Radicado DADEP No. 20171300001043

Bogotá D.C, 13-01-2017
130-OCI

MEMORANDO

PARA: **NADIME YAVER LICHT**
Directora

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

ASUNTO: **Informe seguimiento a riesgos e indicadores de tecnología.**

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, así como también lo establecido en el artículo 4 y 6 de la resolución 305 de 2008 de la Comisión Distrital de Sistemas y lo consagrado en la estrategia de Gobierno en Línea, realizó un seguimiento a los riesgos e indicadores relacionados con el ámbito tecnológico en la Entidad.

Con base en lo anterior, a continuación se presentan los siguientes ítems:

I. OBJETIVO Y ALCANCE:

La labor de auditoria tuvo como enfoque principal la validación y seguimiento de los riesgos e indicadores establecidos y relacionados con el ambiente tecnológico en la entidad y que son directamente administrados por la Oficina de Sistemas, así como también el grado de alineación y cumplimiento a lo establecido en las normas oficiales respecto al tema.

El alcance de la auditoria contempló los riesgos e indicadores pertenecientes al proceso de Gestión de la Información y la Tecnología, registrados en el mapa de riesgos y en el cuadro de mando de indicadores del SIG, los cuales son gestionados por la Oficina de Sistemas.

II. METODOLOGIA

El ejercicio de auditoria se realizó por medio del análisis de la información publicada en la página web e intranet de la Entidad, así como también se hizo validación con el personal de la Oficina de sistemas encargado de los temas estratégicos.

III. ASPECTOS POSITIVOS Y FORTALEZAS

A continuación se presentan los temas positivos conceptuados en la auditoria:

- El tablero de indicadores y el mapa de riesgos se encuentran actualmente publicados en la página web de la Entidad dentro del botón de transparencia, con fecha de última actualización septiembre de 2016.
- Durante la presente vigencia, la Oficina de Sistemas ha realizado reuniones internamente donde se han tratado los temas de riesgos e indicadores, redundando en la actualización de la información contenida en los documentos oficiales del SIG, para tal fin y como ejemplo se mencionan los indicadores que durante el primer semestre de 2016, se presentaba un único indicador y como resultado de la revisión se eliminó el existente y se adicionaron dos nuevos para su correspondiente proceso de medición y gestión.
- En el 2016 se ejecutaron diferentes estrategias y acciones con el fin de minimizar los riesgos por parte de la Oficina de sistemas; esta información se reportó en el seguimiento realizado en el segundo semestre del año.

IV. OBSERVACIONES Y RECOMENDACIONES

En los siguientes numerales, presentamos las observaciones producto del seguimiento:

a) RIESGOS:

1. Riesgos no incluidos en el mapa:

A nivel tecnológico, los siguientes riesgos, entre otros no se tienen contemplados dentro del mapa de riesgos asociados al proceso de gestión de la información y la tecnología, los cuales han sido presentando en los diferentes informes de las auditorías así:

- Suplantación de personas en los sistemas de información.
- Accesos no autorizados al sistema.
- Indisponibilidad de la plataforma tecnológica.
- Cambios no autorizados a un sistema de información
- Infección de equipos con virus.
- Robo de equipos
- Sanciones por incumplimientos normativos.

2. Eventos a nivel de tecnología que no se tienen tratados dentro del mapa de riesgos:

En la entidad se han presentado eventos o situaciones atípicas relacionadas con el ámbito tecnológico y sobre los cuales no se ha hecho un análisis estratégico para ser incluidos dentro del mapa de riesgos; a continuación se relacionan algunos eventos presentados:

- Ataques informáticos tanto a la intranet como a la página web.
- Represamiento de los tickets de servicio respecto a desarrollo en SIDEP 2.0.
- Suspensión del fluido eléctrico.

3. Riesgo sin controles en materia de Tic´s asociados:

Dentro del mapa de riesgos publicado en el sistema integrado de gestión de la entidad y específicamente en el proceso de gestión de la información y la tecnología, no se tienen controles definidos en materia de informática que atiendan o mitiguen el riesgo denominado..."Incumplimiento de las disposiciones legales en relación con la Gestión documental y la normatividad asociada a las TIC´s"...; únicamente se tienen contemplados controles asociados al tema de gestión documental.

4. Controles de tecnología:

Con respecto a los controles asociados a los riesgos del ámbito tecnológico, a continuación se presentan las siguientes situaciones:

4.1. Controles establecidos a nivel operativo que no están registrados en el mapa de riesgos: La siguiente lista de controles a manera de ejemplo se presentan como aspectos, acciones, actividades o mejoras que ha implementado la oficina de sistemas pero que no se tienen registrados en el mapa de riesgos como controles asociados a los riesgos:

- Bloqueo de puertos USB para evitar copia de información.
- Restricciones para instalación de programas en los equipos de cómputo.
- Control de navegación de internet por medio del servidor proxy.
- Controles ambientales y perimetrales en el centro de cómputo.
- Protección ofrecida por las UPS.
- Logs de auditoria.
- Firewall.
- Uso de FUS para el acceso de los funcionarios a los servicios tecnológicos.
- Segmentación de la red corporativa.
- Identificación y autenticación en los sistemas de información

4.2. Controles definidos dentro del mapa de riesgos sin estar operando: Se tiene definido un control el cual no se encuentra implementado dentro de la entidad; como ejemplo se informa que para el riesgo de alteración o perdida de información el control establecido es la política de seguridad de la información y para tal fin, dicha política no se tiene concebida dentro de la entidad.

5. Falta de diligenciamiento de información en el mapa de riesgos :

Revisando el mapa de riesgos publicado en el Sistema integrado de gestión de la Entidad, se evidencia la falta de diligenciamiento de la información relacionada con el análisis de oportunidades de acuerdo con lo establecido en el numeral 5.5 de la guía de administración

del riesgo oficializada en el SIG que titula Matriz de calificación de oportunidades, allí se ilustra la metodología para el diligenciamiento de este aspecto en el mapa.

6. Calificación de nivel de riesgo:

Aleatoriamente, se revisa la calificación asociada a los riesgos del ámbito tecnológico el cual se calcula del análisis entre la probabilidad y el impacto, obteniendo como resultado lo siguiente:

- Al riesgo denominado alteración o perdida de información se han asignado los valores de impacto (4) y probabilidad (2), no obstante y como se tiene identificado dentro de la Oficina de sistemas, no se está tomando el backup de la información contenida en los equipos de los funcionarios, únicamente se está realizando la copia de seguridad al momento de la finalización de un contrato de prestación de servicios pero para el personal de planta no se está realizando, lo anterior debido a que no se cuenta con el suficiente espacio libre de almacenamiento dentro de los servidores; basado en esta explicación, esta oficina opina que los valores tanto de probabilidad como de impacto conllevan a una variación.

- El riesgo vulnerabilidad de la información tiene como impacto valor 4 y probabilidad 1; respecto a esta calificación se expresa que como resultado de la ejecución de las auditorías a los diferentes sistemas de información de la Entidad, la Oficina de Control Interno ha manifestado debilidades en el tema de administración de usuarios, roles y perfiles así como también las falencias que se presentan a nivel de autenticación (password), también fueron evidenciados temas de no inactivación de cuentas de usuario al momento de tomar periodos de vacaciones por parte de un funcionario de planta. Todos estos factores inciden en el tema de seguridad de la información por tanto, se considera que la calificación asignada actualmente, no es acorde a la realidad, a pesar de no conocerse o haberse presentado eventos que afecten la seguridad de los datos.

- Para el riesgo de daño en infraestructura tecnológica se tienen calificado el impacto con valor 4 la probabilidad 2, no obstante, durante la presente vigencia se han presentado eventos de cortes en el suministro eléctrico.

- En concordancia con el riesgo denominado *incumplimiento de las disposiciones legales en relación con la Gestión documental y la normatividad asociada a las TIC´s*, se menciona que el valor de impacto es 4 y probabilidad 2, no obstante enfatizamos que la probabilidad puede variar debido a que durante las ejecuciones de auditorías por parte de la OCI, se han manifestado incumplimiento normativos en temas tales como derechos de autor, política de seguridad de la información contenida en la resolución 305 de 2008, ley 1712 de 2014 y Decreto 619 de 2007 respecto a información publicada en la página web, así como también se menciona el Decreto 1151 de 2008 por el cual se establecen los

lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia.

b) **INDICADORES:**

Para el proceso de Gestión de la información y la tecnología, la Oficina de Sistemas tiene definidos 2 indicadores propios del ámbito tecnológico los cuales son:

- Porcentaje de requerimientos de software implementados: En el último periodo reportado (septiembre - octubre) se reporta un cumplimiento del 97%.

- Porcentaje de adquisición de componentes TIC´S: En el último periodo reportado (septiembre - octubre) se reporta un cumplimiento del 100%.

Basado en el análisis y revisión de los indicadores, se presenta las siguientes observaciones:

- Con relación a la información publicada en la página web de la entidad, se evidencia diferencia de los indicadores entre el cuadro de mando ubicado en el último vinculo correspondiente al año 2016 versus el tercer reporte de los indicadores (primer vinculo); en el primer caso se reporta un solo indicador denominado porcentaje de servicios atendidos por área y para el segundo caso se reportan 2 indicadores *%de requerimientos de software implementados* y *% Porcentaje de adquisición de componentes TIC´s*. Lo expuesto indica que la información no se encuentra actualizada.

- Para la presente vigencia, en la Entidad, no se realizó diligenciamiento de los formatos que permitan realizar seguimiento a los indicadores definidos por la CDS, debido a que la comisión se encuentra en proceso de redefinición de estrategias. También cabe resaltar que el programa de capacitación para ilustrar los indicadores definidos no fue socializado ni ejecutado por la CDS. Lo anterior contraviene lo estipulado en el artículo 4 y 6 de la resolución 305 de 2008. Entendiendo que para cumplir con el requisito de la norma en gran medida depende de las actividades que desarrolle la Comisión Distrital de Sistemas, desde la entidad se debe solicitar oficialmente instrucciones para atender los artículos mencionados, ya que el incumplimiento continúa.

- No se han publicado en la página web de la entidad los indicadores actualizados a diciembre de 2016; el último reporte evidenciado data del mes de octubre de 2016.

- Respecto a la estrategia de gobierno en línea, es claro que la estrategia cuenta con unos plazos para su total cumplimiento, no obstante esta oficina en su rol de asesoría

y acompañamiento hace un énfasis especial para que dentro de la entidad se contemple el tema de los indicadores que el MINTIC consigna en el manual de la estrategia, informando que para el 2017 el componente de Tic para la gestión en el cual se relacionan varios temas de indicadores, se tiene que implementar al 80%

V. RIESGOS

Los siguientes son los riesgos que se presentan derivados de las observaciones:

- Incumplimientos normativos por la falta de actualización de la información en los sitios oficiales.
- Materialización de riesgos asociados al diario quehacer debido a su falta de contemplación dentro del mapa.
- Fallas en el tratamiento de los riesgos por la ausencia o escasez de controles.
- No conformidades provenientes de las auditorias de calidad o al sistema integrado de gestión.
- Errores en la toma de decisiones.
- Destinaciones inadecuadas de recursos.
- Planificación ineficiente.
- Diagnósticos de problemáticas inadecuados.
- Mediciones o métricas insuficientes.

VI. RECOMENDACIONES GENERALES.

A continuación, a Oficina de Control Interno presenta de manera general las siguientes recomendaciones:

- En las reuniones estratégicas periódicas que se realizan en la Oficina de Sistemas, se debe ahondar en los temas de riesgos e indicadores actualizando la información correspondiente cada vez que se amerite.
- Realizar un análisis de riesgos minucioso incluyendo sus valoraciones y así actualizar los riesgos en el mapa de la Oficina de sistemas.
- Construir un registro de eventos que sucedan a nivel de tecnología, el cual proveerá la información necesaria para la creación de nuevos riesgos y controles.
- Incluir dentro del mapa de riesgos todos los controles que la Oficina de sistemas tiene implementados en pro de la protección en materia de tecnología. Complementariamente asociar controles robustos a todos los riesgos relacionados con tecnología.
- Diligenciar el mapa de riesgos de acuerdo con lo estipulado en la guía de administración del riesgo oficial publicada en el SIG.
- Actualizar la información de riesgos e indicadores en la página web de la entidad.

- Oficiar a la Comisión Distrital de Sistemas respecto al tema de indicadores contemplados en la resolución 305 de 2008, con esto proceder a atender el tema y evitar el incumplimiento normativo.
- Construir para la presente vigencia, indicadores que se encuentren alineados con la estrategia de gobierno en línea (GEL), buscando cumplir con el porcentaje definido.

VII. CONCLUSION

Los riesgos e indicadores son elementos claves de carácter estratégico que permiten entre otros aspectos, el control operativo, directivo y estratégico, la planificación y la toma acertada de decisiones, medición y monitoreo de resultados, orientación del rumbo, identificación y diagnóstico de problemáticas y oportunidades, definición de responsabilidades, así como la estimación de recursos. Todo esto conjugado hacia un fin común que permita la contribución al cumplimiento de los objetivos estratégicos y la misionalidad de la Defensoría.

En sí, es de carácter importante realizar una actualización basada en un análisis detallado de la información registrada en el mapa de riesgos y en el reporte de indicadores, para que de manera eficaz y eficiente se brinde la información requerida, minimizando en su máxima expresión los riesgos que se encuentran asociados a la diaria labor que se tiene en el ámbito tecnológico, así como también permita una toma de decisiones eficiente y eficaz con los datos registrados en los indicadores.

Cordial Saludo,

WILLIAM VALDERRAMA GUTIERREZ
Jefe Oficina de Control Interno.

Copia: Oficina de sistemas.

Proyectó: Diego Alexander Urazán Franco
Fecha: 29 de Diciembre de 2016