PERIODO DE EJECUCION

Entre los días 18 de agosto y el 18 de septiembre de 2020, se llevó a cabo evaluación del proceso de Estrategia de Tecnologías de la Información y las Comunicaciones de la Secretaría General, de acuerdo con lo programado en el Plan Anual de Auditoría para el 2020.

OBJETIVO GENERAL

Evaluar los controles claves aplicables como los asociados a la matriz de riesgos de los procedimientos que conforman el proceso Estrategia de Tecnologías de la Información y las Comunicaciones. Así como, establecer el cumplimiento de directrices normativas internas y externas aplicables en la materia por la Secretaria General a través de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

ALCANCE

Verificar la adecuada aplicación de los controles establecidos por la OTIC de los procedimientos que conforman el proceso Estrategia de Tecnologías de la Información y las Comunicaciones, correspondiente al periodo comprendido entre enero a julio de 2020, con base en la muestra seleccionada como del cumplimiento de las directrices normativas internas y externas aplicables en la materia de acuerdo con las pruebas practicadas.

EQUIPO AUDITOR:

Jorge Eliecer Gómez Quintero - Jefe Oficina de Control Interno.
Constanza Cárdenas Aguirre – Auditora de Sistemas.

METODOLOGIA APLICADA

Para el desarrollo de las pruebas de auditoría al proceso Estrategia de Tecnologías de la Información y las Comunicaciones, se aplicaron las técnicas de auditoria internacionalmente aceptadas tales como indagación, observación, inspección y comprobación selectiva a través de muestreo, entre otros.

MARCO NORMATIVO:

- Caracterización del proceso Estrategia de Tecnologías de la Información y las Comunicaciones (4204000-PO-051 V01 de septiembre 2018).
- Elaboración del Plan Estratégico de TI basado en la Arquitectura Empresarial de TI (2213200-PR-116 V11 de octubre 2019).
- Análisis, Diseño, Desarrollo e Implementación de Soluciones (2213200-PR-106 V13 de febrero 2020)
- Activos de Información (2213200-PR-187 V08 de julio 2020).
- Plan Estratégico de Tecnologías de Información PETI (2211700-OT-043 V06 de octubre 2019).
- Guía para el Inventario, Clasificación, Etiquetado de Información, protección de datos personales y análisis de riesgos de los Activos de Información (2213200-GS-004 V08 de julio 2020)

- Protocolo para la elaboración de Fichas Técnicas para Adquisición de Infraestructura Tecnológica (2211700-GS-048 V02 de junio 2018)
- Manual del Sistema de Seguridad de la Información (4204000-MA-031 V02 de julio 2020)
- Manual de Políticas y procedimientos para el tratamiento de datos personales (4204000-MA-033 V01 de diciembre 2019)
- Metodología para el Desarrollo y Mantenimiento de Soluciones (2213200-OT-006 V04 de enero 2020)
- Lineamientos para la implementación y sostenibilidad del sistema se gestión de seguridad de la información (2211700-OT-048 V02 de julio 2018)
- Mapa de Riesgos del proceso publicada en el Sistema Integrado de Gestión del 5 marzo 2020
- Marco de Referencia Cobit 2019 – Objetivos de Gobierno y Gestión

CONCLUSION

Como resultado de las pruebas de auditoría practicadas al proceso de Estrategia de Tecnologías de la Información y las Comunicaciones para el período comprendido entre enero y julio de 2020, proceso a cargo de la OTIC, el cual apoya la implementación del Plan Estratégico de TI (PETI) y permite el acceso oportuno a la información requerida por la entidad, se concluyó que se encuentran adecuadamente implementados y operando los controles asociados a la definición del Plan Estratégico de TI e identificación de los Activos de Información de la Entidad, en cuanto a:

- Definición y publicación el Plan Estratégico de Tecnología anualmente.
- Identificación, actualización y publicación anual de los Activos de Información por cada una de las Dependencias de la Entidad.
- Procedimientos y documentos contentivos del proceso, debidamente actualizados y publicados.

No obstante, se observaron algunas situaciones susceptibles de mejora, relacionadas con: la actualización de los procedimientos y documentos contentivos del proceso evaluado, análisis detallado del indicador de medición de disponibilidad y operación de los Sistemas de Información, seguimiento al Plan Estratégico de Tecnología y necesidad de implementar una mejora sustancial al procedimiento Análisis, Diseño, Desarrollo e Implementación de Soluciones (2213200-PR-106).

En relación con las situaciones evidenciadas producto de las pruebas practicadas, pueden generar riesgos importantes como detección inoportuna de desviaciones en la ejecución de los proyectos con alto contenido tecnológico, implementación de soluciones incumpliendo los procedimientos establecidos y/o las normas de tratamiento de datos personales. En tal sentido, es necesario tomar las medidas pertinentes y oportunas para reducir la exposición de los riesgos observados en la implementación de soluciones tecnológicas y administración de los activos de información de la entidad. A continuación, detallamos las debilidades encontradas en la operación de los controles aplicados:

- **Plan Estratégico de TI:**

  - Aunque se cuenta con un indicador de medición de la Disponibilidad y Operación de los Sistemas de Información, el mismo no guarda proporcionalidad entre las horas no disponibles reportadas y el porcentaje de cumplimiento calculado. Dicho indicador no ha sido revisado, analizado ni actualizado en los últimos cuatro (4) años, de manera que permita establecer su efectividad, validez y utilidad.
  - Control de seguimiento trimestral que realiza la OTIC con respecto al avance de los proyectos con alto componente tecnológico, no cuentan con análisis y soportes como conceptos técnicos que, permitan asegurar la validez de la información reportada por cada una de las dependencias de la entidad que gerencia dichos proyectos.

- **Análisis, Diseño, Desarrollo e Implementación de Soluciones:**

  - Dificultad para establecer la población total de necesidades y/o requerimientos implementados durante el período evaluado, puesto que no se tienen categorías claramente establecidas en la herramienta Mesa de Servicio, que permita identificar los casos asociados a la tipificación de requerimientos que son objeto del procedimiento PR-106.
  - El procedimiento PR-106 para la implementación de soluciones, no diferencia de manera clara y concisa los tipos de documentos requeridos como soporte de la ejecución de las tareas y controles, teniendo en cuenta que los soportes y documentos dependen del tipo de requerimiento que se realice. Citamos como ejemplo, la documentación soporte es diferente si el requerimiento corresponde a una nueva funcionalidad de un sistema de información o si es alistamiento de nuevos servidores o nuevos repositorios GIT, entre otros.

- **Activos de Información:**

  - En la última actualización de los Activos de Información con corte diciembre 2019, se observó que la Dirección Distrital de Archivo de Bogotá presenta riesgos, sin contar con la identificación de controles para su mitigación, aceptación o transferencia del mismo.

OBSERVACIONES Y RECOMENDACIONES PRODUCTO DE LA EVALUACIÓN

Para evaluar el Proceso de Estrategia de Tecnologías de la Información y las Comunicaciones, se realizaron pruebas a los controles implementados por la Entidad para definir el Plan Estratégico de TI, la implementación de proyectos con alto contenido tecnológico y soluciones tecnológicas, la identificación de los Activos de Información sensibles y de las bases de datos personales que se manejan en la entidad.

En tal sentido a continuación, se describen los principales aspectos observados y las recomendaciones formuladas como resultado de las pruebas practicadas:

1. Documentación del Proceso en el Sistema Integrado de Gestión (caracterización, procedimientos, guías, manuales y otros procedimientos)

Oportunidad de Mejora No. 1:

Se observó que, en el Sistema Integrado Gestión, existen documentos sin actualizar y/o sin evidencia de revisión que confirme su actual aplicación y uso. Los documentos son:

- Caracterización del proceso Estrategia de Tecnologías de la Información y las Comunicaciones (4204000-PO-051 V01 de septiembre 2018).
- Protocolo para la elaboración de Fichas Técnicas para Adquisición de Infraestructura Tecnológica (2211700-GS-048 V02 de junio 2018).
- Lineamientos para la implementación y Sostenibilidad del Sistema de Gestión de Seguridad de la Información (2211700-OT-048 V02 de julio de 2018).
- Recepción Documentación Software (2213200-FT-744 V02 de octubre de 2013).
- Ubicación Física en Cuarto de Medios (2213200-FT-743 V01 enero de 2011).

Para algunos de los documentos actualizados durante el segundo semestre del año 2019 y el primer semestre de 2020, no se encontró evidencia de socialización de los mismos. Adicionalmente, se observaron documentos que no se referencian en la Caracterización del Proceso, aunque hacen parte del mismo y son requeridos para su operación.

De otra parte, el Manual del Sistema de Seguridad de la Información (4204000-MA-031), aunque se encuentra referenciado en la caracterización del proceso, no se encuentra referenciado en ninguno de los tres (3) procedimientos contentivos del proceso.

Recomendación

Desde la OTIC, como oficina líder del proceso, y con el apoyo de la Oficina Asesora Planeación, revisar y actualizar la Caracterización del Proceso, con base en la operatividad de los procedimientos en caminado a asegurar que todos los documentos (manuales, guías y otros documentos) estén claramente referenciados y documentados en la caracterización respectiva, y sean entendibles para todas las partes interesadas.

Asimismo, revisar detalladamente todos los documentos contentivos del proceso Estrategia de Tecnologías de la Información y las Comunicaciones para confirmar que se encuentran actualizados, socializados y/o definir si los que a hoy tiene fechas muy antiguas requieren ser actualizados o siguen vigentes.

2. Indicador de medición del proceso No.138 Porcentaje de Disponibilidad y Operación de los Sistemas de Información de la SG.

Observación No. 1:

Analizados los resultados del indicador No 138, que mide la disponibilidad y operación de los Sistemas de Información de la Secretaría General (misionales, administrativos y portales) para los meses enero a junio 2020, se estableció que el cálculo porcentual no guarda coherencia con la cantidad de horas no disponibles reportadas. Realizados los cálculos porcentuales tanto linealmente como proporcional según porcentajes por cada tipo de sistema de información, no es posible llegar al resultado indicado en los reportes del indicador, se evidenció que las horas no disponibles reportadas (217,33) para un total de 144 en el mes de enero de 2020, no guardan coherencia con el cumplimiento de la meta reportada del 97.1%.

De acuerdo con lo indicado por la OTIC, el cálculo del porcentaje del mes de enero, se evidencia una diferencia bastante marcada entre las horas disponibles y el porcentaje de cumplimiento reportado, se debe a que las horas de ese mes y la cantidad de horas no disponibles incluyó diciembre 2019 y enero debido a que no hubo corte por el cambio de año. Sin embargo, debido a la dificultad del soporte con la herramienta ADPLATEC que genera el indicador, no fue posible confirmar esta situación.

A continuación, se relaciona el análisis realizado al indicador en mención:

	Meta	Medición	Horas Mes	Horas No Disponibles	Porcentaje cumplimiento con Cálculo lineal (1)	% de Diferen-cia	Porcentaje cumplimiento con Cálculo porcentual (2)	% de Diferen-cia
Enero	96%	**97,1%**	744	217,33	71%	-26,3%	71%	-26,3%
Febrero	96%	**99,8%**	696	2,5	100%	-0,2%	100%	-0,2%
Marzo	96%	**100,0%**	744	0,5	100%	-0,1%	100%	-0,1%
Abril	96%	**99,9%**	720	3,92	99%	-0,4%	99%	-0,4%
Mayo	96%	**100,0%**	744	12,58	98%	-1,7%	98%	-1,7%
Junio	96%	**99,9%**	720	25,23	96%	-3,4%	96%	-3,4%

(1) Fórmula porcentaje lineal calculado: 100% - (horas no disponibles/horas mes)*100

(2) Fórmula cálculo porcentual (A.60% misional, B.25% Administrativo, C.15% portales): sobre las horas no disponibles se calcula el % correspondiente a cada tipo de sistema y se aplica la fórmula (100% - (A+B+C)/horasmes)*100)

Las situaciones mencionadas generan riesgos como detección inoportuna de indisponibilidad de los sistemas de información, toma de decisiones erradas debido a deficiencias en la información reportada con la medición del indicador.

Recomendación

Es importante que la OTIC adelante gestiones encaminadas a revaluar las variables y fuentes de información con que se realiza el cálculo de disponibilidad y operación de los Sistemas de Información de la Entidad, garantizando así la validez del mismo y realizar los ajustes necesarios que permitan asegurar que todos los sistemas de información y variables posibles para el cálculo del mismo están siendo incluidas generando resultados coherentes y efectivos, permitiendo a la entidad identificar oportunamente indisponibilidad de los sistemas de información y tomar medidas conducentes a solucionar la causa raíz de las fallas presentadas.

De igual forma es necesario, que se realicen revisiones periódicas del indicador, con miras a identificar mejoras constantes en el mismo o la necesidad de implementar nuevos indicadores para la medición del proceso, aspectos que, según mejores prácticas de mediciones, se gestionan cuando los indicadores existentes se encuentran estabilizados, permitiendo contar con retos y metas diferentes.

3. Base de Datos con información Personal – Registro Nacional de Bases de Datos RNBD

Observación No. 2:

En la consulta realizada en la página de la Superintendencia de Industria y Comercio, correspondientes a los registros de Bases de Datos de la Secretaría General que deben ser publicadas, no se evidencian algunas bases de datos que almacenan información personal como las mencionadas a continuación, con el riesgo de incumplimiento del decreto nacional 090 de 18 ene 2018 del Ministerio de Comercio, Industria y Comercio:

- Bogotá Te Escucha (información de los ciudadanos)
- Sistema de Gestión Contractual (información de los contratistas).
- SIAB (por ejm. Encuestas de satisfacción).

De las veintinueve (29) Bases de Datos cargadas en el RNBD de la SIC, solo una se encuentra publicada en la página Web de la Entidad. La Base de Datos publicada es: “Base de datos de las entidades que conforman el portafolio de servicios de la guía de trámites y Servicios”.

Recomendación:

Es necesario que, desde la OTIC como parte del proceso que actualmente se viene adelantando para la actualización de los Activos de Información, y en conjunto con cada una de las dependencias de la entidad, identificar todas las bases de datos que almacenan información personal de ciudadanos, contratistas, funcionarios, etc, y asegura que se encuentren en las matrices de Activos de Información, al igual que asegurarse que se publican en la RNBD según es requerido por la SIC.

4. Plan Estratégico de Tecnología (2213200-PR-116)

Observación No. 3:

Analizado el PETI, aprobado y publicado en el SIG en el mes de octubre 2019, con respecto a los soportes recibidos de los seguimientos realizados por la OTIC con corte diciembre 2019 y junio 2020, se evidenció que el PETI incluye por cada proyecto sus correspondientes metas y el presupuesto planeado para cada vigencia. Sin embargo, realizado el cruce con los archivos de seguimiento a diciembre 2019 y junio 2020, y verificada la información mencionada en dicho documento para la vigencia 2020 (correspondiente al periodo enero – junio 2020), se observó que en el PETI se indica un presupuesto asignado y que los valores difieren de los detallados en los seguimientos trimestrales sin contar con una conclusión o justificación que de cuenta de las modificaciones o actualizaciones de presupuesto planeado vs ejecutado.

Se identificó que la labor realizada por la OTIC, tiene como objetivo confirmar con base en la información reportada por cada dependencia, el porcentaje de avance y cumplimiento de las actividades programadas para cada proyecto; sin embargo, no se observó un análisis detallado y técnico por parte de la OTIC que permita concluir si los porcentajes de avance reportados por las dependencias son válidos, ni se evidencia un análisis sobre los valores proyectados en el PETI vs los reportados como planeados y ejecutados por cada dependencia en cada corte trimestral.

Por lo anteriormente expuesto, se considera que el seguimiento trimestral realizado por la OTIC se limita a consolidar las respuestas de las dependencias con la información recibida sin practicar un análisis y concepto técnico para confirmar la validez de los avances de los proyectos, adicionalmente, no se evidencian soportes de revisión y análisis técnicos sobre las diferencias de valores planeados vs ejecutados entre el PETI vs los resultados producto de los seguimientos trimestrales.

Recomendación:

Revaluar y replantear los controles actuales que se tienen definidos en los procedimientos, incluyendo aspectos relevantes como análisis y generación de conceptos técnicos desde la OTIC, como área experta en aspectos tecnológicos, evaluando tanto porcentajes de avances y cumplimiento de tareas como las diferencias en valores presentadas entre lo proyectado en el PETI inicialmente y lo realmente reportado como planeado y ejecutado por cada dependencia en cada trimestre.

Los controles que deben ser replanteados son los relacionados con el seguimiento a los proyectos de TI con componente tecnológico y a la evaluación de programas y proyectos de PETI, correspondientes a los controles 14 y 16 establecidos en la versión 12 del procedimiento PR-116.

Por otro lado, se sugiere como parte del control trimestral que se realiza en la OTIC, soportar los valores incluidos en el Excel de seguimiento con evidencias de los contratos o registros presupuestales generados del Sistema de Gestión Contractual, y de ser necesario coordinar el fortalecimiento de este control con la Oficina Asesora de Planeación.

5. Análisis, Diseño, Desarrollo e Implementación de Soluciones (2213200 – PR-106)

Observación No. 4:

El procedimiento PR-106, en su sección 5. Condiciones Generales, relaciona los tipos de requerimientos y necesidades tecnológicas, para las que se deben seguir las actividades y controles definidos en el mismo, sin embargo, no fue factible establecer toda la población objeto, dificultando evaluar de manera adecuada el cumplimiento del procedimiento en la implementación de soluciones tecnológicas.

Para una muestra de quince (15) casos de soporte, recibidos como fuente de información aplicables al procedimiento referenciado, se observaron las siguientes situaciones:

- Tres (3) corresponden a tipos de requerimientos relacionados con nuevas funcionalidades de Sistemas de información, solicitudes de nuevo repositorio GIT y solicitud de nuevas licencias o programas, que no cuentan con el formato FT-264, análisis de viabilidad ni seguimiento periódico, como soporte registrado en GLPI.

- Doce (12) no correspondían a casos aplicables al procedimiento PR-106, con lo cual se concluye que no se cuenta con una fuente de información válida que permita asegurar la integridad y completitud de la población total de requerimientos o necesidades tecnológicas a las que les aplica el procedimiento en mención.

Observación No. 5:

De veintinueve (29) contratos, que de acuerdo con la población remitida por la OTIC corresponden a objetos contractuales relacionados con el procedimiento para la Implementación de Soluciones, para una muestra de nueve (9) contratos (31%), se evidenciaron las siguientes situaciones:

- Seis (6) no cuentan con el formato FT-264 Solicitud de Requerimientos
- Cinco (5) no cuentan con soporte relacionado con el análisis de viabilidad realizado
- Dos (2) sin soporte de seguimiento a la solución o requerimiento

De otra parte, se observó que el procedimiento en su tarea 6 – entrega de la solución o requerimiento, relaciona en detalle los documentos requeridos en la Metodología para el Desarrollo y Mantenimiento de Sistemas de Información (OT-006) en la entrega a satisfacción de la solución, sin embargo, no es factible identificar los documentos soporte que aplican o no a cada caso definido en las Condiciones Generales del procedimiento. Existen algunos documentos que aplican para desarrollo de software, pero no para alistamiento de servidores, solicitudes de nuevos dominios, nuevas licencias o repositorios GIT y REDMINE, a continuación, algunos ejemplos:

Contrato	Objeto Contractual	Observaciones OCI
188	Prestar servicios profesionales para desarrollar, implementar nuevas funcionalidades, brindar soporte y mantenimiento en los sistemas: a) Presupuesto Interno, b) Cuentas por Cobrar - Facturación c) sistema de Gestión Contractual y los ajustes necesarios requeridos en dichos sistemas de	No se cuenta con evidencia de: - Pruebas funcionales y aceptación. - Manuales - Código fuente - Derechos de autor - Plan Capacidad

Contrato	Objeto Contractual	Observaciones OCI
	información, en la Secretaria General de la Alcaldía Mayor de Bogotá D.C.	- Copia de Seguridad - Evaluación Post-implementación - Actualización documental **Nota:** Se aclara que puede no requerirse esos soportes, sin embargo, debido a que el procedimiento no es claro en este aspecto, no es factible confirmar la necesidad o no de la documentación mencionada.
377	Adquirir productos y servicios Microsoft para dar continuidad a las aplicaciones, sitios y/o páginas web a través del Acuerdo Marco de Precios No. CCE-578-2017 para la Secretaría General de la Alcaldía Mayor de Bogotá D.C.	No se cuenta con evidencia de: - Pruebas funcionales y aceptación. - Análisis de impacto - Manuales - Plan Capacidad - Vulnerabilidades - Evaluación Post-implementación - Actualización documental **Nota:** Se aclara que puede no requerirse esos soportes, sin embargo, debido a que el procedimiento no es claro en este aspecto, no es factible confirmar la necesidad o no de la documentación mencionada.

Es de anotar que, la forma como está definido el procedimiento la fuente de información para la ejecución y aseguramiento del procedimiento deberían corresponder a las implementaciones puestas en producción, sin embargo, este procedimiento se aplica para la administración de contratos relacionados con mantenimiento, desarrollo e implementación de soluciones tecnológicas tanto de software como de infraestructura, y de esta forma no es factible asegurar que cada implementación o requerimiento cumple con lo definido el procedimiento PR-106.

Las anteriores situaciones mencionadas, generan riesgos de implementación de soluciones sin cumplir con los controles establecidos por la entidad, inoportunidad en la atención de los requerimientos o solicitudes tecnológicas requeridas para el funcionamiento de los sistemas de información.

Recomendación Observaciones No. 4 y 5:

Evaluar y rediseñar el procedimiento Análisis, Diseño, Desarrollo e Implementación de Soluciones (2213200 – PR-106), detallando las actividades, registros documentales y controles correspondientes a cada tipo de requerimiento o necesidad tecnológica. De otra parte, es necesario separar tareas, responsables, controles y documentos soporte de lo correspondiente a la ejecución de un contrato tecnológico para el mantenimiento y/o implementación de soluciones tecnológicas de lo correspondiente al proceso para la implementación en producción de las soluciones tecnológicas.

Observación No. 6:

Analizados los tipos de requerimientos definidos en el procedimiento vs las categorías parametrizadas en la herramienta GLPI para el registro de las necesidades tecnológicas y medición del cumplimiento de los ANS, se encontró que no existe una relación directa entre el procedimiento y las categorías de la mesa de Servicio, así:

Definición tipo de requerimiento según procedimiento	Posible categoría asociada en GLPI
Nuevos Sistemas de Información y Portales Web Nuevas Funcionalidades sobre los sistemas de información y portales Web	INFRAESTRUCTURA > Despliegue de nuevas aplicaciones o versiones en PRODUCCIÓN PORTALES > Fallo o Ajuste en Funcionalidad SISTEMAS DE INFORMACIÓN > Ajustes a funcionalidades en sitios web SISTEMAS DE INFORMACIÓN > Falla funcionamiento de Sistema de Información SISTEMAS DE INFORMACIÓN > Fallo o Ajuste en Funcionalidad SISTEMAS DE INFORMACIÓN > Sistema de Información SIVIC > Nuevos Desarrollos (Actualizaciones) SISTEMAS DE INFORMACIÓN > Sistema de Información, portales, aplicativos WEB no disponible SISTEMAS DE INFORMACIÓN > Desarrollo e implementación de minisitios o sitios web
Nuevos equipos y componentes tecnológicos para las Dependencias	No se observa una categoría en GLPI que pueda asociarse a este tipo de requerimiento
Solicitudes de alistamiento de nuevos servidores	Equipos de Cómputo > Alistamiento y Configuración INFRAESTRUCTURA > Servidores LINUX > Alistamiento Máquina Virtual
Solicitudes de nuevos dominios	INFRAESTRUCTURA > Directorio Activo > Apuntamiento DNS, Dominio y subdominios INFRAESTRUCTURA > Directorio Activo > Creación de nuevo dominio SISTEMAS DE INFORMACIÓN > Creación y apuntamientos de dominios y/o subdominios
Solicitudes de nuevas licencias o programas	No se observa una categoría en GLPI que pueda asociarse a este tipo de requerimiento
Instalación de módulos o plugins en los portales o micrositios web	No se observa una categoría en GLPI que pueda asociarse a este tipo de requerimiento
Actualización del core de cms o frameworks en los portales o micrositios web	No se observa una categoría en GLPI que pueda asociarse a este tipo de requerimiento
Solicitudes de nuevo repositorio git y redmine	PORTALES > Creación de Repositorio

Recomendación:

Revisar y ajustar tanto el procedimiento PR-106 Análisis, Diseño, Desarrollo e Implementación de Soluciones como la herramienta de Mesa de Servicio GLPI en cuanto a la tipificación de categorías por las que se registran las solicitudes de necesidades y requerimientos tecnológicos, así como definir los ANS respectivos de cumplimiento para la atención por Mesa de Servicio de dichas solicitudes según la tipificación definida en el procedimiento respectivo.

6. Activos de Información

Observación No. 7:

Analizados los archivos Excel recibidos de la OTIC, correspondientes al año 2019, se observó una (1) dependencia con riesgos, sin identificación de controles para su mitigación, aceptación o transferencia del mismo. La dependencia es: Dirección Distrital de Archivo de Bogotá, específicamente para diez (10) activos de información (librejo, inventario bibliográfico, kárdex, CINEP (carpetas), CINEP (Artículos), publicaciones seriadas, audiovisual, publicaciones periódicas, MIDAs, SIAB) cuyo riesgo es pérdida de la disponibilidad de la información.

Lo anterior conlleva a riesgos de pérdida de información sobre los Activos de información de la Entidad, en caso de no contar con planes de tratamiento adecuados para su mitigación.

Recomendación:

Teniendo en cuenta que actualmente la OTIC se encuentra en proceso de actualización de los Activos de Información con las dependencias, se hace necesario asegurar que todas las dependencias de la entidad identificaron sus Activos de Información y, en caso que aplique, que se definieron los Planes de Tratamiento correspondientes. Asimismo, asesorar y confirmar con las áreas que reportan activos de información a cargo de entes externos, se realice el análisis respectivo y como plan de mitigación se acepte o se transfiera el riesgo.

7. Mapa de Riesgos y Controles en el Proceso

Verificada la matriz de riesgos del proceso, se observó que los controles definidos en la misma se encuentran actualizados y son consistentes con los puntos de control de los procedimientos del mismo, observando algunas situaciones que se consideran oportunidades de mejora, como son:

Oportunidad de Mejora No. 2

Los controles definidos hacen parte de la dinámica diaria de la operación, sin embargo, el proceso requiere fortalecerse con controles claves de monitoreo, entre otros, mencionamos los siguientes:

- El procedimiento PR-116 – Plan Estratégico de TI, no cuenta con controles clave para la aprobación formal de los seguimientos trimestrales y revisión de los avances que se realizan a los proyectos tecnológicos, según lo definido en los controles 14 y 16 del procedimiento. Los controles tienes definidos sus responsables, no obstante, no se evidencia como aprobador de estos controles significativos, al jefe de la OTIC como nivel jerárquico adecuado para tan importante labor como es la revisión y seguimiento al cumplimiento de la ejecución de los proyectos tecnológicos.
- El procedimiento PR-106 – Implementación de Soluciones, los controles definidos están dados para las etapas de análisis y diseño, mas no se cuenta con controles asociados a las labores de desarrollo, pruebas e implementación de la solución, de manera que cubra ampliamente el objeto del procedimiento.

Oportunidad de Mejora No. 3:

Se evidenció que el Mapa de Riesgos del proceso publicado en el SIG con fecha marzo 2020, se encuentra desactualizado, por las siguientes razones:

- ✓ En el procedimiento PR-187 – Activos de Información, el responsable del control No. 13 detallado en el procedimiento difiere del indicado en la descripción del control del Mapa de Riesgos. En el mapa de riesgos los responsables de la ejecución del control son el Oficial de Seguridad de la Información y la Dependencia responsable, y en el procedimiento es únicamente el Oficial de Seguridad de la Información. De otra parte, el control 14 del mismo procedimiento, no se encuentra actualizado en el mapa de riesgos.
- ✓ Solicitados los soportes de los monitoreos realizados a los controles definidos en los mapas de riesgo, se encuentran evidencias de la ejecución de los mismos, más no un monitoreo periódico que se realice desde la OTIC para concluir sobre la efectividad de los mismos y la materialización o no de los riesgos. Por ejemplo, se evidencian memorandos, archivos, reuniones, formatos que dan cuenta del cumplimiento de los controles definidos en los procedimientos, sin embargo, no se realiza monitoreo periódico que permita asegurar la efectividad de los mismos.
- ✓ El procedimiento PR-116 – Plan Estratégico de TI, en su versión 12 publicada en agosto se evidencia el control No. 15 – Verificar recibo de respuestas avance a proyectos con componente TI, el cual aún no se encuentra detallado en el mapa de riesgos.

Con respecto al procedimiento PR-106 Análisis, Diseño, desarrollo e implementación de solucione, se observó que los registros documentales de los controles No. 3, 5 y 8 difieren de los establecidos en el mapa de riesgos. Asimismo, en las evidencias analizadas en cumplimiento a la ejecución del control No.3 respecto al análisis de viabilidad del requerimiento, no se observa relación entre cada solicitud realizada por las dependencias vs un caso de servicio en GLPI, no permitiendo contar con una trazabilidad adecuada sobre la ejecución del control.

De otra parte, se definen dos (2) controles corresponden a las auditorías a cargo de la OCI, que no corresponden a controles propios de la operación del proceso Estrategia de Tecnología ni son de responsabilidad de la OTIC, como encargado en “primera línea” de su óptimo funcionamiento.

En relación con las Oportunidades de Mejora 2 y 3, es conveniente el acompañamiento pronto de la Oficina Asesora de Planeación para actualizar lo antes posible el mapa de riesgos del proceso, asegurar la consistencia del mismo frente a los controles aplicados y los establecidos en los procedimientos.

Oportunidad de Mejora No. 4:

Analizados los seguimientos periódicos realizados a la ejecución del PETI, se evidenció soporte del seguimiento realizado con corte diciembre 2019 y un único documento que contiene el seguimiento de marzo y junio 2020, concluyendo que el control no se ejecutó con la periodicidad definida puesto que no se cuenta con soporte independiente del seguimiento realizado con corte marzo 2020.

Es importante que en instancia del subcomité de autocontrol o las actividades cotidianas de seguimiento al proceso, es fundamental evaluar periódicamente la efectividad de los controles implementados para detectar oportunamente los fallos en su aplicación que pueden permitir la materialización de los riesgos identificados, entre otros como: desarrollo inapropiado de soluciones tecnológicas, proyectos con alto componente tecnológico sin el seguimiento adecuado, activos de información sensibles o bases de datos con datos personales sin identificar o sin publicar.

Plan de Mejoramiento

Producto de la evaluación practicada y resultado del análisis del informe preliminar por la Oficina de Tecnologías de la Información y las Comunicaciones, definió acciones de mejora dirigidas a subsanar y prevenir las observaciones identificadas como gestionar las oportunidades de mejora, las cuales conforman el plan de mejoramiento establecido que hace parte integral del informe final, a efecto de adelantar los respectivos seguimientos por los responsables como por la Oficina de Control Interno para su cumplimiento.

Criterios de clasificación de conceptos derivados de la auditoría.

Tipo de observación	Descripción
Observación	Incumplimiento de normas o procedimientos internos que pueden materializar un riesgo.
Oportunidad de mejora	Sin implicar un incumplimiento normativo o de procedimientos internos, es susceptible de mejora el proceso.

Elaborado por: Constanza Cárdenas Aguirre – Contratista, Auditora de Sistemas
Revisado y Aprobado por: Jorge Eliecer Gómez Quintero – Jefe Oficina de Control Interno