Radicado DADEP No. 20161301091753

Bogotá D.C, 26-08-2016

MEMORANDO

PARA: **NADIME YAVER LICHT**
Directora

DE: **WILLIAM VALDERRAMA GUTIERREZ**
Jefe Oficina de Control Interno

ASUNTO: Informe final seguimiento SIDEP.

La Oficina de Control Interno en cumplimiento de su rol de evaluación y seguimiento y en ejercicio de sus funciones en especial las establecidas en la Ley 87 de 1993 y teniendo en consideración lo dispuesto en los artículos 1°,2°, 3°, 4° y 12 de la misma norma y la 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, realizó un seguimiento al informe emitido por esta oficina en la vigencia 2015 en referencia a la seguridad e integridad de datos del sistema SIDEP versión 2.0.
Con base en lo anterior, a continuación se presentan los siguientes puntos:

I. OBJETIVO Y ALCANCE:

El seguimiento tuvo como objetivo principal, el grado de cubrimiento y atención de las observaciones emitidas en el informe de 2015 por la Oficina de Control Interno respecto a SIDEP.

La revisión se enfocó de la nueva versión del sistema SIDEP 2.0 el cual entró en producción en el mes de febrero de 2016 y el trabajo de campo se realizó principalmente con la Oficina de Sistemas.

II. METODOLOGIA

Para el desarrollo del seguimiento, se solicitó a la Subdirección de Registro Inmobiliario la asignación de un funcionario responsable el cual se puso en disposición inmediata ante la Oficina de Control Interno. Paralelamente y como el trabajo de seguimiento se enfocó en su mayoría con la Oficina de Sistemas, se estableció contacto con el ingeniero responsable del soporte y administración del sistema con el cual se realizaron las validaciones respectivas.

Las evidencias se tomaron por medio de muestreo, a las cuales se aplicaron procedimientos de auditoria tales como consulta, análisis de datos, observación, inspección y confirmación.

III. ASPECTOS POSITIVOS Y FORTALEZAS

En los siguientes ítems, se exponen los temas positivos producto de la labor del seguimiento:

- La autenticación de los usuarios ante SIDEP 2.0 se realiza por medio del servidor de dominio de la entidad, permitiendo un único punto de control para parametrización de reglas de acuerdo a las mejores prácticas de seguridad. Actualmente los password de los usuarios presentan un buen nivel de seguridad.

- Las cuentas de usuarios del sistema se encuentran debidamente matriculadas y asociadas a funcionarios de manera exclusiva, también se menciona que no se están usando usuarios genéricos y que un usuario no tiene más de una cuenta asociada.

- Se ha generado y actualizado documentos relacionados con el sistema de acuerdo a las recomendaciones dadas, los cuales permiten una óptima administración y soporte del sistema.

- La información contenida en las tablas de auditoria es consistente la cual permite realizar trazabilidad.

IV. OBSERVACIONES

A continuación presentamos las observaciones derivadas del seguimiento:

1. **Seguridad de password para autenticación:**

Se valida el sistema SIDEP en su versión 2.0, y con respecto a esta observación se menciona lo siguiente:
Aspectos mejorados:

- El proceso general de identificación y autenticación ante el sistema SIDEP 2.0, se hace en sincronía con el servidor de directorio activo (LDAP), por tanto todas las políticas y reglas aplicadas a nivel de este servidor, se replican sobre SIDEP, permitiendo tener centralizado el control de los usuarios del sistema.

- Dentro de Las características parametrizadas actualmente para los password son: longitud mínima 8 caracteres, exigencia minino de una mayúscula, minúscula y números, histórico de 3 contraseñas para base de datos y caducidad de password a 30 días también para la base de datos.
-
- El tiempo de inactividad en el sistema esta parametrizado en 30 minutos.

Aspectos que presentan observación:

- Para algunos usuarios del sistema, el password no caduca, permitiendo el uso de la misma contraseña durante todo el tiempo activo en el sistema. Respecto a este tema se menciona que el password en el directorio activo de la entidad no está parametrizado para vencimiento permitiendo un uso prolongado de tiempo; lo mencionado replica sobre SIDEP ya que su proceso de identificación y autenticación se hereda del servidor de directorio activo.

- SIDEP no bloquea el inicio de sesión después de varios intentos fallidos de acceso.

- No se tiene parametrizado el histórico de contraseñas para SIDEP 2.0, únicamente se cuenta con el histórico para la base de datos.

2. Administración de usuarios del sistema:

Aspectos mejorados:

- Para un mejor control y administración de los usuarios matriculados en el sistema, la Oficina de Sistemas generó la matriz de roles y perfiles en SIDEP, la cual contiene los privilegios y permisos que se deben otorgar de acuerdo a la función que vaya a desarrollar un nuevo usuario.

- Usuarios genéricos: No se evidencian usuarios genéricos dentro del listado del sistema SIDEP 2.0.

- Funcionarios con 2 cuentas: No se evidencian funcionarios con 2 o más cuentas de acceso asociadas.

Aspectos que presentan observación:

a) Usuarios activos en el sistema sin contrato vigente: Respecto a este tema, en 2015 se menciona que... *Se valida el tema de administración de usuarios del sistema y basado en la entrevista realizada con el Administrador, se observa que no se están recibiendo por parte del área de gestión humana las novedades de personal tales como periodos de vacaciones y licencias, lo anterior permite que los usuarios queden activos en el sistema en periodos de ausencia.*

Como respuesta por parte del área se comenta que... "Al respecto se informa que se crearán acuerdos con los jefes de las diferentes áreas para que mediante notificación escrita, informen de manera anticipada a la oficina de Sistemas, sobre las vacaciones o suspensión de contratos de los servidores públicos a su cargo, para realizar la correspondiente inactivación temporal o definitiva según sea el caso de los usuarios".

Como resultado del seguimiento se evidencia que los siguientes usuarios en SIDEP 2.0 continúan activos sin contrato vigente o en proceso de renovación en la entidad:

hblanco	Helbert Arbey Blanco Valencia	OFICINA DE SISTEMAS
jalvarez	Jessica Paola Álvarez Miranda	OFICINA DE SISTEMAS

b) Usuarios con tiempo mayor a 2 meses sin ingresar al sistema: en el informe de 2015 se manifestó en la observación que: "Se evidencian usuarios activos en el *sistema con más de 6 meses sin ingresar al aplicativo, incluso hay usuarios que su ultimo acceso fue en los años 2011, 2012 y 2013.*"

Como respuesta al punto, el área responsable comenta. "Se comunica que una vez entre en funcionamiento SIDEP 2.0, el usuario tendrá la misma configuración que se maneja actualmente en el LDAP".

Para el seguimiento realizado se presenta lo siguiente:

Se evidencian 36 registros de usuarios en estado activo con tiempo mayor a un mes y medio sin ingresar al sistema, lo que quiere decir que los usuarios no se están inactivando por tiempo considerable sin uso. Complementariamente, se menciona que dentro de la base de datos de usuarios de SIDEP, el dato de último acceso al sistema para los usuario se comenzó a registrar posterior al día 17 de junio de 2016, es por eso que para algunos usuarios ese dato se encuentra en blanco implicando que su ultimo acceso fue anterior a la fecha mencionada o que nunca han ingresado al sistema.

A continuación se presentan los siguientes ejemplos:

USUARIO	NOMBRE_USUARIO	ULTIMO_ACCESO	ACTIVO
aalbarracin	Andrea Yasmin Albarracín Reina	Este dato se encuentra en blanco	SI
aruiz	Amalia Ruiz González		SI
cchinchilla	Carolina Chinchilla Torres		SI
cgalvis	Claudia Galvis Sánchez		SI
cpoveda	Claudia Jannethe Poveda Fandiño		SI
dgarcia	Daniel García Jiménez		SI
dvalencia	Diana Milena Valencia Montealegre		SI
emarciales	Elizabeth Marciales Daza		SI
gavila	Guillermo Enrique Ávila Barragán		SI
ghernandez	German Alberto Hernández Prieto		SI
gherrera	Giovanni Herrera Carrascal		SI

c) En el año 2015 se presentó en el informe la siguiente observación con relación a los formatos FUS donde se solicita, autoriza y aprueban los accesos a los sistemas de la entidad: .."Formato Único

de sistemas para SIDEP: revisando el tema de autorización para el sistema, se observa la inexistencia de formatos FUS para los siguientes funcionarios:

Alexis Adriam Vargas. Avargas
Mónica C Romero. Mromero"

Y como respuesta por parte del área auditada se menciona que..."Es importante informar que los FUS sí se recibieron junto con la solicitud de creación de usuarios al correo electrónico de mesa de ayuda, pero no se encontraban dentro del repositorio creado para facilitar la búsqueda de los formatos. En este momento el repositorio se encuentra actualizado."

Derivado del seguimiento realizado, para los siguientes usuarios de SIDEP 2.0, no se evidencia el correspondiente formato FUS que soporta la autorización de acceso al sistema:

- Sandra Carolina López Viveros.
- Fabián Steven Peñaloza Rivera.
- Jimmy Alexander Parra Barrera.
- Alexander Javier Rodríguez Alarcón.
- Helbert Arbey Blanco Valencia.
- Lina Fernanda Quenguan.

Finalmente, para este tema se menciona que no fue creado un plan de mejoramiento en CPM.

C) Integridad de información:

Para el seguimiento realizado se toman las siguientes tablas como muestra de la base de datos de SIDEP 2.0, sobre las cuales se realiza revisión la consistencia e integridad de datos:

- Tabla inventario: Esta tabla presenta la mayor transaccionalidad en el sistema y en ella se registra todo el inventario del patrimonio inmobiliario distrital.
- Tabla Auditoria / Inventario: Contiene la auditoria de la tabla inventario.
- Tabla usuario: contiene todos los usuarios matriculados en el sistema
- Tabla Auditoria / usuario: Contiene la auditoria de la tabla usuarios.
- Tabla Log_Login: contiene las fechas de acceso de los usuarios en el sistema.

Como resultado se presenta lo siguiente:

Tabla inventario:

- Se observan 113 registros con el campo CODIGO_ARCHIVO en blanco, los restantes 88802 registros contienen información.

- Se identifican 28084 registros con el campo UBICACIÓN en blanco.

- El campo APROBO_DESINCORPORACION, ID_VIABILIDAD_ADMINISTRACION, USUARIO_VIABILIDAD, FECHA_VIABILIDAD, FECHA_VIABILIDAD se encuentra en blanco dentro de la base de datos.

- Se identifican 24391 registros con el campo ID_GEO en blanco.

Tabla Auditoria / Inventario: la información registrada en la tabla es consistente e integra.
Tabla usuarios: presenta información consistente en todos los campos revisados, no obstante es importante resaltar el completo diligenciamiento del campo número de documento.
Tabla Auditoria / usuario: contiene información consistente e integra para los campos revisados.
Tabla Log_login: la información registrada en los diferentes campos de la tabla es consistente y no presenta observaciones.

D) Control de cambios para el sistema SIDEP.

En el informe de 2015 se menciona por parte de la Oficina de Control Interno que..."No se tiene una documentación estructurada de los cambios realizados al sistema SIDEP; para tal fin en años anteriores se venía llevando una bitácora con los cambios realizados al sistema pero esta práctica se desmontó. Adicionalmente dentro de la guía de sistemas de información, se menciona que para cambios en los sistemas se debe usar el formato control de modificaciones actualizaciones en SIDEP, sin embargo no se evidencian los soportes documentales."

La respuesta emitida por el área fue:" En estos momentos no tenemos un registro detallado de todos los cambios realizados en SIDEP WEB. Se cuenta con copias de seguridad de todos los despliegues de la aplicación, que nos permite llevar un control sobre las modificaciones realizadas al sistema.

También se cuenta con las solicitudes de cambios realizadas por los usuarios para los Sistemas de Información, entre los cuales está el SIDEP. Dicha solicitud llega a través de la herramienta GLPI, acompañada del formato "Solicitud de Información, Restauración o Modificación a la Base de Datos", el cuál reemplazó al formato "control de modificaciones actualizaciones en SIDEP". Vamos a actualizar las guías de sistemas de información para que estén acorde a los procesos actuales de la oficina y más con ocasión de la próxima entrada en producción del SIDEP 2.0."

Como parte del seguimiento se evidencia que la guía de sistemas de información oficializada en el SGI de la Entidad tuvo actualizaciones en referencia al uso del formato control de modificación actualizaciones en SIDEP el cual fue removido de las actividades. Por otro lado la Oficina de sistemas viene trabajando en la implementación del formato para control de requerimientos sobre las aplicaciones y adicionalmente tiene contemplado la actualización de las guías y procedimientos publicados en el sistema integrado de gestión. Estas actividades mencionadas están relacionadas con procedimientos para controlar los cambios realizados a SIDEP, sin embargo se reitera la importancia

en la culminación de las actividades relacionadas con la estructuración del procedimiento que permita gestionar los cambios y/o modificaciones sobre el sistema. Finalmente se menciona que la Oficina de sistemas tiene creada oficialmente la acción Numero 100070 en el aplicativo CPM, la cual titula Revisión y actualización a la documentación del Proceso; dicha acción venció el día 30 de junio de 2016 y tiene el 50% en su grado de cumplimiento.

E) Plan de continuidad de las operaciones para SIDEP.

En el informe de 2015 se menciona que... "Para el sistema SIDEP, no se tiene actualizada ni oficializada la documentación del plan de continuidad de las operaciones, únicamente se tienen establecidas estrategias y/o actividades tales como copia de seguridad de base de datos y pruebas de restauración de datos, también se cuenta con una base de datos instalada en otro servidor y finalmente se menciona que se realiza el resguardo de copia de información en el Archivo Distrital. Se resalta para este tema que la copia del aplicativo SIDEP (objetos) como actividad de respaldo, no se ha remitido al archivo distrital en 2015.

Adicionalmente, con la infraestructura que se tiene actualmente implementada para el sistema, no se puede garantizar completamente la disponibilidad de la información, debido a que no se cuenta con una redundancia tecnológica externa para atender eventualidades que afecten el centro de cómputo principal de la Entidad".

Como respuesta por parte del auditado se obtuvo... "Para el documento del plan de continuidad, se realizará la respectiva actualización incluyendo las estrategias y actividades necesarias para la correcta restauración de los sistemas. Se realizará el respectivo envío de las copias de seguridad de los despliegues del SIDEP-WEB al archivo distrital.

Si bien es cierto que en este momento no contamos con un centro de cómputo externo, sí se puede revisar como poder lograr la continuidad de la entidad."

Basado en esto y como parte del seguimiento, se establece dentro de esta observación que existen lineamientos y actividades contemplados en la guía de seguridad del proceso de gestión de la información y la tecnológica en el SGI, así como también el documento preliminar de plan de contingencia el cual viene siendo trabajado por la Oficina de Sistemas conteniendo las estrategias de cómo proceder ante una eventualidad de manera general, no obstante, se informa que no se ha realizado la actualización ni documentación del mencionado plan.

Respecto al tema de continuidad de las operaciones en el ámbito tecnológico, no ha sido creado un plan de mejoramiento en CPM.

F) Logs de sistema:

En el informe de 2015 se menciona que..."A nivel de aplicación, no se evidencian logs de auditoría, sin embargo en la base de datos se cuenta con la tabla auditoría en la cual se registra la información de los eventos sobre la base de datos tales como inserción, actualización y eliminación; esto quiere decir que si se requiere una proceso de revisión es indispensable la participación del administrador de la base de datos para la extracción y análisis de la información."

La respuesta emitida por los auditados fue..."Para consultar la tabla de auditoria en SIDEP WEB se puede solicitar un reporte de la información allí contenida y así podrá ser analizada por un usuario sin la participación activa de Administrador de la base de datos. En SIDEP 2.0 se implementó un módulo de auditoria."

En el seguimiento se evidencia que para SIDEP 2.0 se creó una estructura de tablas de auditoria para cada una de las tablas transaccionales del sistema, dichas tablas registran información CONSISTENTE de cada registro tales como fecha de inicio y fin, usuario que realizó la acción, dirección IP, entre otros. Adicionalmente, para el sistema de implementó la administración de procesos por medio de trámites, quedando registrada toda la trazabilidad de las actividades realizadas en el sistema por parte de los usuarios. Basado en lo anterior se reporta como un notable aspecto positivo para SIDEP 2.0.

G) Documentación del sistema:

Administración de sistemas de información:
SIDEP cuenta con el manual de usuario, el cual contempla el tema de creación y asignación de roles como temas de administración, sin embargo no se evidencia que el manual contenga..."Indicaciones de parametrización del sistema de información a nivel de usuarios, roles y perfiles de acceso..." Tal y como lo estipula la guía de sistemas de información literal C del numeral 4.2.5.2."
Como respuesta el área contesta dentro del informe que..."No se cuenta con el detalle de las "Indicaciones de parametrización del sistema de información a nivel de usuarios, roles y perfiles de acceso". Se tendrá en cuenta la inclusión de esta información en la construcción del manual técnico de SIDEP 2.0."

Durante el proceso de seguimiento fue evidenciada el documento matriz de roles y perfiles de SIDEP, el cual fue construido entre la Subdirección de Registro Inmobiliario y la Oficina de Sistemas, dicha matriz contiene todos los permisos asignados a tramites y módulos cruzado contra cada rol existente en el sistema, por tanto y basado en esto, se da por cubierta esta observación.

V. Otras observaciones:

- La dirección o URL para conexión al sistema SIDEP 2.0 para internet actualmente es http://SIDEP.dadep.gov.co, evidenciando que no se utiliza el protocolo **HTTPS**, el cual permite la protección de las conexiones cada vez que se intercambie información con los usuarios sobre

todo en conexiones externas al sistema, ya que en caso de ser interceptada esta se encontraría cifrada.

- En el seguimiento se observa que en los puntos de los Supercades, los funcionarios continúan utilizando como fuente de información el SIDEP Web, por tanto y al no usar la versión 2.0 se presentan riesgos de entregar a la ciudadanía información desactualizada. De igual manera se establece con los funcionarios la falta de capacitación respectiva acerca del uso del sistema SIDEP 2.0. Complementariamente dentro la Entidad la versión WEB se está usando para todo el tema de defensa administrativa que corresponde a querellas, hechos notorios, restituciones voluntarias y talleres, así como también en administración se usa para contratos de apoyo y administraciones directas, no obstante esta última parte se encuentra desactualizada según revisión realizada por Sistemas.

VI. RECOMENDACIONES GENERALES.

- Complementar las reglas de seguridad para los usuarios y su proceso de autenticación en SIDEP tales como caducidad de password por tiempo prolongado sin acceso al sistema, bloqueo de cuenta por intentos fallidos de login e histórico de contraseñas.
- Fortalecer el procedimiento para inactivación de usuarios que se han retirado de la entidad o han finalizado su contrato. De igual manera realizar un control estricto sobre los formatos FUS donde se registran los permisos para el acceso al sistema. Complementariamente, contar dentro de los formatos FUS con la aprobación del dueño de la información para cuando se otorgan permisos de acceso en SIDEP.
- Validar las inconsistencias reportadas en referencia a integridad de datos y realizar las respectivas correcciones.
- Generar, formalizar, publicar y socializar el procedimiento con el cual se controlen los cambios en la plataforma tecnológica. aplicando a todo el ámbito tecnológico de la Entidad.
- Generar la documentación relacionada con el plan de continuidad de las operaciones de la Entidad y dentro de esta especificar las actividades relacionadas con los diferentes sistemas de información.
- Validar la adquisición de un certificado de seguridad ante un ente o autoridad de certificación debidamente registrada, lo que permite dar un mayor fortalecimiento al sistema SIDEP en el tema de seguridad.
- Capacitar y conectar a los funcionarios de los Supercades con SIDEP 2.0.
- Generar y formalizar los planes de mejoramiento necesarios, sobre todo para los casos reiterativos, analizando la causa raíz y estableciendo estrategias y actividades que eviten nuevamente la presentación de las observaciones.

VII. RIESGOS

De acuerdo el seguimiento, los riesgos presentados son los siguientes:

- Interceptación de datos.
- Falta de integridad de la información - inconsistencia de datos.
- Cambios no autorizados al sistema.

VIII. CONCLUSION

Como resultado del seguimiento realizado por esta Oficina, como aspecto general se menciona la gestión realizada por la Entidad con la implementación de la nueva versión de SIDEP con la cual se abordaron y se cubrieron temas expresados en el informe de 2015 disminuyendo los riesgos expresados en su momento.

Fue observado un mayor grado de integridad y consistencia de la información registrada en la base de datos del sistema, lo cual redunda en la confiabilidad y el buen servicio que como Entidad se da a la ciudadanía. También se presenta un parte de tranquilidad respecto al control que se tiene sobre los usuarios del sistema, principalmente en los temas de administración, así como también el fortalecimiento de las contraseñas lo cual se consideró en el informe anterior el tema más crítico para atender.

Finalmente, se expresa la importancia en desarrollar actividades en pro de la operación del sistema en general y también crear los planes de mejoramiento necesarios para atender los temas expuestos.
Cordial Saludo,

WILLIAM VALDERRAMA GUTIERREZ
Jefe Oficina de Control Interno

Con Copia: Hugo Roberto Hernández Díaz

Proyectó: Diego Alexander Urazán Franco
Fecha: agosto de 2016
Revisó: William Valderrama Gutiérrez
Aprobó: William Valderrama Gutiérrez