ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE HÁBITAT

Informe de Evaluación Independiente y Seguimiento

Informe de Evaluación Independiente	Fecha de Expedición	24	07	2018

Proceso (s) y/o proyecto auditado:	Gestión Tecnológica / Seguridad de la Información
Responsable proceso y/o proyecto auditado:	Subsecretaria de Gestión Corporativa y CID
Objetivo de la Auditoría:	Evaluar el Sistema de Gestión de Seguridad de la Información en su alcance correspondiente al proceso de Gestión Tecnológica de la Secretaria Distrital del Hábitat - SHDT conforme a los requisitos legales vigentes de la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones - MIN TIC.
Alcance de la Auditoría:	El alcance se definió para el Sistema de Gestión de Seguridad de la Información relacionado con el proceso de Gestión Tecnológica de la Secretaria Distrital del Hábitat - SHDT, correspondiente a la vigencia 2017 hasta el 31 de mayo de 2018.
Criterios de la Auditoría:	• Ley 1266 de 2008. "*Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*". • Ley 1273 de 2009. "*Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".* • Ley 1341 de 2009. *"Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC y se dictan otras disposiciones".* • *Decreto 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008*". • Ley 1581 de 2012. "*Por la cual se dictan disposiciones generales para la Protección de Datos Personales*". • Ley 1712 de 2014. *"Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones*". • Decreto 1377 de 2013. "*Por el cual se reglamenta parcialmente la Ley 1581 de 2012*". • Decreto 886 de 2014. "*Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"*. • Decreto 2573 de 2014. "*Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones*". • Decreto 1083 de 2015. "*Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012*". • Decreto 1078 de 2015. "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías Decreto de la Información y las Comunicaciones*" • Decreto 415 de 2016. "*Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el*

	fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones". • Decreto 1499 de 2017." *Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015"*. • Política Pública: CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad Digital. • Norma ISO 27001:2013. Técnicas de seguridad: Sistemas de gestión de la seguridad de la información. Requisitos.
Metodología	Técnicas de auditoría basados en los métodos de observación, confrontación, revisión y comparación. De acuerdo con las normas internacionales de auditoria, la presente es una auditoria de cumplimiento legal, es decir se verificará el cumplimiento del sistema, procedimientos, registros, instructivos y demás documentos que soporten el sistema.

Reunión de Apertura						**Ejecución de la Auditoría**				**Reunión de Cierre**					
Día	08	**Mes**	06	**Año**	2018	**Desde**	12/06/2018 D / M / A	**Hasta**	28/06/2018 D / M / A	Día	29	Mes	06	Año	2018

Representante Alta Dirección	**Asesor de Control Interno**	**Auditor (es)**
Giovanni Salgado Rubiano	Viviana Rocio Bejarano Camargo	Giovanny Mancera Marín

I. FICHA TECNICA

De acuerdo con el artículo 2.2.9.1.2.3 del decreto 1078 de 2015 *"…los instrumentos para la implementación de la estrategia de Gobierno en Línea serán los siguientes: Manual de Gobierno en Línea."***,** el cual define las acciones que corresponden ejecutar a las entidades del orden nacional y territorial para la implementación de dicha estrategia, tomando como base Modelo de Seguridad y Privacidad de Seguridad de la Información – MSPI que consta de cinco (5) fases de implementación.

Universo:

Ciclo de operación de cinco (5) fases del Manual de Gobierno en Línea - Modelo de Seguridad y Privacidad de Seguridad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones – Min Tic.

Las fases son:

- Diagnostico,
- Planificación,
- Implementación,
- Evaluación del Desempeño y
- Mejora Continua.

Población objeto:

Ciclo de operación de cinco (5) fases del Manual de Gobierno en Línea - Modelo de Seguridad y Privacidad de Seguridad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones – Min Tic.

Las fases son:

- Diagnostico,
- Planificación,
- Implementación,
- Evaluación del Desempeño y
- Mejora Continua.

Muestra de Auditoria:

Ciclo de operación de cinco (5) fases del Manual de Gobierno en Línea - Modelo de Seguridad y Privacidad de Seguridad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones – Min Tic.

Las fases son:

- Diagnostico,
- Planificación,
- Implementación,
- Evaluación del Desempeño y
- Mejora Continua.

Herramientas Utilizadas:

- **Documentales:**
- Archivo Word denominado Análisis de Contexto.
- Archivo Word denominado Resultados de evaluación y Diagnósticos – Dominios ISO 27001 – ISO 27002.
- Archivo Word denominado pruebas de vulnerabilidad.
- Archivo power point denominado SDHT- Informe ejecutivo de pruebas externas.
- Archivo Word denominado pruebas de Ingeniera Social SDHT.
- Archivo PDF denominado PS05-MN13 Manu Políticas V2.
- Archivo PDF denominado Resolución 137 de 2017.
- Archivo Excel denominado Matriz Activos de Información.
- Archivo Excel denominado Índice Clasificación Información SDHT.
- Archivo Word denominado Plan Diagnóstico y Estrategia Transición IPV4 a IPV6.
- Archivo Excel denominado Instrumento de Evaluación 2018 MSPI – Actualizado (Consolidado).
- Archivo Excel denominado Mapa de Riesgo de Proceso Gestión Tecnológica.
- Sistema Integrado de Gestión – SIG / Procedimientos / Proceso Gestión Tecnológica.

Tecnológicas

N/A

Dando cumplimiento al plan de auditoria, en reunión del 29 de junio de 2018, la Asesora de Control Interno realizó comunicación de los resultados auditoria y entrega del informe preliminar, al responsable del proceso auditado, Subsecretario de Gestión Corporativa y Control Interno Disciplinario.

Mediante radicado 3-2018-03379 del 09 de julio de 2018, el Subsecretario de Gestión Corporativa y Control Interno Disciplinario, presentó respuestas a las observaciones del informe preliminar de fecha 29 de junio de 2018. Con el fin de expedir el informe definitivo se analizarán las manifestaciones realizadas a cada observación del informe preliminar de la siguiente manera:

II. FORTALEZAS

- La entidad estableció formalmente el Comité de Seguridad de la Información y de Tecnologías de la Información y las Comunicaciones mediante la resolución No 137 de 2017, en el cual unas de las principales funciones es definir las estrategias en materia de seguridad, tecnologías de la información y conectividad que deben implementarse.
- Se realizaron las actividades relacionados con el diagnóstico que conllevaron a determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.
- Se han asignado recursos (físicos, financieros, humanos) para llevar a cabo la planificación del Sistema de Seguridad de la Información en la entidad.
- Se resalta el esfuerzo en cuanto a la actualización de los procedimientos que hacen parte del Sistema de Gestión de Seguridad de la Información -SGSI.
- Se evidenció la disposición y colaboración por parte de los servidores públicos durante el desarrollo de la Auditoría, así como la atención, importancia y respeto que se dio durante el desarrollo de la misma.

III. RESULTADOS DE LA AUDITORÍA

Observación No 1. Documentación incompleta de componentes en la Fase de planificación

En la verificación de la fase de planificación Modelo de Seguridad y Privacidad de la Información – MSPI, se evidenció que de los nueve (9) componentes exigidos, cinco (5) no cumplen con lo establecido en dicho modelo.

A continuación, se describe el estado actual de componentes y requisitos exigidos en la fase de planificación del Modelo de Seguridad y Privacidad de la Información – MSPI:

COMPONENTE	ESTADO	Requisito MSPI
Política de Seguridad y Privacidad de la Información.	En revisión por parte de la Subdirección de Programas y Proyectos (no cumple).	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.
Políticas de seguridad y privacidad de la información.	En revisión por parte de la Subdirección de Programas y Proyectos (no cumple).	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.
Procedimientos de seguridad de la información.	En revisión por parte de la Subdirección de Programas y Proyectos (no cumple).	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.
Roles y responsabilidades de seguridad y privacidad de la información.	Cumple.	
Inventario de activos de información.	Cumple.	
Integración del MSPI, con el sistema de gestión documental de la entidad.	No presentó avance (no cumple)	Documento relacionado con seguridad de la información alineado con el sistema de gestión documental conforme a los parámetros emitidos por el Archivo General de la Nación.
Identificación, Valoración y tratamiento de riesgo.	Presentó un avance parcial (no cumple).	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.
Plan de Comunicaciones.	Cumple.	
Plan de diagnóstico de IPv4 a IPv6.	Cumple.	

Análisis del control frente al riesgo

El posible riesgo que se puede ocasionar es el incumplimiento de un mandato legal, específicamente al numeral 2.2.9.1.3.2. del decreto 1078 de 2015, el cual otorga los plazos para implementar las actividades establecidas en el Manual de Gobierno en línea que para la vigencia de 2018 es el 100%.

De igual modo, al carecer con el desarrollado de la fase de planificación se podría llegar a incurrir en una elaboración errónea del plan de seguridad y privacidad de la información que no se encuentre alineado con los objetivos misionales de la entidad.

Frente a la matriz de riesgos de procesos, se observa que se identificaron tres (3) riesgos, así

- Dificultad en el desarrollo de las funciones a cargo de los servidores de la Entidad por incidencias de carácter tecnológico.
- Interrupción de los servicios tercerizados de telecomunicaciones y Data Center.
- Vulnerabilidad de los sistemas de información de la entidad.

Estos riesgos se planean ser mitigados mediante los controles:

- Escalamiento de incidencias según la tipificación de las mismas.
- Capacitación a los usuarios de mesa de ayuda.
- Garantizar que todos los servicios tercerizados cuenten con acuerdos de niveles de servicio.
- Hacer efectivos los acuerdos de nivel de servicio.
- Registro y monitoreo de fallas en la prestación del servicio.
- Realización de copias de seguridad.
- Aplicación de políticas de seguridad informática, por medio de tecnología dedicada para este fin.
- Implementación del Sistema de Gestión de Seguridad de la Información

Se recomienda identificar riesgos que no están siendo reportados en el proceso con respecto a seguridad de la información y continuidad del negocio de la entidad y revisar los controles establecidos para los riesgos establecidos.

Criterio de auditoria:

- Modelo de Seguridad y Privacidad de la Información en la entidad de acuerdo con los requisitos de legales vigentes de la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones - Min Tic – 8.2 fase de Planificación.
- Decreto 1078 de 2015 - Numeral 2.2.9.1.3.2.
- Decreto 2573 de 2014 – Artículo 10º

Componente: Política de Seguridad y Privacidad de la Información

Respuesta del responsable del proceso auditado:

"Como se indicó en la auditoría realizada, la política general fue aprobada el 1-06-2012 en el Comité del sistema integrado de gestión, Acta No 002 de 2012 y publicada en el mapa interactivo del SIG desde el 27/06/2012. En este sentido, la política se sometió a actualización y fue presentada y aprobada en el comité de seguridad de la información y de las tecnologías de la información y comunicaciones el 19-12-2017 tal como consta en el Acta No 002 de dicho comité, seguido de esta aprobación se presentó a la subdirección de Programas y Proyectos, donde actualmente se encuentra en revisión para aprobación de los cambios realizados y previamente aprobados por dicho comité:"

Respuesta Control Interno:

Durante la auditoria se evidenció que la Política de Seguridad y Privacidad de la Información fue actualizada y aprobada por dos (2) miembros del Comité de Seguridad de la Información y de las Tecnologías de la Información y Comunicaciones (Subsecretario de Gestión Corporativa y CID y Subsecretario de Inspección, Vigilancia y Control de Vivienda), sin embargo, no es el quorum establecido para la toma de decisiones de acuerdo con la Resolución 0137 de 2017. Adicionalmente esta se encuentra en revisión por parte de la Subdirección de Programas y Proyectos. No obstante, se observó que no ha sido socializada al interior de la entidad.

De conformidad con lo establecido en el numeral 8.2 Fase de Planificación del Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - Min Tic, en el cual cita que el resultado de la política de seguridad y privacidad de la información es *"Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad".*

Así mismo, es importante tener en cuenta el decreto 1078 de 2015, específicamente el numeral 2.2.9.1.3.2. el cual otorga los plazos para implementar las actividades establecidas en el Manual de Gobierno en línea que para la vigencia de 2018 es el 100%.

Conclusión: Se mantiene la observación, en las mismas condiciones del informe preliminar.

Componente: Políticas de Seguridad y Privacidad de la Información

Respuesta del responsable del proceso auditado:

"Como se indicó en la auditoría realizada, la política general fue aprobada el 1-06-2012 en el Comité del sistema integrado de gestión, Acta No 002 de 2012 y publicada en el mapa interactivo del SIG desde el 27/06/2012. En este sentido, la política se sometió a actualización y fue presentada y aprobada en el comité de seguridad de la información y de las tecnologías de la información y comunicaciones el 19-12-2017 tal como consta en el Acta No 002 de dicho comité, seguido de esta aprobación se presentó a la subdirección de Programas y Proyectos, donde actualmente se encuentra en revisión para aprobación de los cambios realizados y previamente aprobados por dicho comité:"

Respuesta Control Interno:

Si bien durante el desarrollo de la auditoria, se evidenció en la auditoría que el manual con las políticas de Seguridad y Privacidad de la Información fue aprobado por dos (2) miembros del Comité de Seguridad de la Información y de las Tecnologías de la Información y Comunicaciones (Subsecretario de Gestión Corporativa y CID y Subsecretario de Inspección, Vigilancia y Control de Vivienda), sin embargo, no es el quorum establecido para la toma de decisiones de acuerdo con la Resolución 0137 de 2017. Adicionalmente esta se encuentra en revisión por parte de la Subdirección de Programas y Proyectos. No obstante, se observó que no ha sido socializado al interior de la entidad.

De conformidad con lo establecido en el numeral 8.2 Fase de Planificación del Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - Min Tic, en el cual cita que el resultado de las políticas de seguridad y privacidad de la información es *"Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad."*

Así mismo, es importante tener en cuenta el decreto 1078 de 2015, específicamente el numeral 2.2.9.1.3.2. el cual otorga los plazos para implementar las actividades establecidas en el Manual de Gobierno en línea que para la vigencia de 2018 es el 100%.

Conclusión: Se mantiene la observación, en las mismas condiciones del informe preliminar.

Componente: Integración del MSPI, con el sistema de gestión documental de la entidad.

Respuesta del responsable del proceso auditado:

"La entidad no dispone de una directriz para registros en Entornos electrónicos de Oficina. Tampoco existe un lineamiento establecido por el distrito para dar cumplimiento a la Guía 6 – Gestión Documental del MSPI"

Respuesta Control Interno:

De conformidad con lo expresado en el Artículo 15°, del Decreto 2609 de 14 de diciembre de 2012, que cita "*Armonización con otros sistemas administrativos y de gestión. El Programa de Gestión Documental (PGD) debe armonizarse con los otros sistemas administrativos y de gestión establecidos por el gobierno nacional o los que se establezcan en el futuro",* por tal razón, el modelo de seguridad y privacidad de la información es un sistema de gestión que permite el establecimiento e implementación de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, el cual debe estar integrado con el sistema de gestión documental de la Entidad.

Así mismo, el Modelo de Seguridad y Privacidad de la Información cuenta con la guía No 6 que describe la relación de normas técnicas colombianas - NTC, de consulta, emitidas por el Archivo General de la Nación, sobre la gestión documental.

Conclusión: Se mantiene la observación, en las mismas condiciones del informe preliminar.

Componente: Identificación, valoración y tratamiento del riesgo.

Respuesta del responsable del proceso auditado:

"El documento de metodología de gestión de riesgo se encuentra en revisión, debido a que ya existe una metodología de riesgo general para la SDHT. El documento de análisis de riesgo está aprobado y publicado en el SIG. Como se indicó en la auditoría realizada, la declaración de aplicabilidad fue aprobada en el comité de seguridad de la información y de las tecnologías de la información y comunicaciones el 19-12-2017 tal como consta en el Acta No. 2 de dicho Comité, seguido de esta aprobación se presentó a la Subdirección de Programas y Proyectos, donde actualmente se encuentra en revisión para aprobación e inclusión en el SIG".

Respuesta Control Interno:

Es importante mencionar que la Secretaría Distrital del Hábitat tiene un procedimiento denominado Administración del Riesgo con código PG03-PR06 versión 3 del 24/05/2018, el cual se encuentra alineado a la gestión de riesgos a nivel general y no está enfocado a la identificación, evaluación, tratamiento y seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de información.

Así mismo, de conformidad con lo establecido en el numeral 8.2 Fase de Planificación del Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - Min Tic, en el cual describe que el resultado de la **i**dentificación, valoración y tratamiento del riesgo son los documentos con la metodología, análisis, evaluación y plan de tratamiento de riesgos asociados a seguridad de la información. Igualmente, que el documento con la declaración de aplicabilidad. Estos documentos deben ser revisados y aprobados por la Alta Dirección de la entidad.

Si bien, durante la auditoría se evidenció que el proceso de Gestión Tecnológica se encuentra elaborando un procedimiento para la Gestión de Riesgos de Seguridad de la Información. Así como, se observó que la declaración de aplicabilidad se encuentra aprobada por dos (2) miembros del Comité de Seguridad de la Información y de las Tecnologías de la Información y Comunicaciones (Subsecretario de Gestión Corporativa y CID y Subsecretario de Inspección, Vigilancia y Control de Vivienda), sin embargo, no es el quorum establecido para la toma de decisiones de acuerdo con la Resolución 0137 de 2017. Adicionalmente esta se encuentra en revisión por parte de la Subdirección de Programas y Proyectos.

Conclusión: Se mantiene la observación, en las mismas condiciones del informe preliminar.

Observación No 2. Incumplimiento de los requisitos legales en los componentes de la fase de implementación

En la verificación de la fase de implementación, se evidenció que no existe documentación sobre los componentes exigidos con el Modelo de Seguridad y Privacidad de la Información – MSPI.

A continuación, se describe el estado actual de componentes y requisitos exigidos en la fase de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI:

COMPONENTE	ESTADO	Requisito MSPI
Planificación y Control Operacional.	No cumple	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
Implementación del plan de tratamiento de riesgos.	No cumple	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.
Indicadores de gestión.	Cumple	
Plan de Transición de IPv4 a IPv6	No cumple	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la alta Dirección.

Análisis del control frente al riesgo

El posible riesgo que se puede ocasionar es el incumplimiento de un mandato legal, específicamente al numeral 2.2.9.1.3.2. del decreto 1078 de 2015, el cual otorga los plazos para implementar las actividades establecidas en el Manual de Gobierno en línea que para la vigencia de 2018 es el 100%.

De igual modo, al no contar con la fase de implementación se podría llegar a incumplir las metas previstas de esta fase, tales como: la implementación de plan de tratamiento de riesgos, los indicadores de gestión y el plan de transición de IPv4 a IPV6.

Frente a la matriz de riesgos de procesos, se observa que se identificaron tres (3) riesgos, así:

- Dificultad en el desarrollo de las funciones a cargo de los servidores de la Entidad por incidencias de carácter tecnológico.
- Interrupción de los servicios tercerizados de telecomunicaciones y Data Center.
- Vulnerabilidad de los sistemas de información de la entidad.

Estos riesgos se planean ser mitigados mediante los controles:

- Escalamiento de incidencias según la tipificación de las mismas.
- Capacitación a los usuarios de mesa de ayuda.
- Garantizar que todos los servicios tercerizados cuenten con acuerdos de niveles de servicio.
- Hacer efectivos los acuerdos de nivel de servicio.
- Registro y monitoreo de fallas en la prestación del servicio.
- Realización de copias de seguridad.
- Aplicación de políticas de seguridad informática, por medio de tecnología dedicada para este fin.
- Implementación del Sistema de Gestión de Seguridad de la Información

Se recomienda Identificar riesgos que no están siendo reportados en el proceso con respecto a seguridad de la información y continuidad del negocio de la entidad y revisar los controles establecidos para los riesgos establecidos.

Criterio de auditoria:

- Modelo de Seguridad y Privacidad de la Información en la entidad de acuerdo con los requisitos de legales vigentes de la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones - Min Tic – 8.3 fase de Implementación.
- Decreto 1078 de 2015 - Numeral 2.2.9.1.3.2.
- Decreto 2573 de 2014 – Artículo 10º

Componente: Indicadores de Gestión.

Respuesta del responsable del proceso auditado

"El documento presentado contiene los indicadores de gestión de seguridad y privacidad de la información, los cuales están sujetos a revisión y aprobación, una vez estén aprobada la actualización de los documentos de la fase de planificación".

Respuesta de Control Interno:

Una vez revisada la respuesta a la solicitud de información se observó que en el repositorio de almacenamiento de información \\192.168.12.79\d\documentosauditoria2018-1, existe un documento que contiene los indicadores de gestión de seguridad de la información, el cual cumple con lo establecido en el Modelo de Seguridad y Privacidad de la Información.

Conclusión:

Se acepta la réplica del auditado con respecto al componente de indicadores de gestión. No obstante, se mantiene la observación con respecto a los tres (3) componentes restantes relacionados con la fase de implementación del Modelo de Seguridad y Privacidad de la Información.

Componente: Plan de transición IPv4 a IPv6.

Respuesta del responsable del proceso auditado

"El documento presentado contiene el plan y estrategia para realizar la implementación del protocolo IPv6, el cual está en revisión por parte de gestión tecnológica para ser presentado al comité de seguridad de la información y de las tecnologías de la información y comunicaciones para aprobación y puesta en marcha".

Respuesta de Control Interno:

Si bien el proceso de Gestión Tecnológica presentó un documento con el diagnóstico, actividades del plan y estrategias de transición al protocolo IPv6, no se evidenció que dicho documento se encuentre aprobado por el Comite de Seguridad de la Información y de las Tecnologías de la Información y Comunicaciones, tal como lo establece el numeral 8.2 Fase de Planificación del Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - Min Tic, en el cual cita que el resultado del Plan de Transición de IPv4 a IPv6 es *"Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la alta Dirección".*

Conclusión:

Se mantiene la observación, en las mismas condiciones del informe preliminar.

Observación No 3. Incumplimiento de los requisitos legales de los componentes de la fase de Evaluación y Desempeño

En la verificación de la fase de Evaluación y Desempeño, se evidenció que no existe documentación sobre los componentes exigidos con el Modelo de Seguridad y Privacidad de la Información – MSPI.

A continuación, se describe el estado actual de componentes y requisitos exigidos en la fase de evaluación y desempeño del Modelo de Seguridad y Privacidad de la Información – MSPI:

COMPONENTE	ESTADO	Requisito MSPI
Plan de Ejecución de Auditorías	No cumple	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.
Plan de revisión y seguimiento, a la implementación del MSPI.	No cumple	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.

Análisis del control frente al riesgo

El posible riesgo que se puede ocasionar es el incumplimiento de un mandato legal, específicamente al numeral 2.2.9.1.3.2. del decreto 1078 de 2015, el cual otorga los plazos para implementar las actividades establecidas en el Manual de Gobierno en línea que para la vigencia de 2018 es el 100%.

Así mismo, al carecer con el desarrollo de la fase de Evaluación y Desempeño no se podría llegar a verificar la efectividad, eficiencia y eficacia de las acciones y controles implementados.

Frente a la matriz de riesgos de procesos, se observa que se identificaron tres (3) riesgos, así:

- Dificultad en el desarrollo de las funciones a cargo de los servidores de la Entidad por incidencias de carácter tecnológico.
- Interrupción de los servicios tercerizados de telecomunicaciones y Data Center.
- Vulnerabilidad de los sistemas de información de la entidad.

Estos riesgos se planean ser mitigados mediante los controles:

- Escalamiento de incidencias según la tipificación de las mismas.
- Capacitación a los usuarios de mesa de ayuda.
- Garantizar que todos los servicios tercerizados cuenten con acuerdos de niveles de servicio.
- Hacer efectivos los acuerdos de nivel de servicio.
- Registro y monitoreo de fallas en la prestación del servicio.
- Realización de copias de seguridad.

- Aplicación de políticas de seguridad informática, por medio de tecnología dedicada para este fin.
- Implementación del Sistema de Gestión de Seguridad de la Información

Se recomienda Identificar riesgos que no están siendo reportados en el proceso con respecto a seguridad de la información y continuidad del negocio de la entidad y revisar los controles establecidos para los riesgos establecidos.

Criterio de auditoria:

- Modelo de Seguridad y Privacidad de la Información en la entidad de acuerdo con los requisitos de legales vigentes de la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones - Min Tic – 8.4 fase de Evaluación del Desempeño.
- Decreto 1078 de 2015 - Numeral 2.2.9.1.3.2.
- Decreto 2573 de 2014 – Artículo 10º

Observación No 4. Incumplimiento de los requisitos legales de los componentes de la fase de Mejora Continua

En la verificación de la fase de Mejora Continua, se evidenció que no existe documentación sobre los componentes exigidos con el Modelo de Seguridad y Privacidad de la Información – MSPI.

A continuación, se describe el estado actual de componentes y requisitos exigidos en la fase de mejora continua del Modelo de Seguridad y Privacidad de la Información – MSPI:

COMPONENTE	ESTADO	Requisito MSPI
Mejoramiento Continuo	No cumple	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

Análisis del control frente al riesgo

El posible riesgo que se puede ocasionar es el incumplimiento de un mandato legal, específicamente al numeral 2.2.9.1.3.2. del decreto 1078 de 2015, el cual otorga los plazos para implementar las actividades establecidas en el Manual de Gobierno en línea que para la vigencia de 2018 es el 100%.

Así mismo, al carecer con el desarrollo de la fase de Mejora Continua no se podría diseñar el plan de mejoramiento de seguridad y privacidad de la información para la mitigación de las debilidades y vulnerabilidades encontradas en las fases anteriores.

Frente a la matriz de riesgos de procesos, se observa que se identificaron tres (3) riesgos, así:

- Dificultad en el desarrollo de las funciones a cargo de los servidores de la Entidad por incidencias de carácter tecnológico.
- Interrupción de los servicios tercerizados de telecomunicaciones y Data Center.
- Vulnerabilidad de los sistemas de información de la entidad.

Estos riesgos se planean ser mitigados mediante los controles:

- Escalamiento de incidencias según la tipificación de las mismas.
- Capacitación a los usuarios de mesa de ayuda.
- Garantizar que todos los servicios tercerizados cuenten con acuerdos de niveles de servicio.
- Hacer efectivos los acuerdos de nivel de servicio.
- Registro y monitoreo de fallas en la prestación del servicio.
- Realización de copias de seguridad.
- Aplicación de políticas de seguridad informática, por medio de tecnología dedicada para este fin.
- Implementación del Sistema de Gestión de Seguridad de la Información

Se recomienda Identificar riesgos que no están siendo reportados en el proceso con respecto a seguridad de la información y continuidad del negocio de la entidad y revisar los controles establecidos para los riesgos establecidos.

Criterio de auditoria:

- Modelo de Seguridad y Privacidad de la Información en la entidad de acuerdo con los requisitos de legales vigentes de la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones - Min Tic – 8.5 fase de Mejora Continua.
- Decreto 1078 de 2015 - Numeral 2.2.9.1.3.2.
- Decreto 2573 de 2014 – Artículo 10º

IV. RECOMENDACIONES

- Elaborar un plan de trabajo que determine en el corto plazo, las actividades para implementar las acciones necesarias, con el fin de cumplir con lo establecido en la normatividad vigente y cumplir con los plazos establecidos en el manual de Gobierno Digital.
- Elaborar e implementar un plan de comunicaciones relacionado con los temas de seguridad y privacidad de la información dirigido a todos los funcionarios, contratistas y terceros de la entidad.
- Identificar riesgos que no están siendo reportados en el proceso con respecto a seguridad de la información y continuidad del negocio de la entidad y revisar los controles establecidos para los riesgos establecidos.
- Contar con las licencias de cuentas de correo institucional necesarias y evitar que los funcionarios y contratistas de la entidad usen las cuentas de correo personal y así evitar posibles riesgos de fuga de información.
- Desarrollar un plan de trabajo enfocado a implementar los controles necesarios, con el fin de mitigar las vulnerabilidades a las cuales se encuentran expuestos y comprometidos los componentes informáticos que se relacionan en los informes de las pruebas realizadas (equipos de red interna, aplicaciones web).
- Actualizar el normograma de la entidad con los requisitos y normas legales vigentes relacionados con el sistema de Gestión de Seguridad de la Información SGSI.

EQUIPO AUDITOR

NOMBRE	TEMA AUDITADO	FIRMA
Giovanny Mancera	**Sistema de Gestión de Seguridad de la Información**	**ORIGINAL FIRMADO**

AUDITOR LIDER

NOMBRE	FIRMA
Viviana Rocio Bejarano Camargo	**ORIGINAL FIRMADO**

Para constancia se firma en Bogotá D.C., a los 24 días del mes de julio del año 2018.