Radicado DADEP No. 20201300017113
20201300017113

Bogotá D.C, 06-07-2020
130-OCI

MEMORANDO

PARA: **BLANCA STELLA BOHÓRQUEZ MONTENEGRO**
Directora

DE: **ROGER ALEXANDER SANABRIA CALDERÓN**
Jefe Oficina de Control Interno

ASUNTO: Auditoría al Mantenimiento y Soporte de la Infraestructura tecnológica incluido el Plan de Gestión de Riesgo del proceso y Seguridad de la información (digital)

La Oficina de Control Interno en ejercicio de sus funciones y en especial las establecidas en la Ley 87 de 1993, así como los roles definidos en los Decreto 648 de 2017, también respecto a la estipulado en el Decreto 1078 de 2015, las Resoluciones 004 de 2017 y 305 de 2008, y el Plan Anual de Auditoría PAA 2020-V2, las norma ISO 27001 DE 2013, se permite presentar el informe del asunto, en los siguientes términos:

1. OBJETIVO Y ALCANCE

El objetivo de la presente auditoría consistió en determinar análisis, seguimiento y el grado de cumplimiento a lo establecido en el decreto 1078 de 2015, constatando la seguridad y privacidad de la información. El alcance del presente informe tiene como propósito validar el plan del Modelo de Seguridad y Privacidad de la Información MSPI y su cumplimiento, el plan de la gestión del riesgo de seguridad digital.

2. CRITERIOS DE AUDITORÍA

- Ley 87 de 1993, *"Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones"*.
- Decreto 1008 de 2018, *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"*
- Decreto 648 de 2017, "*Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.*
- Decreto 1078 de 2015, *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*.
- Decreto 1087 de 2015, *"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"*.
- Resolución 305 de 2008 con su respectiva actualización Resolución 004 de 2017, *"Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre"*.
- Norma Técnica ISO 27001 de 2013, Permite el aseguramiento, la confidencialidad e integridad de datos y de la información, así como de los sistemas que permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

- Guía del 2016, "Modelo de Seguridad y Privacidad de la Información" del MINTIC.
- Documentación SIG de la Defensoría del Espacio Público.

3. METODOLOGÍA DE ANÁLISIS

La auditoría se desarrolló en cuanto al plan que ejecuto la Oficina de Sistemas (OS) en el último trimestre de 2019 y las actividades que viene desarrollando y ejecutando durante lo formulado para la vigencia 2020, e igualmente en la verificación de los procedimientos, formatos, guías y por lo que la auditoría se encaminó al cumplimiento de la seguridad de la información en la entidad.

En respuesta al memorando con radicado No. 20201300013483 del 20 de mayo del 2020, en el cual se da apertura a la auditoría, esta oficina procedió a validar la información puesta a disposición por la Oficina de Sistemas-OS a través del radicado 20201400013953, así mismo se solicitó el diligenciamiento de un documento en Excel diagnóstico de cumplimiento relacionado con el MSPI y los dominios de control de la norma ISO 27001 DE 2013. Esta oficina realizó seguimiento a los anexos presentados en la carpeta pública provista por la OS para verificar, observar, cotejar y confrontar, constando con las respuestas suministradas en reuniones de fechas 18 y 30 de junio de la presente vigencia, con el personal encargado y responsable de la ejecución de las actividades en el área.

El desarrollo del seguimiento se realizó de la siguiente manera:

a) Validación de la información reportada en la carpeta publica de la OS denominada EVIDENCIA AUDITORIA MSPI de la entidad.
b) Solicitud a la OS el diligenciamiento de la herramienta de verificación al cumplimiento de la norma ISO 27001 de 2013 orientada al cumplimiento del MSPI de la entidad.
c) Verificación de cada uno de los anexos y soportes que comprende el MSPI y los mantenimientos a la infraestructura tecnológica de la entidad.
d) Revisión del plan de gestión del MSPI de la entidad del 2020.
e) Evaluar los procesos y procedimientos en el cumplimiento de la seguridad de la información de la entidad.

Seguido del análisis técnico y confrontación de evidencias, a través de la revisión con el responsable del proyecto, se procede a revisar los planes de la 2020. Adicional a lo anterior, se verificó cada uno de los puntos solicitados en el memorando de apertura de auditoría, relacionados con los planes de seguimiento para la implementación del MSPI y los mantenimientos a la infraestructura tecnológica.

4. ANÁLISIS RESULTADOS Y OBSERVACIONES.

Es necesario señalar que el contenido de este informe se socializó a la Oficina de Sistemas los días 1 y 2 de julio, quienes manifestaron sus observaciones dentro del término establecido respuestas que fueron soportadas, resueltas y tenidas en cuenta, y forman parte integral del presente informe.

Se destaca que en el desarrollo de la presente auditoría la OS ha actuado con celeridad y con toda la disposición en la entrega de la información solicitada, así mismo para estar atento durante la ejecución de esta esto con el propósito de realizar la respectiva verificación de las evidencias suministradas.

Es importante mencionar que la respuesta al memorando de apertura, la OS indico que la mayoría de las evidencias relacionadas, son acciones enfocadas al mejoramiento de la implementación del MSPI desde el último trimestre de 2019 y de lo que se viene desarrollando para la vigencia actual. Por lo

que la OS elaboró un diagnóstico de gestión del MSPI a partir de las nuevas implementaciones a nivel tecnológico y con los nuevos requerimientos generales en relación con las TIC para la entidad. La OS también indica que, en cuanto a los procedimientos, instructivos, protocolos, formatos, guías y lineamientos internos relacionados con seguridad de información se encuentran en constante actualización producto de las nuevas adquisiciones a nivel tecnológico que se está haciendo actualmente en la entidad para el fortalecimiento de la plataforma tecnológica de la Entidad, ubicados en el proceso de Tecnologías de la Información.

Igualmente se realizó la verificación de la herramienta de análisis que establece el grado de avance por dominio u objetivo de control en donde resume y comprende 114 controles del autodiagnóstico del MSPI y al Norma ISO 27001 de 2013 de la OS para el cumplimiento la seguridad de la información en la entidad. Por lo anterior, está auditoría procedió a revisar el cumplimiento y el nivel de avance del MSPI la implementación y verificación en la OS (planificación y organización, e implementación, soporte, servicios y monitoreo), por lo que a continuación las observaciones son:

4.1. Diagnóstico del Modelo de Seguridad y Privacidad de la Información MSPI

La Oficina de Control Interno, solicito a la OS el diligenciamiento de una herramienta de verificación que forman parte de los componentes del MSPI y orientados al cumplimiento de este. Y que se especifica bajo 14 dominios, 35 objetivos de control y un total de 114 controles propuestos para mitigar los riesgos y realizar una adecuada gestión de seguridad de la información en la entidad, aquí se mencionan los que presentan un cumplimiento parcial o no presentan cumplimiento.

- Definición del Marco de Seguridad y Privacidad de la Información

PREGUNTA	VALORACIÓN	EVIDENCIA	OBSERVACIÓN OCI
La entidad ha identificado los aspectos internos y externos que pueden afectar el desarrollo del proyecto de implementación de la seguridad de la información	Cumple parcialmente	Autodiagnóstico del MSPI del MINTIC. Carpeta de Auditoría	Se tiene el diagnóstico realizado en el 2018. Por lo que se debe actualizar a la fecha con las nuevas implementaciones.
La entidad ha identificado las partes interesada, necesidades y expectativas respecto al Sistema de Seguridad de la Información	No cumple	No se observa evidencia para el cumplimiento de este ítem	Se debe realizar la identificación de las partes interesadas por medio de la planeación de encuestas y las expectativas que generen dichas encuestas.

Fuente: OS

- Dominios de Control de la Implementación del Modelo de Seguridad y Privacidad de la Información

Aquí se mencionan los dominios de control que tiene el MSPI de MinTic que comprende los dominios de control de la norma ISO 27001 de 2013 en donde se mencionan los que presentan un cumplimiento parcial y los que no presentan cumplimiento de la implementación de la Seguridad de la Información en la entidad. Es de aclarar que para el dominio de control de la seguridad física y del entorno que corresponde a la prevención de acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento en la entidad, que corresponden a verificaciones que se tenía que hacer en sitio de forma presencial, pero debido a la emergencia sanitaria no fue posible verificar y la cual se consideró una exclusión de la auditoría y no se encuentran previstas en la verificación de cumplimiento.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DOMINIO	VALORACIÓN	EVIDENCIA	OBSERVACIÓN OCI
Revisión de las políticas para la seguridad de la información	Cumple parcialmente	- http://sgc.dadep.gov.co/6/127-MANGI-01.php Manual de Gestión de Seguridad de la Información. - http://sgc.dadep.gov.co/6/127-PPPGI-01.php Política de Seguridad de la Información	Los documentos Política de Seguridad de la Información y Manual de Gestión de Seguridad de la Información se consideran documentos vivos y por consiguiente podrán ser objeto constante de actualizaciones o mejoras que aporten valor en el fortalecimiento de los controles o medidas para proteger de la información del DADEP. Actualmente, se están actualizando todos los documentos teniendo en cuenta los cambios tecnológicos que ha tenido la entidad. Adicional a esto se debe realizar una revisión de las políticas de seguridad en periodos mínimo semestralmente.

Fuente: OS

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
DOMINIO	**VALORACIÓN**	**EVIDENCIA**	**OBSERVACIÓN OCI**
Roles y responsabilidades para la seguridad de la información	Cumple parcialmente	- http://sgc.dadep.gov.co/6/127-MANGI-02.php Manual de Roles y Responsabilidades de Seguridad de la Información	Está definido un documento con roles y responsabilidades en seguridad de la información, falta divulgación y socialización. Por lo que se hace necesario formalizar el documento definido y hacer seguimientos periódicos estableciendo indicadores de cumplimiento.
Política de Dispositivos Móviles	Cumple parcialmente	- http://sgc.dadep.gov.co/6/127-MANGI-01.php Manual de Gestión de Seguridad de la Información.	En el Manual de Gestión de Seguridad de la Información se tienen dos lineamientos que refieren al uso de recursos tecnológicos y el uso de dispositivos de almacenamiento externo móviles. Por lo que se considera que debe ser más específico y debe ser necesario implementar controles de seguridad para el uso, procesamiento, almacenamiento y protección de información con los dispositivos móviles.

Fuente: OS

CRIPTOGRAFÍA			
DOMINIO	**VALORACIÓN**	**EVIDENCIA**	**OBSERVACIÓN OCI**
Política sobre el uso de controles criptográficos	Cumple parcialmente	Certificado de sitio seguro SSL para las plataformas y sistemas de información misionales de la entidad SIDEP y SIGDEP. Así como VPN de Fortinet para un uso protegido de los equipos físicos y virtuales de la entidad.	Se bien se utilizan mecanismos de comunicación de manera segura para la información misional. No se cuenta con mecanismos de encriptación para la información administrativa para garantizar la confidencialidad e integridad de la información.
Gestión de llaves	Cumple parcialmente	Se observo la elaboración de la Circular Interna donde se define los lineamientos de seguridad de la Información para la protección y gestión y uso de documentos electrónicos, y gestión de las firmas digitales.	La circular interna se encuentra pendiente de la aprobación y respectiva socialización, este documento sirve como insumo para la implementación de una política interna para el uso adecuado y protección de gestión de llaves.

Fuente: OS

GESTIÓN DE ACTIVOS

DOMINIO	VALORACIÓN	EVIDENCIA	OBSERVACIÓN OCI
Etiquetado de la información	No cumple	No se observa evidencia para el cumplimiento de este ítem	El cumplimiento de este dominio no se ha cumplido en su totalidad por que la OS trabaja en conjunto con el área de gestión documental. Por lo que se debe tener en cuenta que para asegurar que los activos de información de la entidad reciban el nivel de protección adecuado, estos deben clasificarse teniendo en cuenta la necesidad, las prioridades y el grado de protección en el manejo de estos.
Disposición de Medios	No cumple	No se observa evidencia para cumplimiento de este ítem	Establecer un procedimiento formal debido a que existe información sensible que debe estar dispuesta de manera segura en caso de darla de baja de medios tecnológicos, con el fin de minimizar el riesgo de fuga de la información confidencial.

Fuente: OS

SEGURIDAD DE LAS OPERACIONES			
DOMINIO	**VALORACIÓN**	**EVIDENCIA**	**OBSERVACIÓN OCI**
Registro de eventos	Cumple parcialmente	Se observó que existe un plan de auditorías de TI que establece el análisis y revisión periódica de los registros de seguridad para los sistemas de información.	Si bien se está realizando para los aplicativos misionales de la entidad, se hace necesario que realicen y se revisen los registros de eventos para los demás sistemas de información, para una detección oportuna de las actividades de procesamiento de información no autorizadas.
Registros del administrador y del operador	Cumple parcialmente	Se observó que existe un plan de auditorías de TI que establece el análisis y revisión periódica de los registros de seguridad.	Se está trabajando para que no se logre afectación en la sincronización de tiempos en los recursos. Establecer que solo los roles con función de auditoría tienen acceso a los logs de eventos, así como habilitar todas las aplicaciones el registro de eventos.
Gestión de las vulnerabilidades técnicas	Cumple parcialmente	La evidencia que se observó refiere al tema de análisis de vulnerabilidades basado en servidores de la infraestructura tecnológica.	Se realizó análisis de vulnerabilidades detallado para la infraestructura física de la entidad, para la mitigación respectiva, en base a este análisis la OS realizó un plan armonizado para las vulnerabilidades de criticidad alta, por lo que aún se encuentra pendiente mitigación que presentan vulnerabilidades de criticidad media y baja debido a la falta de recursos financieros. Igualmente se debe establecer un análisis de vulnerabilidades para los servicios que están actualmente en la nube, lo cual depende de la disponibilidad de los proveedores de servicios.

Fuente: OS

SEGURIDAD DE LAS COMUNICACIONES			
DOMINIO	**VALORACIÓN**	**EVIDENCIA**	**OBSERVACIÓN OCI**
Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cumple parcialmente	En el documento “La guía Sistemas de información” en su numeral 4.2.4 PUESTA EN PRODUCCIÓN define que “una vez finalizadas las pruebas descritas en el punto 4.2.3, el administrador de la aplicación presentará en reunión del comité de cambios técnicos, en el cual se evalúan los cambios aprobados para el paso a producción, revisando los servicios que se pueden afectar y acordando las soluciones y los pasos a seguir para cada despliegue así como el plan de reversión del cambio en caso de ser requerido”.	Verificar las demás aplicaciones críticas de la entidad que se deben someter a revisión y ser probadas para asegurar que no hay impacto adverso en la seguridad y realizar pruebas integrales que mantengan datos de protección de la confidencialidad, integridad y disponibilidad.

SEGURIDAD DE LAS COMUNICACIONES			
DOMINIO	**VALORACIÓN**	**EVIDENCIA**	**OBSERVACIÓN OCI**
Protección de datos de prueba	Cumple parcialmente	En la política de adquisición, desarrollo y mantenimiento de sistemas de información define el siguiente lineamiento: "La instalación y configuración de los sistemas de información en los computadores será coordinada y realizada por la Oficina de Sistemas como único responsable. Se generarán los mecanismos necesarios para garantizar la protección y control de datos de prueba y códigos fuente de los programas".	Se tienen ambientes de pruebas que utilizan BD ficticias y BD réplicas de producción (por el tipo de información sensible que se maneja), se recomienda complementar el registro que se tiene actualmente para controlar el tipo de datos, la eliminación segura para no vulnerar la confidencialidad de la información.

Fuente: OS

SEGURIDAD FÍSICA Y DEL ENTORNO			
DOMINIO	**VALORACIÓN**	**EVIDENCIA**	**OBSERVACIÓN OCI**
Disposición segura o reutilización de equipos	Cumple parcialmente	No se observa evidencia para el cumplimiento de este ítem	Se debe llevar un registro de la eliminación o reutilización de los activos de información de forma que la información original no se pueda recuperar.

Fuente: OS

RELACIONES CON LOS PROVEEDORES			
DOMINIO	**VALORACION**	**EVIDENCIA**	**OBSERVACIÓN OCI**
Gestión del cambio en los servicios de los proveedores	No cumple	No se observa evidencia de cumplimiento de este ítem	La entidad requiere realizar diferentes tipos de compras, y contrataciones de servicios, en tal sentido es necesario establecer controles de seguridad para garantizar que se tenga en cuenta los requisitos del negocio antes de gestionar compras o bienes y servicios que afecten la seguridad de la información de la entidad.

Fuente: OS

ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO			
DOMINIO	**VALORACIÓN**	**EVIDENCIA**	**OBSERVACIÓN OCI**
Planificación de la continuidad de la seguridad de la información	Cumple Parcialmente	127-MANGUI-03 Manual de Contingencia de las Tecnologías de la Información donde se identifica los activos de información más críticas del DADEP	Este documento se encuentra desactualizado porque ya que casi todos los servicios de tecnologías de la información están en la nube, Por lo que se debe realizar su respectiva actualización teniendo en cuenta que la entidad debe determinar la continuidad de la seguridad de la información minimizando el impacto generado en su capacidad de ejecución, creando el proceso de gestión de continuidad del negocio.
Implementación de la continuidad de la seguridad de la información	Cumple parcialmente		Tener en cuenta que, para darle continuidad adecuada a la gestión de la seguridad de la información en situaciones adversas, es necesario establecer, documentar, implementar y mantener procesos, procedimientos de la seguridad de la información.
Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Cumple parcialmente	Se observa que al interior de la OS se tienen planes de contingencias para la seguridad de la información	Esta documentación se debe establecer formalmente ya que cualquier cambio sé que se realice al interior de la entidad pueden conducir a cambios en los requerimientos de continuidad de los procesos, procedimientos y controles para la seguridad de la información y se debe realizar revisiones en intervalos en tiempos regulares.

Fuente: OS

CUMPLIMIENTO			
DOMINIO	**VALORACIÓN**	**EVIDENCIA**	**OBSERVACIÓN OCI**
Reglamentación de controles criptográficos.	Cumple parcialmente	Se tiene establecidos mecanismos, lineamientos y buenas prácticas orientados a la reglamentación de controles criptográficos.	Se debe implementar un procedimiento que establezca la respectiva reglamentación por lo que se debe buscar asesoramiento jurídico previo para asegurar el cumplimiento normativo.
Revisión del cumplimiento técnico	Cumple parcialmente	Algunos responsables de las aplicaciones realizan la revisión de archivos de seguridad.	En la actualidad se encuentra construyendo un documento de plan de seguimiento y la formalización que especifique los criterios de revisión periódica de la mano de un plan de auditoria que especifique una periodicidad y se realicen pruebas de penetración y evaluación de vulnerabilidades, teniendo precaución en no comprometer la seguridad del sistema.

Fuente: OS

- Monitoreo y Mejoramiento Continuo

PREGUNTA	VALORACIÓN	EVIDENCIA	OBSERVACIÓN OCI
¿La alta dirección realiza revisiones periódicas al Sistema de Gestión de Seguridad de la Información?	No cumple	No se observa evidencia para el cumplimiento de este ítem.	Es necesario realizar una revisión periódica del Sistema de Gestión de Seguridad de la Información para garantizar la mejora continua, implementando acciones de mejora para que se ajusten a los cambios que puedan surgir en la entidad. Estas revisiones deben ser conocidas y aprobadas por la alta dirección. Así mismo es pertinente capacitar a los usuarios en las modificaciones que sean realizadas.
¿En las revisiones realizadas al sistema por la Dirección, se realizan procesos de retroalimentación sobre el desempeño de la seguridad de la información?			

Fuente: OS

4.2 Mantenimientos de la infraestructura tecnológica

Se evidenció que los registros y actas de soporte de los mantenimientos al hardware de la infraestructura tecnológica de la entidad no tienen un diligenciamiento claro y conciso, se recomienda solicitar al proveedor una mejora de calidad en la presentación de estos que conlleve a mejorar el seguimiento de las actividades de mantenimiento por parte de la OS. Por otra parte, la OS se encuentra adelantando un proceso de contratación de mantenimientos que se denomina “Bolsa de servicios tecnológicos- outsourcing y mantenimiento”. Que incluye como un plan de mantenimiento y de soporte técnico de los recursos tecnológicos de la entidad. Este proceso de contratación se encuentra en una ficha técnica que debe pasar por comité de contratación para que la aprueben, luego se publica en el SECOP para empezar el proceso de licitación y adjudicación del proponente. Por lo que se recomienda que la OS realice seguimiento exhaustivo a todo el proceso previo y de la ejecución del contrato.

4.3 Autodiagnóstico de MIPG

La herramienta de autodiagnóstico se presenta como un instrumento que apoya a las entidades públicas en determinar el estado de avance frente a la gestión de la entidad y con base en ello establecer medidas y acciones de planeación para el mejoramiento continuo, por lo que se debe realizar un análisis y revisión periódica de los procesos y resultados de la gestión, con el propósito de identificar la implementación de planes de mejoramiento pertinentes. Por lo anterior se cuenta con un autodiagnóstico para la Política de Gobierno Digital de la entidad y en un capítulo específico para la seguridad y privacidad de la información, por lo que a continuación se mencionan las que preguntas de seguridad de la información que no se han cumplido en su totalidad.

¿La entidad define indicadores de gestión de la seguridad de la información?

En la actualidad se mide el avance sobre el cronograma de gestión MSPI. En él se evidencia la planeación de la definición de estos indicadores. En el documento soportado por la OS para la presente auditoría se evidenció un plan de seguimiento del 2019 de las fases del ciclo PHVA para el seguimiento a las actividades del MSPI en cumplimiento de seguridad de la información de la entidad con una medición que se tuvo que replantear por la generación de nuevas actividades. Igualmente se observó para el seguimiento de la implementación del MSPI del 2020 más acorde y planificado de cada una de las fases del ciclo PHVA, por lo anterior el porcentaje de avance que se indica en la herramienta web de autodiagnóstico a la pregunta es del 30 % indicando que aún falta por construir actividades dentro del plan y que se estará ejecutando en lo que resta de la presente administración. Por lo que hasta que estas actividades no se ejecuten el porcentaje de cumplimiento dependerá del grado de avance que se ejecute por cada una de estas actividades.

¿Respecto al plan de auditoria de seguridad de la información, la entidad: (definido, definido y se ejecuta, no se tiene)?

Se encuentra definido, se planea ejecutar una vez se hayan realizado las actualizaciones a los documentos en razón a la migración a la nube. Para este ítem la OS desarrollo un documento en donde se observó un cronograma de actividades de vigencia del 15 de mayo de 2020 que establece el plan de trabajo para la verificación y evaluación en el cumplimiento de las buenas prácticas especificadas en la Norma ISO 27001:2013 en los procesos que interactúan con la seguridad de la información. Así como la evaluación de controles implementados vs los indicadores de cumplimiento en la entidad y el porcentaje de avance es del 30% por lo que hasta que no se cumpla y ejecute el cronograma que va desde junio a diciembre del año en curso esta calificación subirá de acuerdo con el cumplimiento de cada una de las actividades aquí descritas.

¿La entidad define un plan de mejoramiento continuo de seguridad de la información?

El cronograma de gestión MSPI 2020 se encuentra con un plan de acción que se está desarrollando sin embargo se debe documentar y medir los posibles impactos que podrían afectar los servicios contratados en la nube. Se cuenta con un seguimiento de la verificación y cumplimiento orientado a las buenas prácticas basados en la Norma ISO 27001 de 2013 desarrollado y ejecutado por la OS , de acuerdo al cronograma de trabajo se vienen cumpliendo con normalidad, por lo que en la actualidad se está realizando el seguimiento al plan de backups, y se tiene proyectado ejecutar durante el presente año algunos otros seguimiento dentro de los que se encuentran los demás dominios de la norma como son el control de acceso, seguridad física y del entorno y seguridad operativa, revisión de la seguridad de las comunicaciones. Por lo anterior la OCI recomienda que se continúe con las actividades de seguimiento en la implementación del MSPI teniendo en cuenta el ciclo PHVA y que se ejecutaran durante la vigencia actual.

4.4 Matriz de Seguridad Digital y el Plan de gestión de riesgo del Proceso

Se cuenta con una matriz de riesgos de seguridad digital de la vigencia 2020 el documento en referencia 127-FORGI-24 en donde se encuentran los riesgos de la infraestructura tecnológica (on premise) y de los riesgos en la nube, esta matriz se encuentra actualizada a marzo del presente año ya que la OS indica que se actualiza trimestralmente con los responsables de los activos tecnológicos de información en la entidad, Por otra parte con el objetivo de establecer un nivel aceptable del riesgo se cuenta con un documento para la declaración de aplicabilidad, pero está pendiente su ejecución e implementación.

En cuanto al plan de gestión de riesgos de seguridad digital se observó diferencias en cuanto a lo reportado vs lo publicado en la página web, el documento 127-PPGI-06 en su versión 01 de 2018 esta publicado en la página web de la entidad y lo que se anexo como evidencia para la presente auditoría esta en versión 2 de 2020 por lo anterior se debe corregir, igualmente no se encontró la definición de cada cuanto (periodicidad) se debe realizar la verificación para la actualización de la matriz de riesgos, así mismo se deben efectuar revisiones en sitio comparando los controles implementados contra la lista de controles que deberían estar.

En cuanto a los activos de información se evidenció que se encuentra pendiente la actualización de los activos de información. De acuerdo con esto, se debe establecer un plan de trabajo en donde se gestione las siguientes observaciones:

- Los siguientes procesos están en el mapa de procesos y no aparecen registrados en el archivo de inventarios de activos de información: Direccionamiento Estratégico, Administración del Patrimonio Inmobiliario, Gestión Jurídica y Gestión Documental.
- Los siguientes procesos no aparecen en el mapa de procesos, pero tienen inventario de activos con análisis de riesgos: Atención al Ciudadano, Verificación y Mejoramiento Continuo, Investigaciones y Administración

Por lo que se debe tener en cuenta que la actualización y clasificación de activos hace parte importante en el MSPI con respecto a la seguridad de los activos de información de la entidad, y se debe cotejar a que todos los procesos de la entidad se le haga el respectivo control de activos y sea coherente con el mapa de procesos.

4.5 Cronograma de Actividades MSPI del 2020

En cuanto al cronograma de seguimiento de las actividades de cumplimiento del MSPI para la vigencia actual se encuentra las diferentes fases del ciclo PHVA y el ultimo seguimiento se encuentra al 30 de abril y de las cuales se mencionan los siguientes que son materia de análisis para la presente auditoría.

FASE	OBJETIVO	ACTIVIDAD	OBSERVACIÓN
Planificación	Establecer las actividades y procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información establecidos en el MSPI	Establecer la Declaración de Aplicabilidad	Se debe construir un documento donde cada uno de los controles es justificado como si se implementa o como si se excluye, lo cual ayuda a la entidad se tenga identificado, documentado y de fácil acceso al inventario de controles.
		Diseñar el programa de sensibilización y capacitación	Se observo un borrador de la vigencia 2019 no se encuentra formalizado por lo que se debe tener en cuenta la definición los temas de las capacitaciones en seguridad de la información de acuerdo con la misionalidad de la entidad. Establecer una metodología que permita evidencias cuales son las necesidades de capacitación para la entidad. Evaluar, medir y cuantificar si el programa implementado genera impacto en la entidad.
		Definir herramientas para el programa de sensibilización y capacitación en seguridad de la información	Se cuenta con un documento en borrador del plan de sensibilización y comunicación, así mismo se cuenta con un cronograma de actividades que van orientadas a el cumplimiento del plan. Se encuentra pendiente la aprobación. Por lo que se recomienda que se pueda aprobar para formalizar el documento, así mismo se recomienda al responsable de seguridad de la información acelerar el proceso de publicación de las herramientas de sensibilización para dar cumplimiento y lograr los objetivos de la seguridad de la información de la entidad.

FASE	OBJETIVO	ACTIVIDAD	OBSERVACIÓN
		Establecer y documentar procedimientos de seguridad de la información	Si bien la OS cuenta con procedimientos orientados al cumplimiento de la seguridad de la información se deben actualizar y elaborar procesos que refieren a las plataformas, aplicaciones o procesos específicos y que sean creados para delinear pasos que deben seguir por una dependencia para la implementación de seguridad relacionada con cada proceso.
		Revisar Informe entregado y hacer seguimiento a la gestión de vulnerabilidades técnicas	Aún se está en proceso de revisión las vulnerabilidades técnicas que se realizaron en la vigencia anterior, por lo anterior de acuerdo con las vulnerabilidades técnicas aún vigentes se debe hacer un análisis de impacto y un plan de remediación contemplado la necesidad de subsanar o aplicar los controles, correcciones o actualizaciones que se le puedan aplicar.
		Definir indicadores de gestión de la seguridad de la información	No se ha desarrollado los indicadores de gestión de la seguridad de la información, por lo que se debe contemplar la medición de efectividad, eficiencia y eficacia de los componentes de seguridad y privacidad de la información, que son de utilidad para la mejora continua. Evaluando la efectividad de la implementación de controles de seguridad.
Implementación	Ejecutar actividades, controles y medidas de protección que permitan la mitigación de riesgos de seguridad de la información.	Realizar análisis de impacto del negocio	No se ha construido la gestión del plan de impacto del negocio en la entidad, este debe contemplar una serie de políticas de restablecimiento de actividades y servicios que apoyen el normal funcionamiento de la infraestructura tecnológica de la entidad que en lo posible las fallas no afecten a máximas interrupciones de la operación.
		Implementar transición Protocolo IPV4 - IPV6.	Analizar, configurar, puesta en marcha, transferencia de conocimiento y hacer pruebas de funcionamiento de la implementación de IPV6 en el DADEP, incluyendo el soporte y pool de direcciones IPV6.
Evaluación de Desempeño	Hacer seguimiento y medición a la implementación del MSPI.	Realizar plan de seguimiento y revisión de la efectividad de la implementación del MSPI.	Se debe seguir con la construcción y el seguimiento del MSPI de la entidad que debe ir orientando a la confidencialidad, integridad y disponibilidad de la información.
		Definir y ejecutar pruebas al Manual de Contingencia de Tecnologías de la Información	El plan de contingencia de tecnologías de la información debe hacer pruebas a los Datos críticos, equipo lógico de base, aplicaciones, equipos físicos y de comunicaciones, documentación. Además, debe contemplar también todos los recursos auxiliares, sin los cuales el funcionamiento de los sistemas podría verse seriamente comprometido suministro de potencia.
Mejora Continua	Determinar los factores y/o aspectos a mejorar que hacen parte del MSPI	Desarrollar plan de mejora continua	Establecer protocolos de seguimiento y revisión y de mejora continua con base en el monitoreo de políticas de seguridad de la información y que permita implantar nuevos controles y/o mejoras al MSPI
		Gestión de indicadores	Este se debe implementar la gestión de seguridad de la información y que permita la medición de la efectividad, eficacia y eficiencia de los controles de seguridad.
		Actualizar guía (procedimiento) para la gestión de eventos	Implementar un documento unificado que apruebe la entidad detectar vulnerabilidades y amenazas que puedan afectar la seguridad de los activos de información por medio de un monitoreo continuo.

5. ANÁLISIS DE POTENCIALES RIESGOS

- Riesgo de seguridad de la información: No tener asociado y contemplado en la matriz de riesgos la revisión de todos los activos de información de la entidad por lo que se debe tener identificado todos los activos para prevenir los riesgos, eventos de riesgos, y una mejora en la efectividad de los controles en la correcta implementación y uso en la entidad.
- Riesgo por Vulnerabilidad de la información: Se observó que se destinó inicialmente recursos para la mitigación de las vulnerabilidades que tienen impacto alto. Por lo anterior se debe realizar nuevos tratamientos a las vulnerabilidades medias y bajas que puedan afectar los sistemas de seguridad de la información.
- Riesgo de ausencia de un plan formal de continuidad: Se debe conocer la capacidad de recuperar y restaurar todas las funciones críticas que hayan sido interrumpidos por algún incidente o desastre y de esta manera prestar los servicios en niveles aceptables.

6. CONCLUSIONES Y RECOMENDACIONES

A nivel general se **observó** que la entidad viene cumpliendo con la fase de planificación prevista y rigurosa con base en diagnósticos realizados para la presente vigencia y que son claros y que permiten que existen planes de acción concretos que se encuentran en ejecución y con tiempos establecidos dentro de las matrices que se suministraron y que aplican a toda la entidad.

Al finalizar el proceso de auditoria realizado por esta Oficina, se observan actualizaciones al MSPI durante la presente vigencia, alineándose a las mejores prácticas del sector y también con lo determinado por el Ministerio de Tecnologías de la Información y las comunicaciones-MINTIC en sus documentos soporte (guías) relacionadas con el desarrollo del tema.

Como conclusión principal se identificaron que la mayoría de los controles se cumplen y se reconoce el esfuerzo y la gestión a la OS, por lo que la OCI recomienda hacer tratamiento a los dominios u objetivos de control del MSPI que están pendientes en su ejecución y cumplimiento, ya que estos pueden generar vulnerabilidades en la seguridad de la información. Muchos de los requerimientos de seguridad establecidos son reconocidos al interior de la OS y en cada uno de los procesos, y algunos de ellos han sido implementados por la necesidad de que no se vuelva a presentar una pérdida de información como sucedió en el año inmediatamente anterior.

Las principales debilidades identificadas en la gestión de la Oficina de Sistemas consisten en que no se observó una adecuada planeación durante la vigencia 2019 teniendo que replantear e identificar las necesidades de adquisición de nuevas tecnologías y de solicitar nuevos recursos para poder mantener la operación en la entidad. También se **observó** que se está dando cumplimiento a las actividades del cronograma de seguimiento al MSPI del ciclo PHVA y se recomienda que se sigan gestionando las actividades de implementación al plan de trabajo establecido en el cronograma.

La auditoría resalta la importancia de continuar con la adopción de los parámetros y requerimientos establecidos en la norma vigente, así como lo establecido en las guías vigentes del MINTIC para mejorar la implementación de la seguridad de la información en la entidad, seguir con la optimización de las capacitaciones técnicas con transferencia de conocimiento principalmente en cabeza del personal de planta de la entidad.

Con base en las observaciones desarrolladas en el informe y las conclusiones presentadas, la Oficina de Control Interno **recomienda**:

- Aprobar y socializar el plan de comunicaciones establecido para el MSPI el cual es dirigido a todos los funcionarios y colaboradores para sensibilizarlos y comprometerlos mediante las buenas prácticas de la seguridad de la información.

- Tener en cuenta la situación a la que se ve abocada la entidad y todas las entidades gubernamentales por la pandemia del Covid-19 que podría afectar el presupuesto requerido para el sostenimiento del personal mínimo requerido para la ejecución de los diferentes proyectos, así como de la plataforma tecnológica; previendo desde este momento una alternativa que permita en forma oportuna lograr la continuidad de la operación en la entidad.

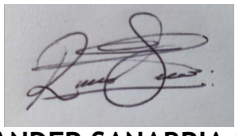
- Formalizar y ejecutar el plan de trabajo para el tratamiento y mitigación de vulnerabilidades técnicas y el buen uso de las herramientas tecnológicas en las que se pudieran ver afectados o comprometidos los componentes informáticos.

- Fortalecer la gestión de los riesgos incluyendo los riesgos asociados a los activos de información que no se han actualizado en la entidad por cada proceso y la criticidad actualizando la matriz de riesgos de seguridad digital.

NOTA: Las observaciones y recomendaciones presentadas por la Oficina de Control Interno en sus informes tienen como fin último generar valor para la Defensoría del Espacio Público, contribuyendo al logro efectivo de los objetivos misionales a través de la mejora continua de los procesos, por esta razón, se espera sean consideradas por los responsables, a quienes se conmina a la realización de los ajustes, correcciones o mejoras a que haya lugar, y a incluirlas en el aplicativo MAP y gestionarlas de manera adecuada, oportuna y preventiva, ante la posible materialización de riesgos y/o pronunciamientos de los diferentes organismos externos de control.

Adicionalmente, es de gran importancia comprender que dada la magnitud de la información, lo evaluado, observado, recomendado y demás aspectos señalados en los informes por esta Oficina, tienen fundamento en verificaciones y revisiones realizadas sobre muestras seleccionadas con técnicas de auditoría, es decir, no es posible cubrir el cien por ciento del universo, por lo cual los responsables de los procesos y la Alta Dirección deben tener presente el autocontrol y considerar la existencia de riesgos en dentro de la información no seleccionada, para lo cual es factible pensar en extrapolar los posibles efectos, controles y correctivos sugeridos para la muestra sobre el total del universo.

Atentamente,



ROGER ALEXANDER SANABRIA CALDERÓN
Jefe Oficina de Control Interno

Copia: **Claudia Liliana Paipa**, Jefe Oficina de Sistemas

Proyectó: Fernando Andrés Salgado Tovar
Fecha: 06-07-2020
Aprobó: Roger Alexander Sanabria Calderón
Código de archivo: 130-85-10