ALCALDÍA MAYOR
DE BOGOTÁ D.C.
GOBIERNO SEGURIDAD Y CONVIVENCIA
Departamento Administrativo de la
Defensoría del Espacio Público

130-0CI

MEMORANDO

AL CONTESTAR CITE EST 20151E1487
Fol:6 Anex:0 Tipo doc:MEMORANDO
DEFENSORIA ESPACIO PUBLICO 11-09-2015 02:20:33
ORIGEN : SD:48 - OADI /VALDERRAMA GUTIERREZ WILLIAM
DESTINO: DESP /JIMENEZ GONZALEZ NELSON YOVANY
ASUNTO: INFORME FINAL DEL PROCESO DE EVALUACION EN REFE
OBS : DIEGO URAZAN FRANCO

PARA: **NELSON YOVANY JIMENEZ GONZALEZ**
Director

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

Asunto: **Informe Final del proceso de evaluación en referencia a seguridad e integridad de datos del sistema SUMA.**

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, también de la Directiva de la Alcaldía Mayor N 005 de 2005 respecto a las políticas generales de Tecnología de información y comunicaciones aplicables a las Entidades del Distrito Capital y la Resolución 305 de 2008 Por la cual se expiden políticas publicas 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 una evaluación respecto a la seguridad e integridad de datos del sistema SUMA. Con base en lo anterior, a continuación se presentan los resultados con las siguientes iteraciones:

I. OBJETIVO Y ALCANCE:

La evaluación tuvo como objetivo principal, la validación de la seguridad de la información, así como también la integridad de los datos registrados en el sistema SUMA

La revisión se enfocó de manera primordial en el sistema SUMA en sus ambientes de producción y pruebas, específicamente temas como la administración del sistema y la revisión de la información registrada en la base de datos. Adicionalmente, el trabajo de campo se realizó con la Subdirección de Administración Inmobiliaria y la Oficina de Sistemas

130-OCI

II. METODOLOGIA

Para el desarrollo de la evaluación, se realizó un requerimiento de información a la Subdirección de Administración Inmobiliaria y a la Oficina de Sistemas el cual fue respondido en óptimas condiciones de calidad y tiempo; las fuentes de información remitidas a esta Oficina en general fueron:

- Documentación del sistema.
- Manuales de Administrador y de usuario del sistema.
- Listado de usuarios registrados en el sistema.
- Listado de personal administrador del sistema.

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

III. ASPECTOS POSITIVOS Y FORTALEZAS

Ejecutada la labor de auditoría, a continuación se expresan los siguientes aspectos, los cuales permiten determinar la gestión y el trabajo realizado por la Entidad en pro del avance del sistema, así como también permitieron ser factores críticos de éxito para la evaluación:

- El sistema cuenta con documentación clara, concisa, organizada y administrada por parte de la Subdirección de Administración Inmobiliaria.
- Se evidencia la utilización de software libre, alienándose con las políticas Distritales en referencia al uso de este tipo de software en las Entidades.
- Para el sistema se cuenta con personal idóneo y calificado para el desarrollo, administración y soporte del mismo.
- El sistema SUMA opera actualmente sobre una plataforma tecnológica adecuada permitiendo realizar actividades vitales tales como operación diaria, copia de seguridad, continuidad de las operaciones, restauración a punto anterior y pruebas ya que cuenta con sus respectivos ambientes separados de producción y pruebas.
- Se cuenta con un portal denominado Liferay que permite la administración de los usuarios y de la seguridad por medio de una interfaz amigable y parametrizable.
- Los usuarios del sistema con privilegios se tienen debidamente controlados sin evidenciar usuarios genéricos o duplicados.

130-0CI

- SUMA cuenta con la bitácora sobre la cual se están registrando cambios importantes en la base de datos del sistema, dicha funcionalidad permite realizar trazabilidad sobre acciones ejecutadas.
- Para la carga de datos al sistema, este realiza validaciones tales como listas desplegables y campos calendario para evitar el registro erróneo de información. Adicionalmente al momento de presentar un error de registro, por medio de los mensajes de error, el sistema guía claramente al usuario acerca de las correcciones que deba realizar.
- Las áreas auditadas respondieron con claridad los cuestionamientos, permitieron el agendamiento eficaz de las citas para el desarrollo del trabajo de campo y los requerimientos de información fueron respondidos por los canales definidos con prontitud.

IV. HALLAZGOS Y RECOMENDACIONES

A continuación presentamos los hallazgos derivados del trabajo de auditoría que requieren una intervención por parte de las áreas auditadas por medio de un plan de mejoramiento:

1. Cálculo de la fórmula de retribución:

Se revisan en los registros de la base de datos del sistema SUMA el cálculo del valor total a cancelar por parte de un aprovechador, evidenciando que para 2 registros de solicitud con tiempo mayor a 1 día, se genera una diferencia en el valor al cruzarlo contra el simulador de la fórmula así:

ID de solicitud	Fecha de ocupación inicial	Fecha de ocupación final	Días calculados y aplicados por el sistema	Valor de Administrador + Gestor	Valor Simulador (Excel SAI)	Diferencia
6	03/12/2014	03/12/2014	5	11.380.739,32	17.189.141	-5.808.401
8	14/03/2015	14/03/2015	2	42.396.962,49	52.249.921	-9.852.958

De acuerdo con la anterior tabla, también se evidencia que los días aplicados por el sistema para el cálculo en los registros expuestos son 5 y 2 respectivamente y según los campos fecha de ocupación inicial y fecha de ocupación final el resultado es 1 día.

130-0CI

Recomendaciones:

- Realizar una revisión detallada del cálculo de la fórmula de retribución en el sistema, realizando los ajustes necesarios y teniendo en cuenta los diferentes escenarios que se pueden presentar, validando que el resultado para todos los casos sea el esperado.

- Establecer por parte del área responsable un monitoreo y revisión periódica del cálculo de la fórmula de retribución basado en casos de usos y emitiendo la respectiva documentación de los resultados.

Respuesta del área auditada:

Una vez revisada la observación por parte de la auditoría, se encuentra que el cálculo de la fórmula de retribución en el sistema se está realizando correctamente. Sin embargo, el inconveniente que se registró no se encuentra a nivel de la aplicación de la fórmula, si no del guardado de los cálculos en la base de datos. Al momento de realizar las simulaciones los valores arrojados son correctos, pero al momento de hacer el guardado de estos correspondientes a solicitudes por periodos mayores a 1 día se estaba guardando el factor correspondiente a la temporada únicamente para el último día del evento y no para todos los días seleccionados, lo que generaba una diferencia en el valor.
Es necesario aclarar, que los dos registros mencionados corresponden a solicitudes que nunca fueron completadas y por lo tanto no se llegó a expedir recibos de pago o generar un cobro con los valores anteriormente señalados.
De igual manera, una vez la inconsistencia fue detectada y analizado, se levantó la incidencia correspondiente y se procedió a realizar la corrección necesaria en el código de inmediato, debido a que se consideró un requerimiento de importancia alta para el sistema, por lo tanto consideramos este punto NO requiere acción de mejora.

2. **Implementación de protocolo HTTPS para SUMA:**

La dirección o URL del sistema SUMA para internet actualmente es HTTP://suma.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, ya que en caso de ser interceptada esta se encontraría cifrada. Como aspecto de mitigación, la plataforma Liferay realiza un cifrado a nivel del cliente y solamente puede ser descifrada al momento de llegar al servidor; esto aplica para los campos críticos de la base de datos como usuario y contraseña.

130-0CI

Recomendaciones:

- Realizar un análisis costo beneficio en conjunto con la Oficina de Sistemas para atender este aspecto de seguridad, lo que permite dar un mayor fortalecimiento al sistema SUMA en el tema de seguridad.

- En coordinación con la Oficina de Sistemas, validar la adquisición de un certificado de seguridad ante un ente o autoridad de certificación debidamente registrado.

- Instalar, configurar, implementar, probar y monitorear el servidor de SUMA después de la instalación del certificado, posteriormente realizar la documentación del proceso.

Respuesta del área auditada:

En el marco de las competencias del equipo de desarrollo, se han adoptado las medidas de seguridad de la información disponibles a través de herramientas diferentes al protocolo HTTPS, con lo cual se evidencia que efectivamente se está aplicando un esquema de protección de las conexiones durante el intercambio de información.

Se evaluará en coordinación con la Oficina de Sistemas y con la Dirección, las diferentes alternativas de seguridad de acuerdo a las mejores prácticas de la industria y a la disponibilidad de recursos de la entidad para adoptar la alternativa que mejor se adecúe a las necesidades del SUMA.

3. Administración de usuarios del sistema:

En referencia a los usuarios del sistema se presentan los siguientes aspectos:

- Para la creación de usuarios en el sistema SUMA (administradores, entidades gestoras, entidades administradoras y demás usuarios a diferencia de las personas naturales y jurídicas) no se tiene definido un lineamiento que estipule las actividades y los registros documentales que soporten la actividad. Cabe resaltar que en el SIG, dentro del documento Directrices para el manejo de Tics se define que los usuarios de aplicaciones deben ser solicitados a través del formato FUS.

130-0CI

- No se tiene definida una estructura para nomenclatura de los ID de usuarios del sistema. De acuerdo con la validación realizada con la administradora del aplicativo, la estructura que se está usando para usuarios con rol administrador, entidad administradora, entidad gestora y otros usuarios, consiste en la primera letra del nombre seguido del apellido y según lo evidenciado para los ID **karenbernal** y **audientidads** no se aplicó dicha práctica.

- Para usuarios matriculados en Entidades gestoras y Entidades Administradoras, de acuerdo con la vista del aplicativo, no se tienen diligenciado el campo apellido, únicamente se está registrando la información en el campo nombre. A manera de ejemplo se citan los siguientes casos:

    - Usuario MCAMADO: nombre mcamado, apellido (sin datos).
    - Usuario AMURILLO: nombre amurillo, apellido (sin datos).
    - Usuario ASVENEGAS: nombre asvenegas apellido (sin datos).

Recomendaciones:

- Definir un procedimiento estructurado para el tema de administración de usuarios del sistema SUMA incluyendo temas tales como nomenclatura de ID, asignaciones y /o cambios de claves, inactivaciones, autorización y aprobación de creación, soporte documental, entre otros.

- Validar los procedimientos formalizados en el SIG de la Entidad y realizar los que aplique incluir y ejecutar las actividades establecidas y controles definidos del lineamiento para el sistema SUMA.

- Validar los campos que tengan información sin diligenciar y registrar la información correspondiente con el fin de tener integridad de datos.

<u>Respuesta del área auditada:</u>

Se dará aplicación del formato FUS a través de la Mesa de Ayuda del DADEP, para las entidades tanto gestoras como administradoras que necesiten creación de usuario en el sistema SUMA.
Para los temas de nomenclatura de los nombres de usuario y diligenciamiento del campo apellido de los usuarios, se realizarán los ajustes y recomendaciones que se consideren pertinentes. Es importante aclarar, que la aplicación de nomenclatura en los casos señalados se realizó a los nombres de usuario más no al ID.

4. **Control de cambios para el sistema SUMA.**

No se tiene definido un procedimiento documentado para control de cambios para el sistema SUMA; se informa que a pesar de la no existencia del mencionado procedimiento, actualmente se vienen realizando actividades de control al momento de realizar actualizaciones o nuevos desarrollos para el sistema tales como el almacenamiento de archivos planos con cada una de las sentencias SQL ejecutadas, también, se realiza la actualización de la información en el diccionario de datos el cual hace parte de la documentación del sistema y finalmente para controlar el código fuente del sistema se cuenta con la herramienta Subversion (libre), donde se van controlando el versionamiento del sistema.

Recomendaciones:

- En coordinación con la Oficina de Sistemas, generar un procedimiento con sus respectivos soportes documentales, con el cual se puedan controlar los cambios realizados a los sistemas a nivel de hardware y software de manera estricta, siendo lo más genérico posible y que de paso apunte a cambios de la plataforma tecnológica de la Entidad.

- Después de emitido el proceso, realizar un monitoreo periódico del cumplimiento de lo establecido por parte del área responsable.

Respuesta del área auditada:

El control de cambios en el SUMA se realiza con los soportes y aprobaciones de las actas de reuniones de la Comisión Intersectorial, reuniones de equipo y aprobaciones del líder funcional dependiendo de las características de los requerimientos y se encuentran debidamente soportados con las evidencias de aprobación como las copias del versionamiento del sistema. Sin embargo y siguiendo las recomendaciones de la auditoría, se determinará con la Oficina de Sistemas la definición de un procedimiento oficial documentado para registrar el control de cambios de los sistemas de información.

5. **Documentación del sistema**

Se realizó revisión de la documentación del sistema SUMA y comparándola contra el Documento Guía de sistemas de información perteneciente al procedimiento sistemas de información del proceso Gestión de la Información y la Tecnología, se determina que en

130-0CI
el numeral 4.2.5.2 de la guía se definen los tipos de documentación de un sistema de información y para el sistema SUMA se presentan las siguientes situaciones:

- Documento de instalación: dentro del documento "manual de administración y soporte" en el ítem de recomendaciones y sugerencias, se define "*seguir paso a paso el proceso de instalación tal como se describe en los manuales para que no se produzcan resultados inesperados* " sin embargo no se evidencia la existencia del mencionado manual.

- Administración de sistemas de información: para este aspecto se cuenta con el manual de administración y soporte el cual contiene la definición del sistema, la guía de uso, así como también las recomendaciones y sugerencias, sin embargo no se evidencian temas de administración tales como parámetros de configuración del sistema, roles y perfiles de acceso; Adicional, se menciona que no se tienen contemplados dentro del manual aspectos tales como; información sobre los comandos de software, mensajes de error y resolución de problemas y glosario.

- Mantenimiento y soporte del sistema: No se evidencia la existencia de dicho documento.

Recomendación:

- Realizar una mesa de trabajo en conjunto con las Oficinas [illegible] y Planeación, para revisar los procedimientos existentes en el sistema [illegible] de gestión y de ser necesarios actualizarlos, con eso, para el caso de [illegible] realizar un barrido de los lineamientos, actividades y soportes documentados con el fin de que exista alienación entre las actividades que se desarrollan en el sistema SUMA y el SIG de la Entidad.

Respuesta del área auditada:

La guía de administración y soporte del sistema SUMA contiene la definición del sistema, su objetivo, la descripción de la plataforma base, la descripción de software del servidor, la guía de uso y recomendaciones y sugerencias. Se verificará y ajustará los contenidos de la guía del sistema SUMA a los definidos en la Guía de Sistemas de Información de considerarse necesario.

130-0CI

RIESGOS

Basado en los hallazgos expuestos en este informe, se presentan los siguientes riesgos:

- Perdidas económicas debido a los cálculos erróneos de la fórmula de retribución.
- Interceptación de información por parte de un intruso.
- Falta de información de trazabilidad en un proceso investigativo.
- Falta de integridad de la información.
- Cambios no autorizados al sistema.
- Generación de inconformidades en auditorias de calidad por el incumplimiento de los lineamientos del sistema integrado de Gestión.

V. OBSERVACIONES

A continuación se exponen observaciones derivadas del trabajo de auditoria, las cuales se consideran de carácter importante pero que no implican un riesgo para las operaciones, mas sin embargo son mencionadas para su conocimiento:

- SUMA cuenta con el portal Liferay sobre el cual se parametriza y administran los usuarios y la seguridad del sistema y al validar aleatoriamente las características de seguridad que se tienen definidas actualmente, a continuación se menciona lo siguiente:

    - La longitud mínima exigida por el sistema para autenticación son 6 caracteres.
    - Como exigencia de uso de caracteres el sistema solicita que se parametrice mínimo un número y una mayúscula. No se está exigiendo el uso de caracteres especiales.
    - El número de intentos fallidos de autenticación parametrizados son 40.
    - No se tiene activa la opción de historial de contraseñas.
    - El sistema no tiene activada la opción de expiración de password.
    - El sistema tiene parametrizado un time out para conexión de 30 minutos. Este parámetro se actualizó a 15 minutos durante el desarrollo de la auditoria.

- El sistema SUMA cuenta con un log denominado bitácora, la cual registra las acciones de eliminación, inserción y actualización que se hacen sobre la base de datos del sistema por parte de los usuarios, no obstante, y de acuerdo con los controles propuestos por la Norma ISO 27002 en su objetivo número 12.4, los

130-0CI

cuales describen que ..."Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información" y adicionalmente, ..."se deben registrar, las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular..". basado en esto, se manifiesta que en la bitácora, [illegible] sistema se registran información de toda la actividad del usuario [illegible] fallidos de acciones entre otros que apunten a lo mencionado en [illegible]

- Se toma una muestra de tablas de la base de datos (personas, representantes legales, personas jurídicas, entidades, solicitudes, bloqueos, usuarios de sistema, usuarios Liferay y predios) y se [illegible] de datos para cada uno de los campos y como producto [illegible] menciona lo siguiente:

  - Las tablas personas jurídicas, entidades, solicitudes, bitácoras, bloqueos, usuarios, usuarios de liferay y predios contienen campos relacionados con la dirección IP de conexión, sin embargo las direcciones IP que se visualizan en general son cuatro, 127.0.0.1, 172.25.155, 172.25.5.174, 172.25.5.4. Todas estas apuntan a equipos propios de la Entidad (servidores, proxy y equipo de la administradora); lo anterior indica que no se está registrando la IP para conexiones externas.

  - El campo celular en la tabla entidades cuenta con datos genéricos y repetidos (123456789), los cuales fueron cargados al inicio [illegible] del sistema en la base de datos.

- Validando el tema de seguridad del sistema SUMA con el encargado de seguridad informática en la Entidad, se observa que las conexiones tipo FTP al servidor de SUMA (transmisión de archivos) a nivel interno estaba permitido [illegible] es importante cerrar los puertos en todo momento para [illegible] equipos dentro de la red y fuera de esta. Lo anterior se menciona porque [illegible] tipo de conexiones son usadas para transferir archivos de manera [illegible] no ofrece una seguridad idónea. Por otra parte se revisa la [illegible] del Firewall que actualmente protege la Entidad a nivel tecnológico y para temas de monitoreo, este no cuenta con un registro o log de las actividades realizadas por un usuario autorizado para establecer una conexión VPN a los servidores y equipos; para este tema según el encargado de Seguridad Informática, es

130-0C

realizar varias validaciones por consola, con esto obtener una ... más detallada.

...ON

El sistema cumple con condiciones de seguridad, ya que está configurado con parámetros que permiten el control de la información contenida y adicional el uso de buenas prácticas de desarrollo sumado a la experiencia de las comunidades para software libre que se encuentran en la red.

La información contenida en la base de datos del sistema es integra de manera general y se cuenta con buenos controles de validación al momento de la carga de información.

Como aspecto general, se comenta que el Sistema SUMA, dentro de la Entidad se controla y gestiona apropiadamente por parte de la Subdirección de Administración Inmobiliaria con el soporte y colaboración de la Oficina de Sistemas.

Sin embargo y de acuerdo con los hallazgos y observaciones expuestas y las respuesta dada por la línea auditada, que igualmente se encuentran plasmadas en el presente info... estudiar la necesidad de establecer acciones mejoramiento, ... subsanar las desviaciones y minimizar al máximo los riesgos ... lo que solicitamos nos informen sobre su decisión, a fin de que esta ... monitoreo y verificación correspondiente.

Cordial Saludo,

WILLIAM VALDERRAMA GUTIERREZ
Jefe Oficina de Control Interno

Elaboró: Diego Urazán Franco
Aprobó: William Valderrama Gutiérrez
Fecha: Agosto 5 de 2015

Código ...
...
...

Cra 30 ... No 15 ...
Tel ...
www ...
Info ...