Contraloría General de Medellín
¡Con tu participación, Medellín crece!

EVALUACIÓN INDEPENDIENTE PROCESO GESTIÓN RECURSOS E INFRAESTRUCTURA –GESTIÓN TECNOLÓGICA

COMPONENTE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PATRICIA BONILLA SANDOVAL
Contralora General de Medellín

MARÍA ELENA CASTRO ZAPATA
Jefe Oficina de Control Interno

MARTÍN ALEJANDRO COLORADO MESA
Técnico Operativo 1

OFICINA ASESORA DE CONTROL INTERNO

MEDELLÍN, NOVIEMBRE DE 2018

TABLA DE CONTENIDO

TABLA DE IMAGENES

Pág.

INTRODUCCIÓN

En Colombia, durante los últimos años, se ha estado impulsando la eficiencia administrativa y la competitividad de la administración pública como políticas de Estado; en esta vía, una de las iniciativas promovidas por el Gobierno Nacional fue la "Estrategia de Gobierno en Línea"; que ha evolucionado a Política de Gobierno Digital, con cambios sustanciales que buscan construir un Estado más eficiente, transparente y participativo gracias a las TIC. Esto significa que el Gobierno: Prestará los mejores servicios en línea al ciudadano. Logrará la excelencia en la gestión. Empoderará y generará confianza en los ciudadanos.

La política de Gobierno Digital establecida mediante el Decreto 1008 de 2018, forma parte del Modelo Integrado de Planeación y Gestión -M.I.P.G- y se integra con las políticas de Gestión y Desempeño Institucional en la dimensión operativa de Gestión para el Resultado con Valores, que busca promover una adecuada gestión interna de las entidades y un buen relacionamiento con el ciudadano a través de la participación y la prestación de servicios de calidad. La citada política de seguridad, se desarrolla a través de dos (2) componentes, tres (3) habilitadores transversales y cinco (5) propósitos. Si bien no es una política obligatoria para la Contraloría, los avances informáticos y la necesidad de realizar auditorías más oportunas, confiables y eficientes deben apoyarse ciertamente en la tecnología.

En este sentido, la Contraloría General de Medellín -CGM- entidad pública del orden Municipal, en sus Políticas de Operación, 2.7, advierte que pese a no ser sujeto obligado para adoptar los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones -MinTic-, procurará la implementación progresiva de los lineamientos que se definan en este sentido y desarrollar los componentes, los habilitadores y los propósitos antes referidos; razón por la cual la Oficina de Control Interno, dentro de su función evaluadora incluyó en el plan táctico 2018, el habilitador transversal Seguridad de la Información para una evaluación independiente. Elemento éste que procura que las Entidades del Estado, aun las que no hacen parte de la rama ejecutiva, implementen un modelo de seguridad y privacidad de la información que sea la base de aplicación del concepto de Seguridad Digital. Es necesario garantizar este componente, dado la información que se maneja en la entidad y la responsabilidad que se tiene de salvaguardarla, en los términos y condiciones que fijan las leyes que se relacionan con la materia. Es decir, la entidad en todo caso, debe garantizar que las medidas que se asuman, independientes o no de las directrices del MinTic, garanticen la seguridad de la información.

Así, se precisa evidenciar en qué medida la entidad ha procurado el cumplimiento de esos objetivos y qué niveles ha alcanzado.

El modelo de seguridad y privacidad de la información del MinTic contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. Así mismo, advierte seis (6) niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

La Evaluación Independiente se realizó considerando lo señalado en el Plan Estratégico en el Numeral 4. -RUPTURAS ESTRATÉGICAS- que define que la Contraloría, tendrá como fundamento normativo de su gestión entre otros, el Decreto 1499 de 2017, Numerales 11) Gobierno Digital y, 12) Seguridad Digital, es decir, que se sustenta en la Política de seguridad y privacidad de la información, como habilitador transversal a la Política de Gobierno Digital que permite alinearse al componente de TIC para el Estado y TIC para la Sociedad, implementando el modelo de seguridad enfocado en preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la Contraloría General de Medellín.

De conformidad con lo anterior, la evaluación se enfocó en establecer el cumplimiento y los controles que se tienen en la Dirección de Desarrollo Tecnológico, para la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI-, identificar el nivel de madurez obtenido como línea base, así como la apropiación que se tiene en la entidad de este eje habilitador.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Evaluar el nivel de madurez del habilitador transversal seguridad de la información en la entidad de acuerdo con el Plan Estratégico en el Numeral 4. -RUPTURAS ESTRATÉGICAS. (Política de Gobierno Digital).

1.2 OBJETIVOS ESPECÍFICOS

- ✓ Verificar el nivel de cumplimiento de cada una de las cinco (5) fases que comprenden el MSPI según el modelo del MinTic.
- ✓ Establecer si la calificación obtenida a diciembre de 2017 fue desarrollada técnicamente y según la guía de MinTic.
- ✓ Verificar el nivel madurez alcanzado a la fecha en Seguridad y Privacidad de la información.
- ✓ Verificar las tareas de avance durante el 2018, para lograr el 100% establecido por el MinTic.
- ✓ Verificar avances del cumplimiento del Plan de Mejoramiento en relación con Seguridad y privacidad de la información.
- ✓ Establecer si la C.A.D.T. ha identificado los riesgos asociados a seguridad y privacidad de la información.

2. CRITERIOS DE AUDITORÍA

La realización de la evaluación independiente, tiene como fuentes de criterio los siguientes documentos:

- ✓ Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC) vigente de la C.G. de Medellín.
- ✓ Decreto 1078 de 2015 – Reglamentario del Sector de TIC.
- ✓ Decreto 1474 de 2017 – Dirección de Gobierno Digital.
- ✓ Decreto 1008 de 2018 – Política de Gobierno Digital.
- ✓ Guías del MinTic para el modelo de seguridad.
- ✓ Modelo de seguridad y privacidad de la información del MinTic - MSPI.
- ✓ Manual de Gobierno Digital V5,en relación con MSPI.

3. ALCANCE

La información es considerada como un activo de valor estratégico, por esta razón se debieron implementar los mecanismos necesarios que garanticen un adecuado tratamiento en el ciclo de vida de la información, especialmente para los casos que requieren mantener la disponibilidad de la misma.

La Contraloría General de Medellín debe garantizar la seguridad de la información dando cumplimiento a los principios de *Confidencialidad*, *Integridad* y *Disponibilidad* de la información. La información de los entes de control fiscal deberá mantenerse disponible atendiendo las normas que la materia así lo establecen.

La presente evaluación aplica desde el diagnóstico, la planificación, implementación, evaluación del desempeño y mejora continua del MSPI; que dio como resultado la calificación obtenida a diciembre 31 de 2017 y el nivel de avance a octubre de 2018; lo anterior bajo el Marco Normativo aplicable para entidades de Gobierno.

4. METODOLOGÍA

La evaluación incluye: planificación, ejecución, controles, comunicación de resultados, seguimiento al cumplimiento de los planes de mejoramiento en aras de la mejora continua de la entidad.

Cada etapa de la evaluación independiente, será realizada conjuntamente con los dueños del MSPI y el personal de la Entidad involucrado en el mismo, mediante entrevistas y ejecución de pruebas para el desarrollo de la evaluación; conforme se definan. Para lo cual se adelantaron las siguientes etapas:

- ✓ Revisión documental: interna y externa con el fin de definir los criterios para la Evaluación Independiente.

- ✓ Solicitud de información relacionada con el componente teniendo en cuenta el objeto y el alcance definidos.

- ✓ Análisis y evaluación de los documentos soporte con las normas y guías del MinTic.

5. RESULTADOS DE AUDITORÍA

La revisión documental interna permitió determinar las acciones adelantadas por la Contraloría General de Medellín, durante el período de evaluación, en el proceso de implementación de la política de Seguridad de la Información. Igualmente, se compararon dichas acciones con la documentación externa, como: las normas, instrumentos y guías del Ministerio de Tecnologías de la información y las Comunicaciones -MinTic-, el Plan estratégico a 2018, a fin de establecer si la entidad consideró las recomendaciones y aseguró a través de sus propios controles las mejores prácticas de seguridad de la información.

Lo anterior, en virtud a que el Ministerio de las Tecnologías y las Comunicaciones MinTic, en evaluación realizada con corte a junio de 2017, sobre la implementación y los avances en la estrategia de Gobierno en Línea, otorgó a la Contraloría General de Medellín el primer puesto a nivel nacional.

5.1 PLANEACIÓN ESTRATÉGICA

El ente de Control Fiscal ha venido dando cumplimiento en la implementación de la Política de Gobierno Digital, emitida por el Estado a través del MinTic. Gobierno Digital[1] es una de las políticas de gestión y desempeño institucional que se desarrollan en el marco del Modelo Integrado de Planeación y Gestión –M.I.P.G- y se encuentra en el Eje de Gestión para el Resultado con Valores.

La Política de Gobierno Digital está estrechamente relacionada con las políticas de: Planeación Institucional, Talento Humano, Transparencia, Acceso a la Información Pública y Lucha Contra la Corrupción, Fortalecimiento Organizacional y Simplificación de Procesos, Servicio al Ciudadano, Participación Ciudadana en la Gestión Pública, Racionalización de Trámites, Gestión Documental, **Seguridad Digital** y Gestión del Conocimiento y la Innovación.

Por lo anterior y dada la transversalidad de los medios digitales en los procesos internos de la Contraloría de Medellín y en el relacionamiento de ésta con las partes interesadas; las citadas políticas son elemento fundamental en la consolidación de la gestión de TI. La seguridad de la información se constituye entonces en un componente esencial como eje transversal del gobierno digital, la cual debe estar

[1] Manual de Gobierno Digital, 1.2. Gobierno Digital en el Modelo Integrado de Planeación y Gestión, pág.12.

alineada con el Marco de Referencia de Arquitectura TI, con los dos componentes, los demás habilitadores y con los propósitos de la política digital.

La planeación estratégica institucional debe contener acciones concretas para la adopción de un modelo de seguridad y privacidad de la información, que conduzca a la preservación de la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo. En este sentido, la administración dispone de un Plan Estratégico de Tecnologías de la Información y Comunicaciones -PETI- actualizado al año 2018, el cual incluyó un capitulo para el "DIAGNÓSTICO Y SEGUIMIENTO A GOBIERNO EN LÍNEA (…)", dentro del cual está el componente seguridad y privacidad de la información.

De acuerdo con lo consignado en el PETI[2] 2018, el diagnóstico y seguimiento a la entonces denominada estrategia de gobierno en línea, realizado bajo la normativa vigente para la fecha de autoevaluación, Junio de 2017; arrojó como resultado del componente "*Seguridad y Privacidad de la Información*" un puntaje de cumplimiento de 39%.

No obstante lo antes mencionado, encontramos que el Ente de Control Fiscal no describe en su PETI como desarrolla dentro de gobierno de TI, la gestión de la información; gestión que debe estar orientada a generar valor y contribuir al logro de los objetivos estratégicos de la Entidad, utilizando la tecnología como apoyo primordial, en el cual la seguridad de la información juegan un rol fundamental. Tampoco describe como desarrolla lo relacionado con la auditoría y trazabilidad del componente de información[3], de acuerdo con lo señalado por el MinTic.

5.2 NIVEL DE CUMPLIMIENTO DE LAS FASES DEL MSPI

La implementación del Modelo de Seguridad y Privacidad de la Información -MSPI- en la Entidad debe estar determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la CGM; 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.

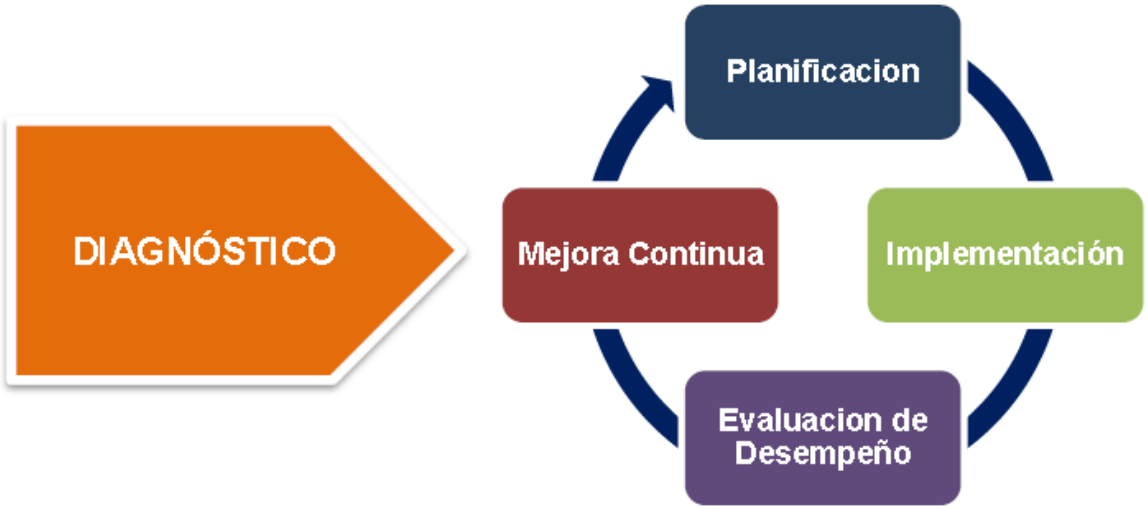
Para una adecuada implementación del MSPI, el Ministerio de TI contempló un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades gestionen adecuadamente la seguridad y privacidad de sus activos de información.

[2] Capitulo 7° Diagnóstico, página 125.

[3] Auditoria y trazabilidad de componentes de información**,** LI.INF.15, Arquitectura de TI, MinTic.

Así mismo, pone a disposición de las entidades 21 guías, instrumentos e instructivos metodológicos que permiten 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. La adopción por parte de la Contraloría de Medellín, de la política de gobierno digital implica la admisión de los lineamientos que en la materia el Gobierno establezca.

Imagen 1. Ciclo de operación del MSPI



Fuente: Modelo de seguridad y privacidad de la información del MinTic.

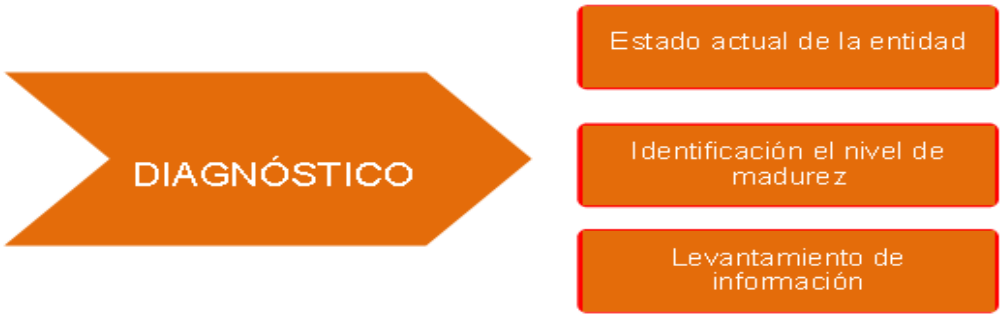
El modelo desarrollado y aplicable a todas entidades públicas de orden nacional, y entidades públicas del orden territorial, reúne una serie pasos e instrumentos que les permiten establecer el estado en que se encuentra la entidad, para posteriormente identificar y adoptar los controles técnicos y administrativos al interior de estas.

5.2.1 Diagnóstico. La fase uno se encarga de identificar el estado del arte de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información -MSPI-.

Para determinar el estado actual o línea base de la gestión de seguridad de la información, el Ministerio habilitó el uso del “INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD” herramienta en Excel conformada por varios componentes. La herramienta de diagnóstico, según la Dirección Administrativa de Desarrollo Tecnológico se empeló en junio de 2017; sin embargo, se evidenció que no se diligenció debidamente ninguno de los elementos del instrumento ya señalados.

No sobra mencionar, que el diagnóstico es fundamental no sólo para determinar el estado actual de la organización con respecto a los requerimientos del MSPI, sino también para identificar y definir las acciones a implementar en el modelo de seguridad de la información en la CGM. Es así como, la política y el modelo de seguridad adoptado deben estar alineados entre sí, direccionados a subsanar las debilidades identificadas en el diagnóstico, apoyados en una metodología de gestión del riesgo, en armonía con la estrategia de TI y enmarcadas en la planeación estratégica de TIC.

Imagen 2. Fase diagnóstico etapa previa a la implementación MSPI



Fuente: Modelo de seguridad y privacidad de la información del MinTic.

Sin un diagnosis técnico o ajustado a los métodos establecidos por el MinTic no hay evidencia, ni claridad cómo la Contraloría de Medellín determinó que el porcentaje de avance a junio de 2017 del 39%; con lo cual se dificulta la elaboración del plan de seguridad de la información ajustado a cerrar las brechas identificadas.

De otro lado, al analizar la última medición del componente, octubre 10 de 2018. Anexo B, (expediente mercurio #0000009564, archivo en Excel #201890009432), en el ítem N°82, la calificación asignada a este criterio fue de uno (1), indicando con ello que si cuenta con ese documento. Empero, el mismo expediente en la hoja “tareas”. Anexo C, incluye como tareas pendientes GEL por realizar: “la construcción del diagnóstico y del correspondiente informe”. Evidenciándose una contradicción en la auto evaluación de la dirección.

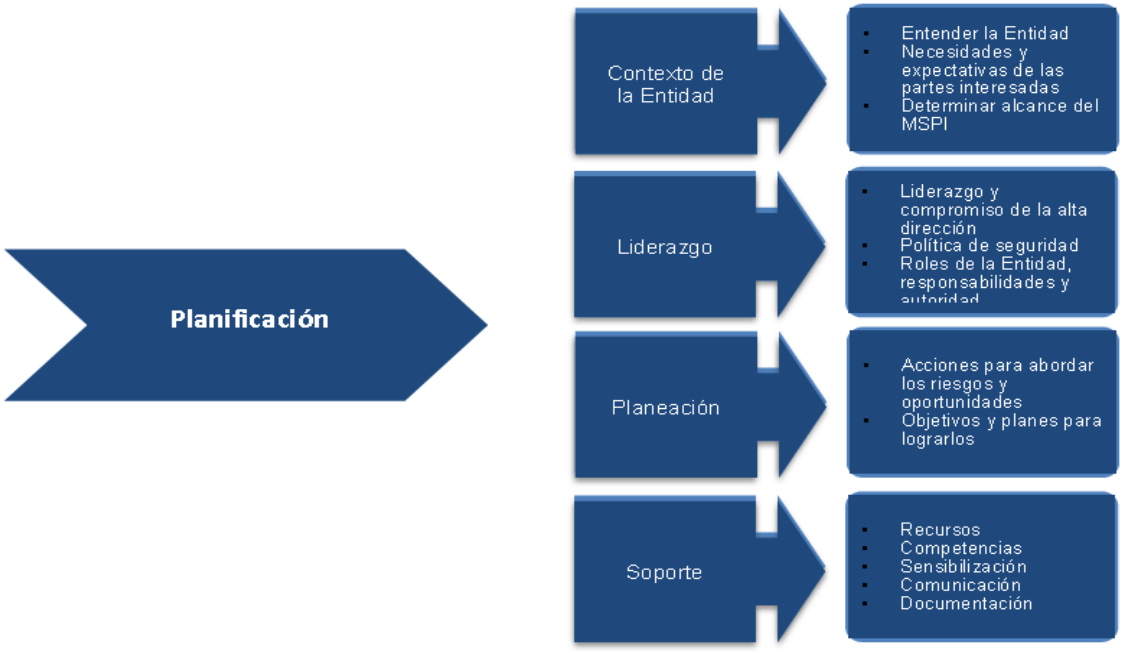
En cuanto al nivel de madurez de los controles de seguridad de la información, tampoco se halló registro que demuestre la medición realizada por la Contraloría y a partir de allí desarrollar la fase de planificación de seguridad. Evaluar el nivel de madurez al interior de la Contraloría, es fundamental para establecer la brecha entre el nivel actual de la entidad y el nivel optimizado, de esta manera diseñar e implementar las acciones que permitan subir de nivel.

Es importante tener presente que en el nivel optimizado, el último de los niveles, se encuentra en las entidades en las cuales la seguridad es un generador de valor para la organización.

Respecto al avance de la implementación del ciclo de operación al interior de la entidad. La Dirección Administrativa de Tecnología efectuó mediciones[4] durante la vigencia 2018. Es así como la última, que data de octubre 10. (Anexo B), indica que el componente Seguridad y Privacidad de la Información alcanza el 87,10% de cumplimiento. Sin embargo, la Dirección de Desarrollo Tecnológico no entrego evidencias físicas suficientes para cada componente, que permita soportar la calificación obtenida.

5.2.2 Planificación. El desarrollo de esta fase inicia con el análisis de los resultados de la etapa de diagnóstico, luego se procede a elaborar el plan de seguridad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad de la información, a través de una metodología de gestión del riesgo.

Imagen 3. Fase planificación MSPI



Fuente: Modelo de seguridad y privacidad de la información del MinTic

[4]Expediente en Mercurio 0000009564, documento #201890009432, archivo en Excel.

La planificación cubre varios aspectos que impactan directamente la consecución de objetivos de la seguridad de la información; para ello el MinTic facilita una serie de guías que describen los procedimientos mínimos que ayudan a desarrollar la planeación, definiendo los límites sobre los cuales se implementará. Los componentes que conforman la planificación del modelo son:

La política de seguridad de la información, como documento de alto nivel, que incluye la voluntad de la Alta Dirección de la CGM de apoyar la implementación del MSPI. En este sentido, de acuerdo con el último seguimiento[5] a la política de gobierno digital realizado por esa Dirección de Desarrollo Tecnológico, enuncia que se dispone de una política que está "Revisada y Aprobada por la alta Dirección". Así mismo, expresa disponer de ella en diversos medios: "Sitio Web, Intranet, Físicamente y en Medios Magnéticos". Sin embargo, la citada política, de acuerdo con la misma Dirección está en construcción, como evidencia entregan a la Oficina de Control Interno una copia de la misma. Ver Anexo A.

Plan de seguridad de la información, la Dirección de Desarrollo Tecnológico no entregó evidencia sobre la elaboración y aprobación de un plan que contemple la manera como la entidad realiza la implementación del MSIP. Tampoco se dispone de un manual que explique de manera general, las políticas, los principios de seguridad y la normatividad pertinente aplicable; en la cual se describan: objetivos, alcances y el nivel de cumplimiento de la política.

Procedimientos de Seguridad de la Información, en este Ítem se desarrollan y formalizan los procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos de la Contraloría. No se halló en la información rendida, procedimientos de seguridad, ajustados con la guía N°3 del MinTic. No obstante, en el numeral 5.1.3 "Implementación" del presente informe; se describen algunas actividades tendientes a gestionar la seguridad de la información.

En cuanto al inventario de activos de información, la entidad cuenta un registro de activos de información actualizado, el cual publican en el portal corporativo. En el cual definen la categoría y la clasificación de la información (Pública, Privada, Interna o Reservada), la criticidad de estos activos, sus propietarios, custodios y usuarios.

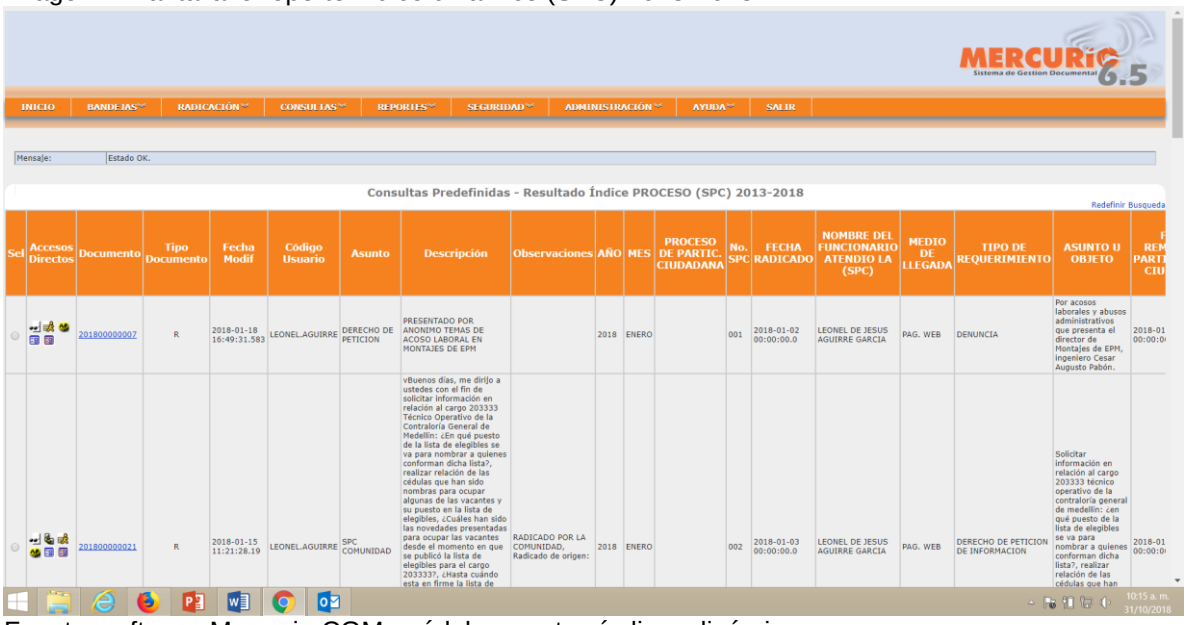
En cuanto a la integración del MSPI con el Sistema de Gestión Documental, conforme a los parámetros emitidos por el archivo general de la Nación; la CGM trabaja en alinearlos. Sin embargo, la Entidad debe realizar un análisis técnico que

[5] Expediente en Mercurio 0000009564, documento #201890009432, archivo en Excel, ítem #89.

permita establecer con los elementos suficientes que el acceso al módulo: Reportes - índices Dinámicos del gestor documental Mercurio, debe estar habilitado para todos los servidores públicos de la CGM. Cabe resaltar que en el año 2017, durante otra evaluación independiente realizada a la Gestión Estratégica: procedimiento Gestión Documental, se evidenció y comunicó que al "reporte índice dinámico proceso (SPC) 2013-2017 puede ser consultado por todos los funcionarios de la entidad, sin restricción alguna". Debilidad de la cual no fue presentada por parte de la administración de TI argumento.

En este sentido, debe analizarse si un exfuncionario de la CGM no se le eliminan o suspenden las credenciales al momento de ser retirado de la Entidad, o encontrarse en vacaciones o en incapacidad, entre otros, tendrá acceso a estos reportes, además sin restricción, lo cual incluye consultar ficha de radicación, así como los datos personales de los peticionarios.

Imagen 4. Pantallazo reporte índice dinámico (SPC) 2013-2018



Fuente: software Mercurio CGM, módulo reportes-índices dinámicos

Los hechos descritos anteriormente toman relevancia al conocer que en varias ocasiones, ciudadanos que elevaron peticiones a la CGM, manifiestan vulneración del derecho a la privacidad de sus datos personales, y que estos fueron filtrados y dados a conocer a otras personas; violando así las normas colombianas en materia de habeas data y protección de datos personales.

Roles y Responsabilidades, la entidad no tiene definido, ni elevado en acto administrativo, los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, de Procesos y Operativos), de acuerdo con la guía N°4 del MinTic. La Dirección de Desarrollo Tecnológico tiene identificado a través del "Instrumento de identificación de la Línea Base" los responsables porcada área, sin que esto se constituya en sí la definición de roles y responsables.

Plan de Comunicaciones**.** La Entidad manifiesta que éste plan de comunicación, sensibilización y capacitación se encuentra en construcción. De su adopción y socialización depende que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles de la entidad.

Plan de transición de IPv4 a IPv6. Para llevar a cabo el proceso de transición de éste protocolo (de IPv4 a IPv6) en las entidades, se debe cumplir con una serie de fases, requisitos y lineamientos establecidos por MinTic en la Guía No 20 "Transición de IPv4 a IPv6" para Colombia, la cual indica las actividades específicas a desarrollar. No obstante, con las respuestas y mediciones de la Dirección de Desarrollo Tecnológico no se puede establecer con suficiencia técnica en qué estado de avance se encuentra la transición del protocolo IP.

Así mismo, no se cuenta con un plan de transición ajustado a las mejores prácticas y guías del Ministerio, el cual debe abordarse por etapas, iniciando en el análisis, la planeación, la implementación y las pruebas de funcionalidad del protocolo IPv6, cada fase tiene definido una serie de entregables por cada una de ellas, con el fin de estimular el proceso de adopción y despliegue del protocolo IPv6.

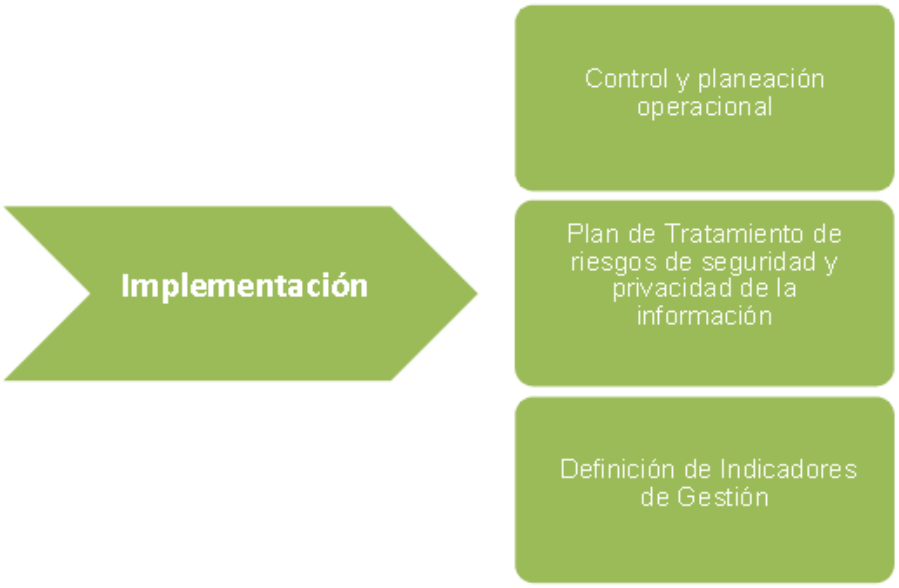
5.2.3 Implementación. La entidad debe gestionar la planeación y la operación de los riesgos de seguridad de la información; para lo cual debió cumplir apropiadamente las dos etapas anteriores del modelo: diagnóstico y planeación. A partir de allí elabora el plan de seguridad, la política, además de la implementación de un plan de continuidad de las operaciones de la CGM.

La planificación y control de los procesos para cumplir con los requisitos de seguridad y privacidad de la información debe estar liderados y bajo la responsabilidad de la Dirección de Desarrollo Tecnológico, para ello debe diseñar e implementar procedimientos de seguridad ajustados a las características particulares, los activos de información, los procesos y los servicios de información que brinda la CGM. Los procedimientos ayudan a implementar las acciones determinadas en el plan de tratamiento de riesgos.

Es fundamental que la Entidad tenga documentada todas las etapas del modelo de seguridad para tener la confianza en que los procesos se han llevado a cabo según

lo planificado, especialmente cuando en la gestión de la seguridad de la información intervienen particulares (contratistas); adicionalmente, el llevar un control de cambios que permita tomar acciones para mitigar efectos adversos cuando sea necesario, acompañado de los indicadores de cumplimiento adoptados en el Manual de Gobierno Digital versión 5.0.

Imagen 5. Fase implementación MSPI



Fuente: Modelo de seguridad y privacidad de la información del MinTic.

No obstante no haber desarrollado esas dos primeras fases, ajustado a los métodos del Ministerio, la Dirección de TI desarrolla múltiples actividades inherentes a la seguridad de la información como lo son:

● La implementación de controles físicos a los sitios donde se procesan y gestionan los datos, para controlar el acceso de personal no autorizado.
● La operación de equipos de suministro de energía eléctrica de respaldo (UPS) para mitigar los cambios repentinos o fallas de suministro eléctrico.
● La operación de un sistema de firewall perimetral para controlar las amenazas existentes en internet.
● Implementación de virtualización de servidores, lo cual coadyuva en la seguridad, facilitando realizar copias de seguridad a las máquinas virtuales, ya que permite programar más rápido y fácil los back-ups.

● La ejecución de antivirus para controlar las amenazas de malware incluyendo los virus informáticos.
● Implementación de un centro alterno de datos, para controlar la amenaza de pérdida de datos.
● La operación de restricciones sobre los equipos de sus usuarios finales (políticas de directorio activo) para controlar amenazas como el abuso de derechos.
● La operación de controles sobre las contraseñas de las cuentas de usuario para controlar amenazas como la suplantación.
● La adopción de un sistema de alta disponibilidad, alto rendimiento y escalabilidad.
● La realización de campañas de concienciación de los usuarios en seguridad informática.
● El establecimiento de políticas operativas para el uso de las TIC que incluyen aspectos de seguridad de la información, para controlar las amenazas derivadas de los comportamientos indebidos de los funcionarios.

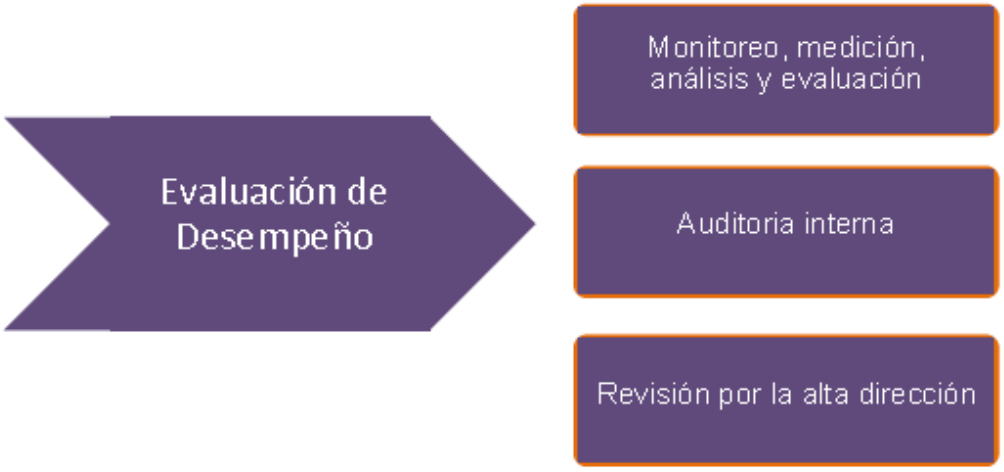
La seguridad perimetral, la gestión de copias de seguridad y la elaboración del plan de contingencias; entre otros, está bajo la responsabilidad directa de un tercero a través de un contrato de prestación de servicios de ingeniería especializada.

En este sentido, llama la atención que luego de la migración del portal web e Intranet a la versión SharePoint 2016, se detectó que no todos los contenidos, como: informes, comunicados, normas internas y externas publicados en la anterior versión (SharePoint 2010), se mantuvieran en los nuevos portales, incumpliendo así normas como la de transparencia, acceso al información y de archivo en relación con las tablas de retención.

5.2.4 Mejora Continua. El proceso de seguimiento y monitoreo del MSPI se debe hacer con base en un plan de revisión y seguimiento a la implementación del modelo, acompañado de los análisis de los resultados que arrojen los indicadores gestión propuestos y adoptados para verificar la efectividad, la eficiencia y la eficacia de las acciones implementadas.

El plan debe consolidar los indicadores periódicamente y su evaluación frente a las metas esperadas; estos deben ser medibles, permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del modelo. Para ello el MinTic dispuso de la Guía No 16 - Evaluación del Desempeño, que brinda información relacionada para poder llevar a cabo la realización de esta actividad.

Imagen 6. Fase evaluación MSPI



Fuente: Modelo de seguridad y privacidad de la información del MinTic.

Respecto a la medición, la dirección de informática de la entidad diligencia periódicamente un instrumento para establecer el avance del MSPI. Al respecto es importante mencionar que durante la evaluación independiente, no se entregaron las evidencias suficientes que sustenten las calificaciones obtenidas, toda vez que cada ítem del modelo calificado debe estar sustentado con evidencias documentales y no se halló o entregó al auditor las pruebas pertinentes para cada componente calificado.

De otro lado, no se ha adoptado indicadores de desempeño, que permitan evaluar el cumplimiento y la efectividad de las acciones implementadas. En cuanto a las auditorías internas, en el año 2017 la Oficina de Control Interno realizó una evaluación independiente a la Estrategia GEL, con corte a diciembre de 2016; evaluación que contempló un apartado para “Privacidad y seguridad de la Información”.

En este sentido, la auditoria antes referida debió ser fuente de mejora, permitiendo que las debilidades detectadas y comunicadas con ocasión de ella, posteriormente se convirtieran en fortalezas, de esta manera complementa el ciclo de mejora continua en relación con el ciclo PHVA.

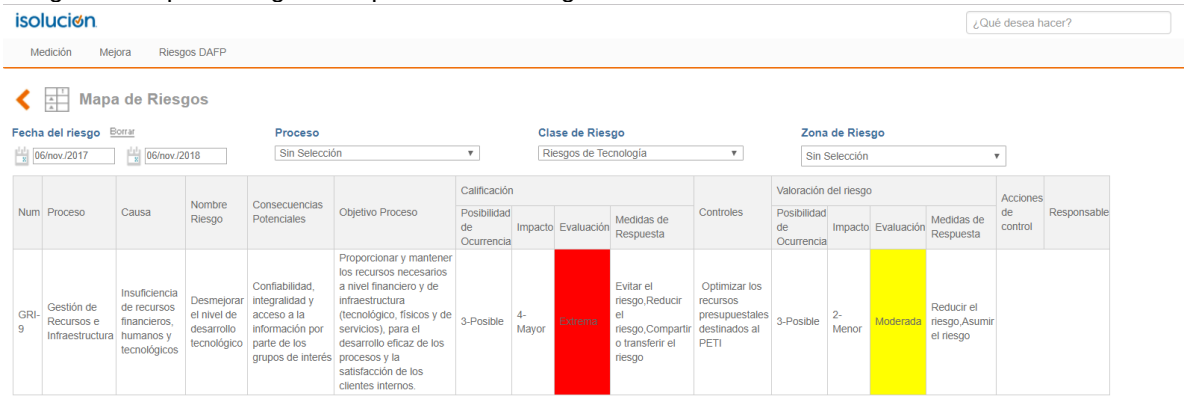
5.3 RIESGOS IDENTIFICADOS EN SEGURIDAD DE LA INFORMACIÓN

Para la identificación, valoración y tratamiento de riesgos, el Ente de Control Fiscal acoge la metodología de gestión del riesgo enfocada a procesos, diseñada por el

Departamento Administrativo de la Función Pública -DAFP-, la cual está orientada a dar seguimiento a los riesgos de gestión y de corrupción. Esta metodología se debe ajustar a la nueva del DAFP: “Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas”, la cual incorpora un capitulo para la seguridad digital.

En mapa de riesgos institucional, el cual se gestiona con sus correspondientes registros en la aplicación ISOlución, incluye solo un riesgo de tecnología; el cual está evaluado a partir de la “insuficiencia de recursos financieros, humanos y tecnológicos”, lo cual puede “Desmejorar el nivel de desarrollo tecnológico”.

Imagen 7. Mapa de riegos componente tecnológico



Num	Proceso	Causa	Nombre Riesgo	Consecuencias Potenciales	Objetivo Proceso	Calificación				Controles	Valoración del riesgo				Acciones de control	Responsable
						Posibilidad de Ocurrencia	Impacto	Evaluación	Medidas de Respuesta		Posibilidad de Ocurrencia	Impacto	Evaluación	Medidas de Respuesta		
GRI-9	Gestión de Recursos e Infraestructura	Insuficiencia de recursos financieros, humanos y tecnológicos	Desmejorar el nivel de desarrollo tecnológico	Confiabilidad, integralidad y acceso a la información por parte de los grupos de interés	Proporcionar y mantener los recursos necesarios a nivel financiero y de infraestructura (tecnológico, físicos y de servicios), para el desarrollo eficaz de los procesos y la satisfacción de los clientes internos.	3-Posible	4-Mayor	Extrema	Evitar el riesgo,Reducir el riesgo,Compartir o transferir el riesgo	Optimizar los recursos presupuestales destinados al PETI	3-Posible	2-Menor	Moderada	Reducir el riesgo,Asumir el riesgo		

Fuente: Sistema ISOlución, módulo riesgos DAFP.

Con respecto a la seguridad digital, el documento CONPES N° 3854 del 2016, con su Política Nacional de Seguridad Digital, aborda el tema como complemento de la política de seguridad y privacidad de la información. El enfoque del CONPES es la ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos: i) defensa del país y ii) lucha contra el cibercrimen; que pueden derivar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico o social para el país, y afectando la integridad de los ciudadanos en este entorno.

Para la seguridad de la información se debe diseñar e implementar un mapa de riesgos, teniendo en cuenta cómo se podría vulnerar alguno de los pilares de la seguridad de la información: i) Disponibilidad, ii) Confidencialidad, iii) Integridad.

Para ello se dispone de la Guía 7 - Gestión de Riesgos del MinTic, como herramienta que facilita la elaboración y la cual está alineada con la Guía de Gestión del Riesgo del DAFP.

No sobra recordar que actualmente la CGM cuenta con su plataforma de rendición de la cuenta para los sujetos que ella vigila, software Gestión Transparente, con hospedaje bajo el esquema de nube pública. Igualmente es fundamental mencionar que no se dispone de un plan de contingencias a pesar de estar definido en el contrato suscrito con HC Inteligencia de Negocios S.A.S.

En este sentido, el MinTic provee a las entidades del estado recomendaciones para minimizar los riesgos para el almacenamiento en nube, para lo cual dispuso la Guía 12 Seguridad en la Nube. Teniendo en cuenta las opciones y que estas pueden variar: nuble pública, nube privada o nube hibrida, los controles de seguridad igualmente varían, dependiendo de la modalidad. De igual manera se deben realizar migraciones de información a la nube basadas en el análisis de riesgos; esto permite tomar las decisiones apropiadas.

6. CONCLUSIONES

La Contraloría General de Medellín ha venido implementando desde hace varios años atrás las políticas que en materia de gobierno digital ha emitido el estado colombiano; sin embargo, a pesar de las gestiones realizadas; según los resultados de las evaluaciones internas, los avances en materia de seguridad de la información no son coherentes con dichos esfuerzos, ni con los parámetros establecidos por el MinTic.

El Modelo de Seguridad y Privacidad de la Información -MSPI, de la Contraloría de Medellín, debe adecuase a las características de la organización, a sus procesos y alinease con el Modelo de Arquitectura TI de la Entidad, de tal forma que respalde transversalmente los dos componentes centrales de la política de Gobierno Digital: TIC para el Estado y TIC para la Sociedad.

El diagnóstico efectuado por la Dirección de Desarrollo Tecnológico, no se desarrolló con la rigurosidad técnica que demanda el MinTic, al no abordar todos los componentes que permiten identificar las situaciones que pueden impactar negativamente a la entidad como consecuencia de vulnerabilidades en la disponibilidad, la confidencialidad y la integridad de la información. Adicional a lo anterior, no se tiene ni el diagnóstico, ni el plan de migración de protocolo IPv6, necesarios para emprender la implementación y las pruebas de funcionalidad.

No disponen de una política de seguridad que aborde la necesidad de la implementación de un sistema de gestión de seguridad de la información planteada desde la Política de Gobierno Digital, apoyados en el grupo de normas ISO 27000. La importancia que ésta política tiene en la entidad, es definir las necesidades de las partes interesadas, la valoración de los controles precisos para mantener la seguridad de la información, teniendo en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales y sus procesos misionales y administrativos.

Por otra parte, dentro de la evaluación independiente se evidenció que las conexiones al portal web, Intranet, correo institucional (a través del servicio de OWA), y el acceso a los aplicativos: Mercurio e ISOlución, no se hacen de manera segura, pues se utiliza el protocolo HTTP y no se emplea un canal cifrado como HTTPS como el implementado para la plataforma Gestión Transparente; esto minimiza los riesgos de intrusos que intercepten la conexión para robar datos de los usuarios, como credenciales de acceso y/o datos personales. Evidencia de lo anterior en el Anexo D, se encuentran imágenes que corroboran lo antes señalado.

En cuanto a la asignación de roles y responsabilidades, no se han definido de manera concertada entre los diferentes servidores públicos o áreas responsables de la seguridad de la información, de esta forma evitar dejar vacíos e imprecisiones respecto a las responsabilidades que cada uno tiene. Por ello la asignación de un responsable para cada acción definida dentro de la planeación de seguridad de la información es un aspecto clave para el correcto funcionamiento del Modelo.

Se debe asignar los roles y responsabilidades, de forma que permita a la Contraloría gestionar adecuadamente la seguridad, ajustada a las cualidades descritas en los manuales: Guía No 4 “Roles y Responsabilidades” del MinTic y en las normas ISO/NTC como el numeral 5.3 de la norma NTC/IEC 27001, toda vez que el modelo abarca aspectos de seguridad como: recurso humano, la gestión de activos, criptografía, la seguridad física y el entorno, la seguridad de la operaciones, entre otros.

Respecto de la identificación, valoración y tratamiento de riesgos, el Ente de Control Fiscal no incluye dentro de su sistema de gestión, aquellos riesgos que impactan la seguridad de la información, ni los riesgos digitales. De esta forma no tiene definido el tratamiento que debe darles, aplicando diferentes enfoques que contengan criterios como: evaluación del riesgo, de impacto y de aceptación del riesgo. Si se materializa un riesgo puede acarrear efectos legales, de imagen y económicos para la entidad, en la medida en que su actividad se detenga durante el tiempo en que tarde en resolver la incidencia. Por otro, la pérdida de datos es un problema cada vez más frecuente. En cuyo caso hay que recordar, que no sólo somos responsables de conservar los datos de la CGM, sino también y sobre todo de nuestros usuarios y sujetos vigilados.

El proceso de mejora continua inicia con los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificar la efectividad, la eficiencia y la eficacia de las acciones implementadas. Pero como poder adelantar un proceso de este tipo, cuando no se dispone de un plan de revisión y seguimiento, ni de los indicadores de cumplimiento o de desempeño, herramientas esenciales para establecer la efectividad de los controles implementados y su apoyo al cumplimiento de los objetivos de seguridad.

Si bien es cierto la Contraloría cuenta con los reportes de desempeño de los diferentes controles de seguridad informática implementados, como lo son el sistema de seguridad perimetral y el sistema de antivirus, los cuales permiten monitorear las amenazas presentes en el entorno y evaluar la efectividad de dichos controles. También es verdad que presta especial atención a los riesgos que puedan comprometer la disponibilidad de la información alojada en su centro de datos, y en

consecuencia, ha desarrollado e implementado un sistema de alta disponibilidad para la infraestructura crítica, unidades de almacenamiento centralizado en discos (SAN) y biblioteca de cintas.

Además, cuenta con un plan de contingencia de tecnologías de la información, actualizado en 2017, en el que se abordan los riesgos catastróficos que puedan comprometer la operación del centro de datos principal y se proponen planes de respuesta a los mismos, a fin de recuperar algunos de los servicios informáticos esenciales.

No obstante, no es entendible cómo a pesar de toda esa infraestructura y estrategia descrita en el citado plan de contingencias, con la migración de la versión SharePoint 2010 de los portales web e Intranet, a la versión SharePoint 2013, se deje de publicar por pérdida, un volumen considerable de contenidos existentes en la anterior versión. Olvidando que mucha de aquella información publicada en la anterior versión de los portales, aún está vigente y que la misma atiende las normas sobre publicidad y acceso a la información.

No se entregó o halló, lineamientos o aspectos a tener en cuenta para el aseguramiento de la información en la nube -Cloud-; de tal manera que se conserve la seguridad de los datos en este tipo de ambientes. La correcta implementación del servicio de información en la nube de la CGM, reducirá el riesgo de que se presenten incidentes de seguridad que afecten la imagen de la entidad y generen un daño irreparable.

Dentro de las políticas de seguridad de la información, se encuentra un elemento trascendental, como lo es la conexión remota o Red Privada Virtual (VPN por sus siglas en inglés). El no disponer de una política que la incluya, expone a la entidad a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas, entre otros.

Es fundamental que la entidad tenga claro el concepto y la finalidad de una política de operación y la política de seguridad de la información. La primera establece las guías de acción para la implementación de las estrategias de ejecución de los procesos y actividades en cumplimiento de la función, los planes, los programas, proyectos.

La segunda tiene por objeto definir claramente las responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización. Se debe entonces establecer los requerimientos mínimos para

configuración de la seguridad de los sistemas y de los datos, y definir las acciones y sanciones por no cumplir con las políticas. Entre otros aspectos.

Finalmente, pero no por ello menos importante es importante que la institución documente, como evidencia de los resultados de la implementación, seguimiento y monitoreo de la gestión que se adelanta en seguridad de la información. Lo anterior en virtud a la puesta en producción de la herramienta de autodiagnóstico y ruta 2019 del MinTic, que entrara en producción entre enero y febrero de 2019.

7. RECOMENDACIONES

Como resultado de la evaluación independiente realizada a la implementación de la seguridad de la información en la Contraloría General de Medellín, ajustada a la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones MinTic; se considera importante realizar las siguientes recomendaciones:

- Dado que la Contraloría General obtuvo del Ministerio de las Tecnologías de la Información y las Comunicaciones -MinTic, en junio de 2017 el primer puesto a nivel nacional, por la implementación y los avances en la estrategia de Gobierno en Línea; se hace fundamental alinear las guías e instrumentos diseñados para la seguridad de la información con la Planeación Estratégica de TI, de esta forma el modelo de gestión de TI incorporaría aspectos de seguridad y privacidad de la información.

- Revisar las diferentes actividades que en materia de seguridad de digital ejecuta la Dirección de Desarrollo Tecnológico, con el objeto de articularlas con el plan de seguridad de la información y así aumentar la capacidad de respuesta para enfrentar las amenazas.

- Conformar un grupo interdisciplinario para la implementación de un Sistema de Gestión de Seguridad de la Información, con roles y responsabilidades definidos claramente; integrado por miembros de la Alta Dirección y de las demás dependencias de la Contraloría, de tal forma que pueda integren aspectos de seguridad como: recurso humano, la gestión de activos, la seguridad física y el entorno, entre otros.

- Formar y capacitar personal de la Dirección de Desarrollo Tecnológico en seguridad de la información y seguridad digital, de esta forma contar con funcionarios al interior de la entidad, en condiciones de liderar y diseñar una coordinación interinstitucional apropiada para la Contraloría.

- Promover la cultura de la seguridad de la información en todos los servidores públicos de la entidad, a fin de generar una mayor conciencia en la gestión de los riesgos asociados a este tema y el impacto en caso de que se materialicen.

- Las entidad debe pensar en realizar pruebas de penetración (también llamadas “pen testing”) a la red de datos; esta es una práctica para poner

a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar. También incluir pruebas de seguridad, son diversas y se orientan a varios ámbitos, especialmente en lo relativo a asegurar el funcionamiento y disponibilidad de los servicios web y contenidos publicados.

- La entidad debe dar cumplimiento a cada una de las cinco (5) fases que comprenden el MSPI propuesto por el MinTic. De esta forma garantizar que se ajusta a las mejores prácticas en materia de seguridad, lo cual busca garantizar que la gestión de riegos de seguridad de la información sea eficaz y eficiente.

- No se puede olvidar que la seguridad de la información debe cubrir todos activos de información de la Contraloría, independiente de su formato: papel, digital, cintas, videos y audios. Toda vez que ya se materializó un riesgo en el archivo central, que funciona en el Centro Administrativo Municipal La Alpujarra, sótano; el cual se inundó, afectando con ello documentación y bienes de la entidad. Razón por la cual se hace esencial que se implemente la gestión de riesgos de información con la rigurosidad debida.

- La política y el plan de seguridad de la información, para estar acorde con las buenas prácticas de seguridad y continuidad, deberá ser actualizado periódicamente; así mismo, recoger los cambios técnicos de las normas de Protección de Datos Personales y Transparencia y Acceso a la Información Pública, entre otras; las cuales se deben tener en cuenta para la gestión de la información.