Auditor Líder OBER SOTO SOLANO - Auditor de Apoyo ANDRÉS ORLANDO RUEDA PEÑA - Auditor de Apoyo TANIA KATHERINE MANZANO BARRERA - Auditor de Apoyo

Reunión de Apertura						**Ejecución de la Auditoría**				**Reunión de Cierre**					
Día	03	**Mes**	05	**Año**	2022	**Desde**	04/05/22	**Hasta**	17/06/22	**Día**	17	**Mes**	06	**Año**	22

DESARROLLO DE LA AUDITORIA

La oficina de control interno se constituye como el "control de controles" por excelencia. Mediante su labor evaluadora determina la efectividad del sistema de control interno de la entidad con el objetivo de contribuir a la Alta Dirección en la toma de decisiones que orienten el accionar administrativo hacia la consecución de los fines estatales.

El diseño, implementación y mantenimiento del sistema de control interno y la ejecución de los controles establecidos es una responsabilidad del representante legal y de los líderes de los diferentes procesos de la entidad. Así mismo el sistema de control interno, previsto en la Ley 87 de 1993, se enmarca como una de las dimensiones de MIPG y, busca asegurar que las demás dimensiones cumplan su propósito y lleven al cumplimiento de resultados con eficiencia, eficacia, calidad y transparencia en la gestión pública.

En este sentido el proceso Gestión TIC tiene como objetivo liderar y promover las TIC (Tecnología de la Información y la Comunicación) soportando a través de los sistemas de información los trámites y servicios de la Dirección de Transito de Bucaramanga y aplicar la estrategias GEL (Gobierno en Línea) con el fin de publicar a los ciudadanos, empresas y demás entidades públicas la información que salvaguarda la Institución. De igual forma con las nuevas dinámicas de gestión administrativa enmarcadas dentro del MIPG la seguridad y privacidad de la información se fundamenta como un eje central para la obtención de resultados. Por lo expuesto el equipo auditor tomo la decisión de estructurar la auditoria basado en el enfoque conceptual del modelo de seguridad y privacidad de la información emanado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

El Modelo de Seguridad y Privacidad de la Información (MSPI), Se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG), La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas. Este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital. El MSPI para estar acorde con las buenas prácticas de seguridad deberá ser actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

A nivel metodológico es importante tener presente que el (MSPI) cuenta con una serie de guías anexas que ayudan a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y como desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Dirección de Transito de Bucaramanga está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Es de precisar que la presente auditoria da cumplimiento al plan general de auditoria en concordancia con el plan de acción del modelo integrado de planeación y gestión, por tanto se enfoca de manera exclusiva a la estructuración y formulación del MPSI.

Teniendo en cuenta que el líder del proceso no hizo uso de su derecho a réplica, advirtiendo que dentro de la reunión de apertura fue socializado el procedimiento de la auditoria, y enviado correo electrónico con el respectivo preinforme el día 07 de junio de 2022 con memorando N°136 de la misma fecha. El equipo auditor procedió a tipificar cada una de las observaciones como hallazgos de la siguiente manera:

HALLAZGO N° 1	
CRITERIO	• Norma técnica NTC ISO/IEC 27001:2013. • Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3 • Modelo de Seguridad y Privacidad de la Información (MSPI) • Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información.(anexo matriz) • Guía No 1 - Metodología de Pruebas de Efectividad • Diagnóstico de Seguridad y Privacidad de la Información PL-GTIC-003
OBSERVACIÓN	**Ausencia del respaldo metodológico y debilidad en el diagnostico de la seguridad y privacidad de la información.** Teniendo en cuenta el documento Diagnóstico de Seguridad y Privacidad de la Información PL-GTIC-003 aportado por el líder del proceso el equipo auditor procedió a verificar la metodología de elaboración, acción que no logró desarrollar toda vez que no se aportó la estructuración metodológica del documento. En este sentido se procedió a tomar como guía el documento Instructivo para el Diligenciamiento de la Herramienta de Diagnóstico de Seguridad y Privacidad de la Información y su respectiva matriz de elaboración, dejando ver una falta de estructuración técnica, y metodológica del documento PL-GTIC-003 el cual solo aborda tareas específicas las cuales precisan sobre 5 temas de la generalidad de la matriz emanada por el MINTIC que corresponde a 42 ítems. Lo anterior cobra mayor relevancia teniendo en cuenta que de acuerdo a los cronogramas establecidos por los equipos transversales del MINTC a la fecha el modelo debió estar implementado en su totalidad por parte de la entidad.

RECOMENDACIÓN	Actualizar el diagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), basado en la metodología emanada por el MINTIC.

HALLAZGO N° 2	
CRITERIO	• Norma técnica NTC ISO/IEC 27001:2013. • Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3 • Modelo de Seguridad y Privacidad de la Información (MSPI) • Plan de seguridad de la información MINTIC • PL-GTIC-002 Plan de seguridad de la información V01
OBSERVACIÓN	**Deficiencia en la estructura y cronograma del plan de seguridad y privacidad de la información.** El equipo auditor observa que el documento PL-GTIC-002 Plan de seguridad de la información V01 no cuenta con el estado actual y estado deseado de la entidad, que permita identificar los riesgos de seguridad actuales, la brecha existente entre estos dos estados, y defina la brecha a cerrar con la implementación de la estrategia de seguridad de la información. El equipo auditor evidencio que el cronograma que forma parte del documento PL-GTIC-002 Plan de seguridad de la información V01, plasma actividades que van de acuerdo con las responsabilidades de los propietarios de la información y usuarios de la información, dejando sin precisar dentro del cronograma las actividades definidas dentro del plan las cuales se relacionan a continuación: • Gestión de activos Los activos de información o digitales en la DTB. Se gestionarán de manera que: 1. Se tendrá un inventario actualizado de los equipos de cómputo. 2. Se tendrá un inventario actualizado de los sistemas de información. 3. Serán asignados a un responsable. 4. Se realizará una valoración de riesgos. 5. Protegidos de acuerdo a su riesgo asignado • Gestión de riesgos: 1. Identificación de vulnerabilidades y amenazas sobre los activos de información. 2. Identificación de Riesgos, Evaluación de Riesgos

	3. Monitoreo 4. Planes de Acción / Tratamiento 5. Criterios de Aceptación de riesgos. De igual forma el cronograma del plan de seguridad de la información vigencia 2021 no tiene una estructura, que proyecte el debido seguimiento, proporcione la gestión y desarrollo de las actividades anuales que son cruciales para el éxito del Modelo de Seguridad y Privacidad de la Información (MSPI). • Descripción de la actividad • Marco legal • Entregable y responsable por actividad.
RECOMENDACIÓN	Realizar los ajustes al plan de seguridad y privacidad de la información de acuerdo al diagnóstico debidamente actualizado incluyendo las actividades definidas en el mismo dentro del respectivo cronograma, acorde a la guía metodología emanada por el MINTIC.

HALLAZGO N° 3	
CRITERIO	• Norma técnica NTC ISO/IEC 27001:2013. • Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3 • Modelo de Seguridad y Privacidad de la Información (MSPI) • Guía 02 de Elaboración de la Política General de Seguridad y Privacidad de la Información.
OBSERVACIÓN	**Falta de adopción y socialización Institucional de la POLÍTICA SEGURIDAD DE LA INFORMACIÓN.** El equipo auditor evidencia que la Dirección de Transito de Bucaramanga cuenta con la POLÍTICA SEGURIDAD DE LA INFORMACIÓN institucionalizada en el Sistema de Gestión de Calidad con el cod: POL-GTIC-002, documento estructurado ajustado a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones MIN-TIC establecidos en la Guía 02 Elaboración de la Política General de Seguridad y Privacidad de la Información. Por otra parte no se evidencio la adopción del documento cod: POL-GTIC-002 por parte de la entidad mediante acto administrativo y/o aprobación institucional en el marco del Comité Institucional de Gestión y Desempeño, ni su respectiva socialización al interior de la entidad.

RECOMENDACIÓN	Adoptar la POLÍTICA SEGURIDAD DE LA INFORMACIÓN cod: POL-GTIC-002 y realizar la socialización institucional que contribuya a la aplicación de buenas prácticas en seguridad y privacidad de la información al interior de la entidad, asegurando el cumplimiento de la integridad, disponibilidad, legalidad y confidencialidad de la información.

HALLAZGO N° 4	
CRITERIO	• Norma técnica NTÇ ISO/IEC 27001:2013. • Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3 • Modelo de Seguridad y Privacidad de la Información (MSPI) • Documento elaboración de la política general de seguridad y privacidad de la información.- MINTIC • Política Seguridad de la Información POL-GTIC-002
OBSERVACIÓN	**Deficiencia, en los lineamientos establecidos por MINTIC y desactualización de las políticas de seguridad y privacidad de la información adoptada por la entidad.** Revisado las políticas de seguridad y privacidad de la información inmersas dentro del documento de política general de la Dirección de Tránsito de Bucaramanga se identificaron las siguientes apreciaciones: 1. No se encuentran incluidas las siguientes políticas 1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 2. NO REPUDIO 3. GESTIÓN DE ACTIVOS 4. POLÍTICA DE INTEGRIDAD 5. REGISTRO Y AUDITORIA 6. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN. Lo anterior cobra relevancia toda vez que si bien es cierto estas políticas son sugeridas por el MPSI, su formulación e implementación es crucial para fortalecer el modelo dentro de la entidad. 2. La 6 políticas incluidas dentro del documento de Política Seguridad de la Información POL-GTIC-002 de la DTB, no se incluyen las directrices y sugerencias emanadas por el MINTIC en el titulo 9 del documento Guía 02 elaboración de la política general de seguridad y privacidad de la información.- MINTIC. El documento de Política Seguridad de la Información POL-GTIC-002 fue

	inicialmente emitido en octubre de 2019 y no cuenta con actualización reciente acorde la implementación y entrada en vigencia del nuevo software misional así como de las directrices del (MSPI) emitidas por MINTIC definidas en la guía mencionada anteriormente.
RECOMENDACIÓN	Fortalecer, Articular y mantener las diferentes políticas institucionales con las directrices impartidas por el MINTIC para velar por una eficiencia en la seguridad y privacidad de la información.

HALLAZGO N° 5	
CRITERIO	• Norma técnica NTC ISO/IEC 27001:2013. • A.7 ISO 27001 Seguridad del Recurso Humano • A.8 ISO 27001 Gestión de Activos • A.9 ISO 27001 Control de Acceso a Sistemas de la Información • A.10 ISO 27001 Criptografía • A.11 ISO 27001 Seguridad Física y del Entorno • A.12 ISO 27001 Seguridad de las Operaciones • A.13 ISO 27001 Seguridad de las Comunicaciones • A.14 ISO 27001 Adquisición, desarrollo y mantenimiento de sistemas de información • A.15 ISO 27001 Relación con los proveedores • A.16 ISO 27001 Gestión de incidentes de seguridad de la información • A.17 ISO 27001 Aspectos de seguridad de la información de la gestión de continuidad de negocio. • Guía N° 3 Procedimiento de seguridad de la información-MINTIC • PR-GTIC-010 Solicitud generación de base de datos v.01. • PR-GTIC-009 Procedimiento atención y solución a incidentes en plataforma v01. • PR-GTIC-008Procedimiento solicitud de recurso TI v01. • PR-GTIC-007 Procedimiento solicitud de información de base de datos v.01. • PR-GTIC-005 Procedimiento Solicitud y uso de Activos de información v.01. • PR-GTIC-002 Procedimiento actualización de contenidos en la página WEB e intranet v.003.

OBSERVACIÓN	**Falta de procedimientos de seguridad de la información y lineamientos definidos por el MiNTIC.** Revisado los procedimientos suministrados por la oficina de Sistemas, y la guía N° 3 del MSPI, el equipo auditor observa que no se tienen establecido procedimientos de seguridad y privacidad de la información para los siguientes ítems: • Seguridad del recurso humano • Gestión de activos • Criptografía • Seguridad física y del entorno • Seguridad de las operaciones • Relación con los proveedores • Adquisición, desarrollo y mantenimiento de sistemas información • Aspectos de seguridad de la información de la gestión de continuidad de negocio. Si bien es cierto la entidad cuenta con algunos de los procedimientos sugeridos por el MPSI, cobra relevancia que se dejen sin implementar los procedimientos indicados anteriormente los cuales son de suma importancia para minimizar los riesgos de pérdida de datos, accesos no autorizados, divulgación no controlada, que afecten la integridad y privacidad de la información de la entidad.
RECOMENDACIÓN	Fortalecer y Articular y procedimientos de seguridad y privacidad de la información con las directrices impartidas por el MINTIC para velar por la integridad y seguridad de la información.

HALLAZGO N° 6	
CRITERIO	• Norma técnica NTC ISO/IEC 27001:2013. • Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3 • Modelo de Seguridad y Privacidad de la Información (MSPI) • Resolución 431 de 2016 por la cual se adopta la estrategia nacional de gobierno en línea en la DTB. • Resolución 320 de 2017 se designa como responsable de la estrategia nacional de gobierno en línea en la DTB. • Resolución 239 de 2018 por la cual se adopta el MIPG y se integra el Comité de Gestión y Desempeño y la resolución. • Resolución 274 de 2019 donde se realizan modificaciones puntuales a la resolución 239 de 2018

OBSERVACIÓN	**Falta de designación del responsable de la Seguridad y Privacidad de la información e inclusión de las funciones en el comité Institucional de Gestión y Desempeño.** La Dirección de Tránsito de Bucaramanga expide resolución 431 de 2016 por la cual se adopta la estrategia nacional de gobierno en línea y adicionalmente con la resolución 320 de 2017 se designa como responsable al jefe de la Oficina de Asesora de sistemas de la misma. Asi mismo se evidencia las resoluciones 239 de 2018 por la cual se adopta el MIPG y se integra el Comité de Gestión y Desempeño y la resolución 274 de 2019, donde se realizan modificaciones puntuales a la resolución 239 de 2018. Sin embargo, la anterior normativa interna no integra los temas de seguridad y privacidad en la información y los respectivos responsables en el marco del Comité Institucional de Gestión y Desempeño en la DTB, acorde con lo definido en el Decreto 1499 de 2017 en donde establece que se deben incluir todos los temas que atiendan la implementación y desarrollo de las políticas de gestión (Gobierno Digital y Seguridad Digital) definidas en el MIPG; Cuya información adquiere un nivel de importancia en la medición del Índice de Desempeño Institucional – IDI, el cual se mide a través del Formulario único de Reportes y Avances de Gestión – FURAG. Lo anterior teniendo en cuenta que el Comité Institucional de Gestión y Desempeño es la instancia encargada de orientar, articular y ejecutar las acciones y estrategias para la correcta implementación, operación, desarrollo, evaluación y seguimiento del Modelo Integrado de Planeación y Gestión – MIPG, en la entidad.
RECOMENDACIÓN	La Oficina de Control Interno y Gestión recomienda realizar la designación del responsable de la Seguridad y Privacidad de la información e inclusión de las funciones en el comité Institucional de Gestión y Desempeño.

HALLAZGO N° 7	
CRITERIO	• Norma técnica NTC ISO/IEC 27001:2013. • Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3 • Modelo de Seguridad y Privacidad de la Información (MSPI) • Plan Estratégico de Tecnologías de la Información –PETI • PR-GTIC-005 Procedimiento Solicitud y uso de Activos de información v.01.

	• Guía N° 5 Gestión Clasificación de Activos • Ítem 8 de la Tabla 2 – de la guía Controles del Anexo A del estándar ISO/IEC 27001:2013
OBSERVACIÓN	**Falta de inventario metodológico de los activos de información de la Dirección de Transito de Bucaramanga** Los activos de la información son elementos de información que la DTB recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes. En este sentido la entidad cuenta con un plan estratégico el cual solo da una aproximación tacita pero no especifica de activos de la información, un procedimiento denominado solicitud acceso y uso de activos de información, un inventario de data center y listado de los equipos de leasing. Por lo anterior el equipo auditor observo la falta de un inventario de activos de información con su respectiva metodología que tipifique cada uno de los elementos de valor de la DTB y contribuya a la seguridad de la misma identificando cada uno de sus activos.
RECOMENDACIÓN	Realizar un inventario metodológico, técnico donde se especifique como mínimo la siguiente información de los activos: nombre, ubicación tanto física como electrónica, su propietario y/o custodio, derechos de acceso y el nivel de clasificación de la información.

HALLAZGO N° 8	
CRITERIO	• Norma técnica NTC ISO/IEC 27001:2013. • Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3 • Modelo de Seguridad y Privacidad de la Información (MSPI) • Mapa de riesgos oficina asesora de sistemas • Guía N° 7 Gestión del riesgo. • Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 - ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS
OBSERVACIÓN	**Ausencia de tipificación de riesgos en temas de seguridad y privacidad de la información dentro de la metodología institucional establecida por la entidad para la administración de los mismos.**

	principal causa de los incidentes de seguridad dentro de un sistema determinado, esto debido al desconocimiento sobre seguridad de la información y su rol dentro de una Entidad. En este sentido la entidad cuenta con la inclusión de un plan de comunicación de la estrategia de gobierno en línea enmarcado dentro del plan estratégico de seguridad y privacidad de la información en sus páginas 44 y 45, de igual forma se cuenta con un plan de comunicación más a fín a una estrategia de medios que al conjunto de los requerimientos del modelo. Sin embargo se puede afirmar que la Dirección de Transito de Bucaramanga **NO** cuenta con un plan de comunicación, Sensibilización y Capacitación de Seguridad de la Información acorde con el modelo emanado por el MINTIC.
RECOMENDACIÓN	Realizar un plan de comunicación, sensibilización y capacitación de seguridad de la información acorde a las directrices del MPSI.

HALLAZGO N° 10	
CRITERIO	• Norma técnica NTC ISO/IEC 27001:2013. • Circular 002 del 6 de julio de 2011 del Ministerio de Tecnologías de la Información y las Comunicaciones • PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI 2021-2023 PL-GTIC-001 • Guía de transición de IPV4 a IPV6 del MSPI.
OBSERVACIÓN	**Fortalecer y estructurar las actividades que conllevan a la transición de IPV4 A IPV6 de forma medible y delimitada en tiempo** Revisado el PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI 2021-2023 PL-GTIC-001 suministrado por la oficina de Sistemas, el equipo auditor observa que el plan actual de la entidad, en relación de la transición de ipv4 a ipv6, hace énfasis en conectividad, en el que indica: "*se planea a futuro cercano mejorar la red de cableado estructurado a los diferentes pisos de la entidad, también pasar del estándar IPV4 a IPV6 para que haya más direcciones IP para conectarse al internet*", seguido se evidencia en el titulo 8.2. Estructura de actividades estratégicas, donde proponen realizar actividades con el fin de mejorar los servicios TI de la entidad; si bien es cierto se cuenta con el plan anterior, este mismo define actividades a futuro, las cuales carecen de termino de tiempo en meses para cumplirlas como lo plantea la guía de transición de IPV4 a IPV6 del MSPI, cabe señalar la importancia de precisar y cumplir el término de las actividades definidas y realizar la validación previa de la infraestructura

	Las entidades públicas podrán mitigar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", esta normatividad y guías antes mencionada da un hoja de ruta para la tipificación de riesgos en estos temas. En este sentido la Dirección de Tránsito de Bucaramanga tipifico los riesgos de la entidad para cada uno de sus procesos en concordancia con las directrices del departamento administrativo de la función pública, siendo identificados tres riesgos para el área de sistemas, donde no se incluyeron riesgos referentes al tema de seguridad y privacidad de la información, estos riesgos de posibles acciones de vulneración deben ser entendidos dentro de la entidad con carácter transversal, toda vez que su materialización estaría vinculada a la operación misional de la entidad. La tipificación de los riesgos debe definir controles que se formulen en concordancia con el ítem 5.4 **Controles asociados a la seguridad de la Información** de la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5.
RECOMENDACIÓN	Identificar y formular los riesgos referentes a los temas de seguridad y privacidad de la información e Incluirlos dentro de la matriz de riesgos del proceso gestión TIC de acuerdo a la normatividad vigente en la materia.

HALLAZGO N° 9	
CRITERIO	• Norma técnica NTC ISO/IEC 27001:2013. • Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3 • Modelo de Seguridad y Privacidad de la Información (MSPI) • Plan Estratégico de Tecnologías de la Información –PETI. • Guía N° 14 Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información
OBSERVACIÓN	**Ausencia de un plan de comunicación, sensibilización y capacitación de seguridad de la información acorde a las directrices del MPSI** El plan de comunicación, sensibilización y capacitación de seguridad de la información es una herramienta fundamental para la adopción de las políticas y procedimientos del MPSI dentro de la DTB. Un programa robusto de seguridad y privacidad de la información no se basa únicamente en el aseguramiento de plataformas y procesos, sino que también debe involucrar el factor humano, que en muchos casos, son la

	tecnológica que permita medir el grado de avance en la adopción del protocolo IPv6 en la Entidad; dentro de dicha validación es necesario revisar el grado de compatibilidad del protocolo IPv6 con la infraestructura de TI de la entidad.
RECOMENDACIÓN	Delimitar el tiempo, fortalecer y estructurar las actividades para el cumplimiento de las mismas, siguiendo los lineamientos dados en la guía del MSPI de tal manera que la información recogida de esta tarea sea insumo para el inicio de fase II de IPv6,

HALLAZGOS	
N° HALLAZGO	**HALLAZGO / DESCRIPCIÓN**
1	Ausencia del respaldo metodológico y debilidad en el diagnostico de la seguridad y privacidad de la información.
2	Deficiencia en la estructura y cronograma del plan de seguridad y privacidad de la información.
3	Falta de adopción y socialización Institucional de la POLÍTICA SEGURIDAD DE LA INFORMACIÓN.
4	Deficiencia, en los lineamientos establecidos por MINTIC y desactualización de las políticas de seguridad y privacidad de la información adoptada por la entidad.
5	Falta de procedimientos de seguridad de la información y lineamientos definidos por el MiNTIC.
6	Falta de integración del Modelo de Seguridad y Privacidad de la Información en el comité Institucional de Gestión y Desempeño.
7	Falta de inventario metodológico de los activos de información de la Dirección de Transito de Bucaramanga
8	Ausencia de tipificación de riesgos en temas de seguridad y privacidad de la información dentro de la metodología institucional establecida por la entidad para la administración de los mismos.
9	Ausencia de un plan de comunicación, sensibilización y capacitación de seguridad de la información acorde a las directrices del MPSI
10	Fortalecer y estructurar las actividades que conllevan a la transición de ipv4 a ipv6 de forma medible y delimitada en tiempo.

RECOMENDACIÓN GENERAL

El equipo auditor recomienda al líder del proceso leer y socializar el presente informe con su equipo de trabajo y formular el respectivo plan de mejoramiento dentro de los 15 días siguientes a la entrega del mismo. De igual forma exhorta al jefe de la oficina asesora a continuar fortaleciendo cada uno de sus procesos en aras de un mejoramiento continuo.

OMAIRA JEREZ TAMI
Asesora Control Interno Gestión - Auditor líder

OBER SOTO SOLANO
Auditor de apoyo

TANIA KATHERINE MANZANO BARRERA
Auditor de apoyo

ANDRÉS ORLANDO RUEDA PEÑA
Auditor de apoyo