Radicado DADEP No. 20211300031883

20211300031883

Bogotá D.C, 10-09-2021
130-OCI

MEMORANDO

PARA: DIANA ALEJANDRA RODRÍGUEZ CORTÉS
Directora

DE: ROGER ALEXANDER SANABRIA CALDERÓN
Jefe Oficina de Control Interno

ASUNTO: Auditoría al Plan de Gestión del Riesgo de Seguridad y Privacidad de la Información.

La Oficina de Control Interno en ejercicio de las funciones conferidas en la Ley 87 de 1993, Decretos 648 de 2017, Plan Anual de Auditoría PAA-2021, y teniendo en cuenta lo establecido en los Decretos 1008 de 2018 y 103 de 2015, realizó la verificación y se permite presentar el informe del asunto.

1. OBJETIVO Y ALCANCE

El objetivo de esta auditoría consistió en determinar y evaluar las actividades del plan de gestión del riesgo de seguridad de la información de los sistemas de la información, así como los procedimientos, protocolos, guías y/o lineamientos relacionados en la entidad. El alcance tiene como propósito validar la metodología y los puntos de control del plan de gestión del riesgo de seguridad de la información.

2. CRITERIOS DE AUDITORÍA

- Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1del 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 1083 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de 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".
- Resolución 305 de 2008, "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".
- Guía No 7 Guía de Gestión de Riesgos del MINTIC.
- Documentación SIG del Departamento de la Defensoría del Espacio Público.

3. METODOLOGÍA

La evaluación se desarrolló en cuanto a las actividades del Plan de Gestión del Riesgo de Seguridad y Privacidad de la Información de lo formulado para la vigencia 2020, e igualmente en la verificación de los procedimientos, formatos, guías y los lineamientos concernientes al cumplimiento de seguridad de la información en la entidad y se relacionó lo concerniente a la metodología y los puntos

de control que se tienen para el plan de gestión del riesgo de seguridad de la información, realizando revisión y verificación, tanto de la documentación allegada por parte de la Oficina de Sistemas-OS, la Subdirección de Registro Inmobiliario-SRI, además de la información reportada por los funcionarios de los procedimientos, formatos y guías; la auditoría se encaminó al cumplimiento del plan de gestión del riesgo de seguridad y privacidad de la información.

En respuesta al memorando con radicado No 20211300026433 del 27 de julio de 2021, 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 20211400026923, en la verificación de los procedimientos, formatos, guías concernientes al cumplimiento de la seguridad de la información en la entidad de la Subdirección de Registro Inmobiliario-SRI con radicado 2021200002911, se solicitó lo relacionado con los desarrollos pendientes o mejoramiento del aplicativo enviadas a la OS por parte de la SRI, también los usuarios activos dentro del SIDEP y los roles. Esta oficina realizó seguimiento a los anexos presentados mediante correo electrónico provista por la OS y la SRI para cotejar y confrontar, constatando con las respuestas suministradas en reuniones virtuales de fechas 18 y 25 de agosto de la presente vigencia, con el personal encargado y responsable de las actividades en las áreas. La verificación del seguimiento se realizó de la siguiente manera:

a) Revisión de la información solicitada y enviada vía correo electrónico por parte de la OS del mapa de riesgos institucionales.
b) Verificación del plan de gestión de riesgos de seguridad digital de código 127-PPPGI-06 versión 2 vigente desde el 29/01/2020.
c) Consulta de la política de administración de riesgos de código 127-PPPDE-08 versión 2 vigente desde el 29/01/2019.
d) Validación de los informes de seguimiento a la política de la administración de os riesgos de seguridad digital.
e) Revisión de solicitudes de desarrollo o mejoramiento del SIDEP enviadas a la OS por parte de la SRI.

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 vigencia 2020. Adicional a lo anterior, se verificó cada uno de los puntos solicitados en el memorando de apertura de la auditoría, relacionados con el plan de gestión y seguimiento relacionados con los sistemas de información y la infraestructura tecnológica.

4. ANÁLISIS Y DESARROLLO

El contenido de este informe fue presentado a los responsables de la Oficina de Sistemas-OS y la Subdirección de Registro Inmobiliario-SRI, a través de correo electrónico el 4 de septiembre quienes manifestaron sus observaciones por medio de correo electrónico del informe preliminar el 7 de septiembre y en el término establecido con el propósito de ajustar los resultados de la auditoría y por ende las respuestas que fueron soportadas, resueltas y tenidas en cuenta, y forman parte integral del presente informe, de manera que se procede a la presentación del informe final.

Es de resaltar que, en desarrollo de la auditoría acaecieron limitantes para su ejecución, relacionada con entrega tardía de la información solicitada, no se allegaron todos los anexos de manera oportuna, pese a reiteraciones verbales y por correo electrónico en el transcurso de la auditoría.

Es importante mencionar que, en la respuesta al memorando de apertura, las dependencias indicaron que la mayoría de las evidencias relacionadas, son acciones y seguimientos enfocados al mejoramiento del plan de gestión de riesgos de seguridad de la información de las actividades que se vienen desarrollando en la presente vigencia, y que van en pro de mejorar y asegurar los procesos misionales para el fortalecimiento de la plataforma tecnológica de la entidad, que se encuentran publicados en el proceso de Gestión de la Tecnología y de la Información. Cabe resaltar que el proceso de ejecución y avances del mismo, cumplen con las necesidades de la operación de los mismos. Con base a lo anterior, se resalta que el objeto de contar con el plan de gestión de riesgos adecuado, así como contar con una documentación adecuada a las funcionalidades de los sistemas de información que consiste en mejorar y asegurar los procesos misionales de la entidad. Los resultados se presentan en los siguientes términos:

4.1. Plan de Gestión de Riesgos de Seguridad Digital

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-PPPGI-06 en su versión 01 de 2018 está publicado en la página web de la entidad y lo que se anexo como evidencia para la presente auditoría está en versión 2 del 29 de enero de 2020. Se identifico que el plan de gestión de riesgos de seguridad digital hace parte del Modelo de Seguridad y Privacidad de la Información-MSPI y se integra con las fases propuestas en el Modelo de Gestión de Riesgos de Seguridad Digital-MGRSD, así mismo no se ha observado una formulación de una medición de desempeño que formula métricas e indicadores que destaquen la evaluación de la eficacia, efectividad de los controles establecidos.

De acuerdo a lo manifestado por el personal encargado de la OS el plan de gestión riesgos de seguridad digital de la entidad surgirá una actualización, en base a la metodología de la guía de administración y gestión de riesgos del DAFP en su versión 5 de noviembre de 2020, así como las buenas prácticas de gestión de riesgos contemplados en la norma ISO 27005 Sistemas de Gestión de Seguridad de la Información e ISO 31000 Directrices y Principios para gestionar el riesgo de las organizaciones, siento este último un marco de referencia más estructurado. El plan de gestión de riesgos deberá contemplar una serie de lineamientos y condiciones, algunos se mencionan a continuación:

- Contemplar en los objetivos específicos el análisis, evaluación en el mapa de riesgos institucional,
- Identificación de amenazas, controles nuevos que se deberán implementar,
- Definir un plan básico de administración de riesgos de acuerdo al nivel de madurez de la entidad,
- Tener en cuenta el contexto interno y externo y actualizar los procesos,
- Culturizar a los diferentes colaboradores de la entidad para hacer una adecuada administración de riesgos,
- Definir roles y responsabilidades de riesgos deben ser alineados con las líneas de defensa de MIPG,
- Tener en cuenta las diferentes guías de gestión de riesgos de seguridad de la información del MINTIC.

En cuanto al seguimiento al plan de gestión de riesgos de seguridad digital se observó que se encuentra pendiente la actualización del plan. "Con respecto a los diferentes seguimientos en el año 2020 y 2021, y se han realizado por parte de la OS y la OAP, la actualización del formato de mapa de riesgos para hacer una consolidación en una sola matriz de riesgos de gestión, corrupción y seguridad digital, así mismo, se realizó mediante mesas de trabajo con los procesos la definición y actualización

de los riesgos entre los que se encuentra los de seguridad digital, este seguimiento esta para el año 2020 y 2021, también se ha venido realizando el monitoreo de estos riesgos por parte de la OAP, y su información o soportes se encuentran bajo los siguientes términos:

- Evidencia o acta de la revisión por la Dirección donde se presentaron riesgos: Con respecto a la revisión por la Dirección de los Riesgos institucionales (corrupción, gestión y seguridad digital) estos se encuentran en el marco del Comité Institucional de Gestión y Desempeño-CIGyD, donde se revisa la política para la administración de los riesgos y estos se encuentran los de seguridad digital y las actas se encuentran en el link https://www.dadep.gov.co/transparencia/sistema-integrado-de-gestion/gestion-riesgos, teniendo en cuenta que en el primer Comité del 2021 se realizó la revisión de la Política ver 04.1. Comité Institucional del Coordinación de Control Interno, 04.1 Comité Institucional del Coordinación de Control Interno | Departamento Administrativo de la Defensoría del Espacio Público (dadep.gov.co).
- Informes o seguimientos realizados e informes del 2016 a la fecha de la gestión de riesgos (Política de Administración de Riesgos, Mapa de Riesgos y Matriz de identificación de peligros, evaluación, valoración de riesgos y determinación de controles-Matriz IPEVRDC) en el DADEP incluyendo las versiones y seguimientos cuatrimestrales del Mapa de Riesgos Institucionales, los cuales son riesgos de gestión, corrupción y de seguridad digital.
- En el Comité Institucional de Gestión y Desempeño CIGD, no se han tratado temas de riesgos de seguridad digital."

Se cuenta con una matriz de riesgos de seguridad digital de la vigencia 2020, el documento en referencia 127-FORVM-13 que contempla el mapa de riesgos institucional del 2021, esta matriz se encuentra actualizada a enero del presente año ya que la OS indica que se actualiza anualmente con los responsables de las áreas en la entidad. El mapa de riesgos institucional suministrado por la OS de fecha de realización del 29/01/2021 se resaltan algunas consideraciones.

➢ Proceso de la información y la Tecnología

Riesgo	Causas Vulnerabilidades	Control	Actividades de Control	Observación
Daño de Información	-Acceso no autorizado -Administración inadecuada de perfiles de usuarios -Divulgación, prestamos de claves, manejo inadecuado de contraseñas -Sesión abierta	Contrato Antivirus Políticas de acceso a la información	Reglas de cambio de contraseña en el Directorio activo	Se **observó** el gestor de cuentas y políticas de acceso a la información se implementó y se realizaron campañas de sensibilización vía correo electrónico a corte del 31 de agosto de la presente vigencia, pero se encuentra pendiente la gestión del contrato de antivirus, las campañas de prevención de las sesiones abiertas y del uso inadecuado de contraseñas, entre otros. Así mismo es importante mencionar que la OS por medio de la mesa de ayuda realizo seguimiento a los colaboradores de la entidad que no lograron realizar el cambio contraseña luego de la fecha establecida.

No disponibilidad de información	-Dependencia del servicio externo. -Perdida de conectividad	PRD Copias de seguridad	Definir PRD	Se **observó** que se cuenta con el PRD definido y se cuenta con copias de seguridad establecidas y se vienen haciendo con periodicidad. Pero se presentó una incidencia de perdida de conexión por cambios de la configuración de políticas de pasar de un canal alterno a el canal principal dando así la continuidad del servicio, mientras ETB realizaba las respectivas validaciones internas. Esta oficina observó falta de gestión contractual por parte de la ETB para gestionar el cambio en la modalidad del contrato que se tiene en la entidad.
Perdida integridad de la información	-Rotación del personal	Indicadores de mesa de ayuda	Crear ambientes de pruebas y desarrollo	Se encuentran los ambientes de pruebas y desarrollo debidamente custodiados, se actualiza el directorio activo de manera periódica o de acuerdo a las necesidades. Si bien se está cumpliendo con la creación y seguimiento a los ambientes de desarrollo y de pruebas. Es importante tener en cuenta una causa de los riesgos que corresponde a que se presenta una constante en la rotación personal, que hace que no exista continuidad en los procesos que se deben desarrollar desde la OS.
Daños ocasionados a los equipos de cómputo	Fenómenos naturales	Mantenimiento preventivo a los equipos de computo	Gestionar la realización de mantenimien-tos preventivos y correctivos a los equipos de cómputo, y alquiler de computadores	En este riesgo solo se contempló una causa o vulnerabilidad, pero de acuerdo a los eventos en los equipos de cómputo que han generado ralentización, fallas en las actualizaciones del sistema operativo de Microsoft, teniendo que hacer backups y formatear los equipos que han presentado esta falla. Por lo que esta oficina sugiere que se contemple otra causa o vulnerabilidad como puede ser, fallas en la actualización del sistema operativo.

Fuente: OS

- Proceso de Inventario de Espacio Público y Bienes Fiscales

Riesgo	Causas Vulnerabilidades	Control	Actividades de Control	Observación
Daño, perdida o alteración de la información y de los expedientes del proceso de inventario general en el SIDEP y el SIGDEP	-Inadecuado manejo de la información de las carpetas y de su cargue en el SIDEP -Desconocimiento de políticas de seguridad digital	-Manejo de roles y perfiles del SIDEP y SIGDEP. -Manual de usuario del SIDEP.	Actualizar los roles y perfiles del SIDEP	En este riesgo de seguridad digital contemplado por la SRI si bien la OS hace el respectivo seguimiento a los roles y perfiles del SIDEP. Se puede presentar uso inadecuado de la información. Por lo que esta oficina sugiere que exista un control más efectivo que ataque las dos causas de riesgo contempladas. Que exista una cultura del riesgo y se puedan hacer campañas de uso y apropiación de la herramienta.

Fuente: OS

De acuerdo a lo observado y manifestado por la OS la actualización del mapa de riesgos institucional se actualiza, se identifica los riesgos, se evalúan los controles y se hace la revisión de manera anual por cada una de las dependencias, se hacen revisiones en sitio comparando los controles implementados contra la lista de controles que deberían estar, estos deben ir alineados de acuerdo a la metodología de la política institucional de la administración de riesgos de la entidad. Así mismo se actualiza contemplando la seguridad de la información o seguridad digital, los responsables deberán propender por implementar acciones encaminadas a la gestión y su plan de tratamiento. De la misma manera se hace seguimiento liderado por la Oficina Asesora de Planeación-OAP, se realiza de manera cuatrimestralmente y el próximo seguimiento se tiene proyectado para el mes de septiembre.

Es de resaltar que para la política de contraseñas la OS desarrollo un gestor de contraseñas, una socialización en la jornada de inducción y reinducción la política de gestión de cambio de contraseñas, se realizaron constantes piezas comunicativas vía correo electrónico antes de la fecha establecida, es importante y se sugiere que se haga seguimiento a los funcionarios que pudieran presentar alguna incidencia respecto al cambio de contraseña de acuerdo a las políticas, esto con la finalidad que no genere retraso e impacto en el uso de los servicios tecnológicos de la entidad.

De acuerdo con esto, se debe continuar con las actividades de monitoreo y seguimiento contemplando las políticas de tratamiento de riesgos, fortaleciendo lo controles y validando la implementación de nuevos riesgos que se puedan presentar, continuar en la orientación del plan de tratamiento de riesgos, las debilidades y generar controles nuevos.

4.2. Estado y Condición de los Roles y Contraseñas actuales del aplicativo SIDEP

En el documento enviado por la SRI y la OS se reporta algunos de los usuarios que de acuerdo a lo observado podrían estar aún activos en el aplicativo, así:

Subdirección de Administración Inmobiliaria: *Linda Amparo Sánchez Aristizábal (lasanchez@dadep.gov.co), Ernesto Salgado Castaño (esalgado@dadep.gov.co), Fanny Constanza Umbarila Casallas (fumbarila@dadep.gov.co), Eder Camilo Ruiz Luna (eruiz@dadep.gov.co), Claudia Yurani Calderon Benítez (cycalderon@dadep.gov.co) Jenny Andrea Almanza Cortes (jalmanza@dadep.gov.co), Deovigildo Segura Sáenz (dsegura@dadep.gov.co), Lesly Esmeralda Obando Olave (lobando@dadep.gov.co), Jenny Paola García Quitian (jgarcia@dadep.gov.co), María Mónica Montealegre murillo (mmontealgre@dadep.gov.co), John Zuluaga Álvarez (jzuluaga@dadep.gov.co), Álvaro Nino Ramírez (aninor@dadep.gov.co), Wilson Andrés Reinoso González (wreinoso@dadep.gov.co), Adriana Pinzón Novoa (apinzon@dadep.gov.co), Maicol Steven Mora Diaz (mmora@dadep.gov.co), Miguel Ángel Rivera Cortes (mrivera@dadep.gov.co), Rubén Camilo Pedraza Sandoval (rcpedraza@dadep.gov.co), William Arnulfo Moreno Rodríguez (wmoreno@dadep.gov.co), Martha Pena Mateus (mpena@dadep.gov.co), Viviana García Pérez (vgarcia@dadep.gov.co), Diana Marcela Bermúdez (dbermudez@dadep.gov.co), Juan Sebastián Arbeláez (jarbelaez@dadep.gov.co), Sonia Patricia Lozano Pacanchipe (slozano@dadep.gov.co), María Paula Farfán Guaqueta (mfarfan@dadep.gov.co), Alejandra del Pilar García Gutiérrez (apgarcia@dadep.gov.co), Paula Natalia Arbeláez Patino (parbelaez@dadep.gov.co), Mónica Patricia Sierra Amaya (msierra@dadep.gov.co), Erick Fabian García Peláez (egarcia@dadep.gov.co), Natalia Andrea Sáenz (nsaenz@dadep.gov.co), Paulo Andrés Nieto Pineda (pnieto@dadep.gov.co), Miguel Eduardo Romero Parra (meromero@dadep.gov.co), Martha Cecilia Villarreal Mejía (mvillarreal@Dadep.gov.co), Yamile Sáenz Mejía (ysaenz@dadep.gov.co), Olga Janneth Suarez López (ecardenas@dadep.gov.co), Paulo Andrés Nieto Pineda (jfuentes@dadep.gov.co).*

Subdirección de Registro Inmobiliario-SRI: *Sandra Alicia Villarraga Vanegas (svillarraga@dadep.gov.co), Charles Alfonso López Castro (clopez@dadep.gov.co), Luis Fernando Torres García (ltorres@dadep.gov.co), Iván Andrés Felipe Serna Galeano (iserna@dadep.gov.co), Felipe Muñoz (fmunoz@dadep.gov.co), Carlos Andrés Zamora (czamora@dadep.gov.co).*

Oficina Asesora Jurídica-OAJ: *Luz Day Castaneda Hernández (lcastaneda@dadep.gov.co).*

Si bien el aplicativo SIDEP tiene funcionalidades de suspensión del estado de los usuarios y cruzado con el directorio activo de la entidad. Esta oficina recomienda que se valide el estado actual y las condiciones de los roles y contraseñas de los usuarios pendientes de deshabilitar los permisos correspondientes, y que aún se encuentran activos en el aplicativo SIDEP, así como coordinar con los responsables de los procesos con el fin de revisar y aclarar las apreciaciones pertinentes para evitar una posible materialización de riesgos de seguridad digital y que va en pro de la mejora de la seguridad de la información en la entidad.

4.3. Nuevos Desarrollos o mejoramiento del aplicativo SIDEP

Algunas mejoras en las funcionalidades que están en proceso de desarrollo y se encuentran pendientes por implementar o desarrollar desde la OS, y algunas solicitudes que propone la SRI para realizar algunos cambios en el aplicativo SIDEP para incorporar, son solicitudes realizas por el área contable y otra por área técnica para la implementación de las normas internacionales, como también se solicita que se pueda realizar un test en un ambiente de pruebas antes de implementarlo a un ambiente de producción son:

"PROPUESTA MEJORAS AL SISTEMA SIDEP 2.0 REALIZADAS POR LA SUBDIRECCIÓN DE REGISTRO INMOBILIARIO
1. Solicitud que se puedan hacer búsquedas en el aplicativo, en el módulo de Urbanizaciones por plano y por escritura.
2. Que se puedan hacer búsquedas en el aplicativo en el módulo de predios por escritura.
3. Efectuar un desarrollo de tal forma que se pueda consignar en el Sistema un folio de matrícula antigua.
4. Elaborar los diferentes vínculos o enlaces en el sistema de manera directa, ya que siempre que se desengloba o engloba un predio es necesario hacerlo por mesa de ayuda. (esta es una solicitud muy repetitiva). Ej.: 1-5602, 1-5063 – tramite 37353.
5. Se pueda elaborar los diferentes motivos de incorporación y vínculos o construcciones asociadas en una construcción de manera directa. (esta es una solicitud muy repetitiva). Ej.: RUPI 2-2320-1 – Tramite 18145.
6. Elaboración de las actas de toma de posesión, recibo y modificación, por medio del sistema SIDEP 2.0, lo que facilita el seguimiento de este documento.
7. Se requiere adelantar un desarrollo que permita migrar desde la aplicación SIDEP 1, el dato de área por uso, PARA LAS CONTRUCCIONES CON UN SOLO USO y que su terreno o lote NO SE ENCUENTRE ASOCIADO A UN CÓDIGO CHIP.
8. Se requiere adelantar un desarrollo que permita migrar desde el reporte del SIIC suministrado por la UAECD, el dato de área por uso, PARA LAS CONSTRUCCIONES CON UN SOLO USO y que la edificación o su lote SE ENCUENTRE ASOCIADO A UN CÓDIGO CHIP."

Así mismo se **observó** que se encuentran pendientes otras funcionalidades respecto a la implementación del marco normativo contable para entidades de gobierno – NMNC Resolución 533-2015 y sus modificatorias una realizada desde el 11 de marzo de 2019 y la otra solicitada de fecha del 5 de enero de 2021 que corresponde a "especificaciones prácticas de la dinámica de cuentas, para los registros contables a partir del año 2018 se deberá tener en cuenta la planilla de dinámica de cuentas establecida de acuerdo al MNC, afectándolos movimientos de acuerdo al tipo de transacción efectuada".

Desde la vigencia 2018 la OS ha venido trabajando en nuevos desarrollos y modificaciones al sistema SIDEP encaminados a la implementación Nuevo Marco Normativo Contable NMNC, que corresponde a requerimientos realizados por la Subdirección de Administración Inmobiliario y de Espacio Público-SAI y la Subdirección Administrativa Financiera y Control Disciplinario-SAF, y hacen parte del conjunto de requerimientos para la implementación del nuevo marco normativo.

La OS menciona que "algunas de las funcionalidades propuestas han sido mencionadas de manera verbal por SRI, sin embargo no se ha pasado un requerimiento formal con la solicitud de cambios y se han solicitado mesas de trabajo para levantamiento de requerimientos como lo indica el procedimiento de la Oficina de Sistemas", igualmente la OS ha atendido los casos de soporte y modificaciones de base de datos solicitados por la SRI, los cuales no requieren modificaciones al código fuente del sistema de información SIDEP sino directamente a la Data, por lo cual no se consideran nuevos desarrollos. Por lo que esta oficina sugiere que se establezcan las mesas de trabajo por las diferentes subdirecciones y la OS para implementar las mejoras y nuevas funcionalidades que vayan en pro del mejoramiento de los aplicativos misionales de la entidad.

4.4. Aplicativo MAP y CPM

En los aplicativos MAP y CPM para la vigencia 2020 se realizó la auditoría al control de calidad de la información cartográfica con radicado de Orfeo 20201300032453 en donde se observó una serie de ejecución de nuevas funcionalidades en el aplicativo SIDEP orientadas a la implementación del nuevo marco normativo contable NMNC, así mismo una de las observaciones presentadas en el aplicativo MAP y corresponde a "Adopción de los parámetros y requerimientos establecidos en el nuevo marco contable NMNC". Para lo cual La OS crea una acción general en el aplicativo CPM, 200631, actividad 2330 que corresponde a desarrollar en devolución contable de bienes. Nuevo movimiento automático y actividad 2335 que corresponde a realizar pruebas funcionales a la modificación de 3 tramites de defensa administrativa, de fecha de inicio del 2020-11-18 y fecha de vencimiento del 2021-08-31, por lo que no cuenta con alguna evidencia o avance cargada en el aplicativo.

Si bien es cierto que la acción general tiene fecha final del 2021-11-19, es importante tener presente la importancia de ir documentándolas en el CPM, el resorte de las acciones debe ser propio del responsable y si dependen de otra área o proceso demostrar la gestión realizada para lograr lo requerido, lo cual ya debería estar cargado en el sistema. Por lo anterior esta oficina recomienda que se realicen todas las actividades y acciones mencionadas, se documenten y protejan adecuadamente para lo cual debe estar debidamente documentado.

5. ANÁLISIS DE POTENCIALES RIESGOS

- Riesgo de seguridad de la información: No tener asociado y contemplado en la matriz de riesgos, algunos riesgos y controles contemplados, por lo que se debe tener identificado los riesgos propuestos por esta auditoría con el fin de prevenir algunos eventos de riesgos, y una mejora en la efectividad de los controles en la correcta implementación y uso en la entidad.
- Riesgo operativo: Falta de controles en los soportes que evidencian el cumplimiento de las acciones, falta de delegaciones para incidentes, reprocesos.
- Riesgos de sanciones disciplinarias: Por los entes de control debido a los incumplimientos que se pudieran llegar a presentar en el decreto 1008 de 2018, resolución 533 de 2015.

6. CONCLUSIÓN Y RECOMENDACIONES

En términos generales se observó que la entidad viene cumpliendo con las diferentes fases del plan de gestión del riesgo de seguridad digital realizados en la vigencia en la entidad, así como el control de roles sobre los aplicativos misionales funciona bien, sin embargo, se sugiere continuar los planes de acción y sus seguimientos concretos, que se encuentran en ejecución para prevenir el riesgo de seguridad digital con los tiempos establecidos dentro de las matrices que se suministran y que aplican a toda la entidad.

Se identificaron los controles que cumplen y reconocen el esfuerzo y la gestión a la OS, por lo que la OCI recomienda continuar con el tratamiento de los riesgos planteados debido a que estos podrían generar vulnerabilidades en la seguridad de la información. Muchos de los requerimientos de seguridad establecidos son adoptados al interior de la OS y en cada uno de los procesos, y algunos han sido implementados de acuerdo a la necesidad de fortalecer la seguridad de la información.

La auditoría resalta la importancia de continuar con la adopción de los parámetros y requerimientos establecidos en el nuevo marco contable NMNC y los requerimientos establecidos en la norma vigente y de buenas prácticas, así como lo establecido en las guías vigentes del MINTIC con el fin de mejorar la implementación del plan de gestión de seguridad digital en la entidad, y seguir con la optimización de las capacitaciones técnicas con transferencia de conocimiento principalmente en cabeza del personal de planta. Con base en las observaciones desarrolladas en el informe y las conclusiones presentadas, la Oficina de Control Interno recomienda:

- Formalizar y ejecutar el plan de gestión de riesgos de seguridad digital 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 de seguridad digital que no se han actualizado por cada proceso y la criticidad actualizando la matriz de riesgos de seguridad digital.
- Frente a las actividades desarrollados o nuevas funcionalidades en los aplicativos misionales continuar con las diferentes actividades que se han establecido entre las diferentes subdirecciones y la OS en la implementación oportuna de los mismos desarrollos.
- Seguimiento a las nuevas funcionalidades implementadas durante lo corrido de la presente vigencia corroborando su respectivo funcionamiento, y las pendientes de implementar.
- Seguir en constante monitoreo del cumplimiento de la normatividad vigente y las buenas prácticas en la gestión de riesgos de seguridad de la información, así como lo emitido por el MINTIC con información amplia, detallada y concisa, adicionando las respectivas evidencias y soportes.

NOTA: Las observaciones y recomendaciones presentadas por la OCI en sus informes tienen como fin último generar valor para el DADEP, 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: Lady Yadira Escamilla Triana, Subdirectora de Registro Inmobiliario
Diana María Camargo Pulido, Jefe Oficina Asesora de Planeación
Syrus Pacheco, Jefe Oficina de Sistemas

Proyectó: Fernando Andrés Salgado Tovar.
Fecha: 10-09-2021