PERIODO DE EJECUCION

Entre los días 8 de mayo y el 12 de junio de 2020, se llevó a cabo evaluación del proceso Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos 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 Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos, así como, verificar el cumplimiento de directrices normativas internas y externas aplicables en la materia por la Secretaría General a través de la Oficina de Tecnologías de la información y las Comunicaciones – OTIC.

ALCANCE

Verificar la adecuada aplicación de los controles establecidos en los procedimientos para la Gestión de Infraestructura y Recursos Tecnológicos de la Entidad, correspondiente al periodo comprendido entre julio 2019 a abril de 2020 por la OTIC, con base en la muestra seleccionada y 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 la auditoría al proceso Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos, 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 Gestión, administración y soporte de infraestructura y recursos tecnológicos (2213200-PO-036 V12)
- Procedimiento Gestión de Incidentes y Requerimientos Tecnológicos (2213200-PR-101 V11)
- Mantenimiento Preventivo de Recursos Informáticos (2213200-PR-104 V09)
- Administración Copias de Respaldo (backup) (2213200-PR-109 V11).
- Administración de Usuarios (2213200-PR-185 V08).
- Administración y Gestión de Bases de Datos (2213200-PR-271 V05).

- Administración Red LAN, WAN, Wireless, Equipos Activos y de Seguridad (2213200-PR-272 V05).
- Administración de Servidores de la Red de Datos (2213200-PR-273 V04).
- Guía para la realización de copias de respaldo (2211700-GS-036)
- Manual del Sistema de Seguridad de la Información (4204000-MA-031 V01)
- Decreto 1499 de 2017 – MIPG
- Mapa de Riesgos del proceso publicada en el Sistema Integrado de Gestión.
- Norma Técnica Colombiana NTC-ISO 27001:2013 – Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información.
- Marco de Referencia Cobit 2019 – Objetivos de Gobierno y Gestión

CONCLUSION

Como resultado de las pruebas de auditoría practicadas al proceso de Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos, perteneciente a la OTIC, el cual soporta la operación tecnológica de la Secretaria General, en el período comprendido entre el 1 de julio 2019 y el 30 de abril de 2020, se concluye que se encuentran implementados y operando algunos de los controles asociados a los proceso de Gestión de Incidentes y Requerimientos Tecnológicos, Administración Copias de Respaldo, Mantenimiento Preventivo de los recursos informáticos, Gestión de Bases de Datos, Administración de Servidores y de equipos de red, así:

- Solicitud, categorización y clasificación de los requerimientos o incidentes atendidos por la Mesa de Servicio. Así como, informes mensuales de seguimiento de la gestión respectiva.
- Copias de respaldo que se encuentran configuradas en la herramienta de backup (Data Protector)
- Monitoreo y alerta para los equipos de cómputo (servidores, firewalls, routers, switches), que se encuentran configurados en la herramienta Nagios.
- Mantenimientos preventivos para algunos equipos de cómputo.
- Monitoreo diario de las bases de datos.

A excepción de algunas debilidades encontradas en la operación de los controles aplicados para:

- **Administración de Usuarios:** El procedimiento vigente PR-185 Administración de Usuarios, sólo contempla lo referente a Directorio Activo, Correo Electrónico y SICAPITAL, dejando por fuera otros sistemas de información de importancia misional para la Entidad, como SIAB, SIVIC, BogotaTeEscucha, etc.

  Asimismo, se evidenciaron usuarios activos con acceso a la red, al correo y a la Base de Datos que ya no tiene relación laboral ni contractual con la entidad, al igual que usuarios genéricos sin contar con un responsable a su cargo.

- **Administración de Redes y Servidores**: Algunos servidores y equipos de red no parametrizados en la herramienta Nagios utilizada para monitorear la disponibilidad de estos recursos y el envío de alertas en caso de falla, implicando posibles demoras en la atención de las fallas de estos dispositivos.

- **Gestión de Base de Datos:** No ha sido factible realizar la aplicación de parches de seguridad a los motores de bases de datos, debido a la desactualización de las versiones que no cuentan con soporte por parte de los proveedores, como es el caso de las Bases de Datos que soportan los aplicativos SIGA, SAT (Sistema Automático de Turnos), SDQS (Sistema Distrital de Quejas y Soluciones) actual Bogotá Te Escucha, SIAB, entre otros.

- **Análisis de Vulnerabilidades**: Si bien, se ha realizado análisis de vulnerabilidades para algunos sitios Web de la Entidad (Soy10 Aprende, BogotaTeEscucha y Registro Distrital) se realiza por solicitud de las áreas de negocio, sin obedecer a una planificación. El plan para la realización de estas pruebas se encuentra sin aprobar ni formalizar, y requiere contar con un detalle de análisis de criticidad de los servicios de la Entidad para priorizar los sistemas operativos, bases de datos y sitios web que sean objeto del análisis de vulnerabilidades.

- **Mantenimiento Preventivo de Recursos Informáticos y Copias de Respaldo:** La priorización de los equipos de cómputo objeto de mantenimiento preventivo programado y de los activos de información sujetos de copias de respaldo, al no contarse con criterios claramente definidos y establecidos.

- **Gestión de Incidentes y Requerimientos Tecnológicos:** Medir la oportunidad en la solución de casos (incidentes y requerimientos) de soporte de la mesa de servicios, con la implicación de incumplimiento de los ANS establecidos y la prestación deficiente del servicio de la Mesa de Servicio.

- **Mapa de Riesgos:** Los controles establecidos en el mapa de riesgos no son consistentes con los definidos en cada uno de los procedimientos contentivos del proceso. Además, se considera que no se han definido controles claves necesarios para la mitigación de riesgos como accesos no autorizados, indisponibilidad de los servicios tecnológicos, pérdida de información, daño de equipos de cómputo, entre otros.

Las situaciones evidenciadas anteriormente, generan riesgos importantes como permitir accesos no autorizados a los sistemas de información, pérdida o indisponibilidad de información sensible para la Entidad, fallas o funcionamiento no óptimo de los equipos de cómputo y detección inoportuna de fallas de los servidores o equipos de red. Es necesario tomar las medidas pertinentes y oportunas para reducir la exposición de los riesgos observados en los sistemas de información de la entidad.

OBSERVACIONES Y RECOMENDACIONES PRODUCTO DE LA EVALUACIÓN

Para evaluar el Proceso de Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos, se realizaron pruebas a los controles implementados por la Entidad para la Gestión de Incidentes y Requerimientos, la Administración de Usuarios, Mantenimiento Preventivo de Equipos de Cómputo, de red y Servidores, Administración de Copias de Respaldo y Gestión de las Bases de Datos.

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:

Analizados los documentos en el SIG que componen el proceso evaluado, se observó que se actualizó el documento de caracterización del proceso a la versión 12, con fecha 22/04/2020 y aprobación del 8 de mayo 2020, a la fecha de finalización de la auditoría (12 de junio 2020), se encontraba pendiente de socializar el cambio presentado con el equipo de trabajo de la OTIC, actividad que se realizará en el próximo Subcomité de Autocontrol del área.

Como parte de los documentos publicados en el SIG (Sistema Integrado de Gestión), tipificados como "Otros Documentos", se encontraron tres (3) que no corresponden a temas del proceso y/o no están referenciados en los procedimientos, para lo que consideramos necesario realizar los ajustes a que haya lugar en el SIG (Sistema Integrado de Gestión). Los documentos son: Lineamiento de Gestión de Información en los portales y micrositios Web de la SG (4204000-OT-060), Plan de Contingencia de TI (2213200-OT-020) y Metodología para valoración de Riesgos de Activos de Información Vs 01 (2211700-OT-037).

Oportunidad de Mejora No. 2:

Se observó que la Entidad cuenta con lineamientos sobre Seguridad de la Información, emitidos bajo el documento Manual de Seguridad de la Información, el cual describe las políticas y normas de seguridad de la información con base en la Norma ISO27001:2013 y las recomendaciones dadas en la ISO27002:2013.

Aunque la norma da lineamientos sobre objetivos de control y controles de referencia mencionados en el Anexo A de la norma, para aspectos de copias de respaldo/restauración y mantenimiento de equipos de cómputo, en la referenciación de los procedimientos PR-104 – Mantenimiento Preventivo de Recursos Informáticos y PR-109 – Administración Copias de Respaldo, no se evidencia que estos procedimientos hayan tenido en cuenta los lineamientos de la norma, los cuales son 11.2 – Equipos. 8.3 Manejo de Medios y 12.3 Copias de Respaldo.

De otra parte, el Manual Seguridad de la Información, en su numeral 7.4 Vigencia y Actualización del Manual, se mencionan los aspectos a tener en cuenta en las revisiones periódicas y como responsable de esta tarea es la OTIC; no obstante, no se evidencian soportes de revisiones periódicas que se hayan realizado al documento actual luego de la creación del mismo en su versión 01 del 27/07/2018.

Para mejorar lo indicado anteriormente, se recomienda revisar y actualizar el Manual de Seguridad de la Información e incluir como parte de las actividades de control del proceso, la revisión anual que se realice desde la OTIC a dicho documento. De otra parte, con base en lo reportado en la observación 1 de este informe y como parte del proceso de actualización del manual en mención, con el propósito de fortalecer el control en esta materia recomendamos reducir el tiempo de la revisión de los derechos de acceso de los usuarios, *de anual a semestral.*

2. Administración de Usuarios del Directorio Activo y de la Base de Datos SI Capital

Observación No. 1:

Se observó que no se cuenta con un control periódico de monitoreo sobre los usuarios que tienen acceso al Directorio Activo y a la Base de Datos SI Capital, que permita controlar efectivamente que todos los usuarios mantienen una relación laboral con la Entidad, ya sea contratación directa o de servicios profesionales, lo que implica el riesgo de posibles accesos no autorizados a la red de la entidad (Directorio Activo) y/o a la Base de Datos SI Capital. Se identificaron las siguientes situaciones:

- Para el Directorio Activo, ochenta y un (81) usuarios que no tienen relación contractual vigente con la entidad, al corte 30 de abril, se identificaron 39 usuarios, desvinculados de la entidad con fechas de retiro que oscilan entre el 1/07/2019 y el 17/05/2020.
- Para los usuarios de la BD SI Capital, no es factible identificar el funcionario responsable debido a que no cuenta con un campo de descripción del usuario y su ID, no cuenta con un estándar para identificar nombre o apellido del responsable (por Ejm: JROBERTOG, LUMAGO, LUZCOMU2).
- Se identificaron usuarios genéricos activos, para los que no se cuenta con un responsable formal de su uso, así: 19 usuarios en el Directorio Activo y 51 usuarios en la Base de Datos SICapital.
- Se identificaron 10 usuarios activos en la Base de Datos SICapital que, según planta de personal al corte 30 de abril de 2020, se encuentran retirados de la entidad.

Las situaciones anteriormente mencionadas, generan riesgos de accesos no autorizados a la base de datos SICapital, dificultad para establecer responsabilidades en caso de uso de indebido de estos usuarios, posible ejecución de operaciones en los sistemas de información en cabeza de usuarios que no cuentan con una relación laboral o contractual con la Entidad, así como un incumplimiento al Manual del Sistema de Seguridad de la Información en su numeral 10.3.1 – Responsabilidades.

Observación No. 2:

El procedimiento 2213200-PR-185 Administración de Usuarios continúa con alcance limitado para el Directorio Activo, correo electrónico y bases de datos de SICapital, que incluye: Limay (Contabilidad), SAI/SAE (Inventarios), Perno (Nómina), Presupuesto y Gestión Contractual, observando que los demás Sistemas de Información que soportan procesos misionales y de apoyo de la Entidad, no cuentan con lineamientos que aseguren un control de acceso adecuado a los sistemas de información de la Entidad, generando riesgos importantes de posibles accesos no autorizados a los Sistemas de Información y posible ejecución de operaciones erradas, no autorizadas o sin las debidas aprobaciones en los sistemas de información.

Para dos (2) aplicativos (Sistema de Gestión Contractual y Sistema de Facturación), de una muestra de cuatro (4), se identificó que no existen procedimientos formalmente establecidos ni controles de depuración de usuarios que garanticen que los usuarios con acceso al sistema mantienen una relación vigente contractual con la entidad y que sus accesos corresponden con sus funciones.

Recomendaciones Observación No.1 y No.2:

Es indispensable implementar como medida de control y en coordinación con el área de Talento Humano, el monitoreo mensual de usuarios para inactivar inmediatamente aquellos que se han retirado de la entidad, como con el área de Contratación, los que no cuenten con un contrato vigente.

Es necesario identificar, depurar y actualizar los usuarios genéricos y los que no se encontraron dentro de los funcionarios activos como funcionarios de la Entidad, según registros de Talento Humano, o como contratistas vigentes, asegurando que únicamente se tiene permitido el acceso a usuarios con relación contractual vigente con la entidad.

Es preciso revisar, actualizar y divulgar el Manual de Seguridad de la Información estableciendo el tiempo de la revisión de los derechos de acceso de los usuarios, de anual a semestral, teniendo en cuenta que en la actualidad el manual indica que: "*Tanto el responsable del área restringida como el encargado del activo de información deberán realizar* ***al menos una revisión anual*** *(o cuando sea requerido) de los derechos de acceso de los usuarios en intervalos regulares, con el fin de mantener un control eficaz de acceso a los datos y a los servicios de información*." (la negrilla es nuestra).

Consideramos importante incorporar y ajustar lo más pronto posible estas medidas de control en el procedimiento de Administración de Usuarios, incluyendo las actividades de control y responsables de gestionar los usuarios (creación, actualización, bloqueo y/o retiro) para todos los Sistemas de Información existentes en la Entidad, evaluando la posibilidad de implementar un control periódico que, bajo responsabilidad de la OTIC, asegure que las directrices y/o políticas generales aplicables a la administración de usuarios se cumplan para todos los Sistemas de Información de la Entidad, alineado a lo establecido en el Manual de Seguridad de la Información (4204000-MA031) relacionado con la revisión anual de los derechos de acceso y la desactivación de los mismos una vez terminados los vínculos contractuales con la Entidad.

Observación No. 3:

De una muestra de dieciocho (18) usuarios activos que fueron creados en la Base de Datos SI Capital durante el periodo evaluado, no se evidencia formato FT-1000 para trece (13) de ellos. Las siguientes situaciones, implican riesgos de usuarios creados sin autorización y/o sin conocimiento de parte de los niveles aprobadores autorizados, dificultad para establecer responsabilidades en caso de realización de operaciones en cabeza de usuarios que no cuentan con una aprobación de acceso a los Sistemas de Información, cuyo ingreso es controlado por la Base de Datos SICapital:

- Nueve (9) usuarios creados, no cuentan con un caso registrado en la mesa de servicio de la solicitud y aprobación por los niveles jerárquicos adecuados, que soporte el proceso de creación y otorgamiento del acceso del usuario a la base de datos.

- Dos (2) usuarios cuya fecha del registro del caso GLPI en la mesa de ayuda no coincide con la fecha de creación del usuario almacenada en la base de datos.

- Un (1) usuario, que en el caso GLPI se registra como observación, que el FT-1000 se encuentra incompleto y no se evidencia el formato actualizado.

Recomendación:

Desde la OTIC, dar cumplimiento estricto al procedimiento Administración de Usuarios (2213200-PR-185 V08) e implementar un control de revisión, se sugiere se realice por muestreo, para asegurar que todos los usuarios creados tengan un caso de soporte en GLPI (Mesa de Servicios) y el formato FT-1000 debidamente firmado y diligenciado.

Asimismo, se considera necesario definir un campo en la herramienta GLPI de la Mesa de Servicios, para incluir el código de usuario y responsable, con que se crean los usuarios en los sistemas de información.

3. Monitoreo y Generación de Alertas para Servidores y Equipos de Red que Soportan la Operación Tecnológica de la Entidad

Observación No. 4:

Analizada una muestra aleatoria de 148 servidores y 226 equipos de red, se observó que algunos servidores, switches o routers, no hacen parte de los procedimientos de monitoreo que tiene implementados la OTIC bajo la herramienta formal de Nagios. Asimismo, no se evidenció que exista un análisis sobre los servicios soportados por estos equipos de cómputo que permita asegurar que se están monitoreando los de mayor criticidad y asegurar que los que no se monitorean no presentan riesgo de indisponibilidad de servicios sensibles de la Entidad.

Las situaciones aquí presentadas generan riesgo de indisponibilidad de los servicios tecnológicos afectando la operación interna de las áreas o la atención al ciudadano en caso de falla de algún servidor o equipo de red no monitoreados o sin alertas oportunas.

1. Servidores:

De 148 servidores Linux, Windows y en la Nube, para una muestra de diecisiete (17): 5 Linux, 5 Windows y 7 Azure-Nube, correspondiente al 11.5%, presentan las siguientes situaciones:

- Los cinco (5) servidores Windows no están siendo monitoreados por la herramienta Nagios:

Servidor	Software	Dir. IP	Servicio que soporta
Registro_Distrital	Registro_Distrital	No recibida	Proceso de publicación de actos administrativos
Emlaze	Emlaze	172.16.103.70	ERP que lleva la trazabilidad de la producción de la imprenta, contiene módulos de talento humano

Servidor	Software	Dir. IP	Servicio que soporta
ServerInfra.alcaldia	ServerInfra.alcaldia	192.101.4.18	Sistema de gestión contractual, sistema de presupuesto, facturación (cades y supercades)
Liquidador_producción	Liquidador_producción	172.16.101.36	Liquidador de nómima
Firma Digital	Firma Digital	172.20.1.250	Firma digital para líderes de la oficina OTIC

- Los siete (7) servidores Azure, se monitorean con herramientas propias de estos equipos, puesto que aún no se ha definido su inclusión formal al procedimiento PR-273 de Administración de Servidores de la Red de Datos.

Servidor	Software	Dir IP	Servicio que soporta
SG-Drupal01	Infraestructura en donde se alojan los sitios web de Internacional, Víctimas Bogotá y Archivo Bogotá.	10.100.1.4	Sitios web de Internacional, Víctimas Bogotá y Archivo Bogotá.
SG-WebApp01		10.100.1.5	
SG-WebApp02		10.100.1.6	
SG-Nginx01		10.100.1.36	
SG-Nginx02		10.100.1.37	
SG-DB01		10.100.1.4	
SG-DB02		10.100.1.5	

- Dos (2) servidores Linux, siete (7) servidores Azure y cinco (5) Windows, no cuentan con alertas automáticas para detectar oportunamente la indisponibilidad y/o falla del servidor. Cabe resaltar, que para los servidores Windows se evidenció el caso de soporte GLPI # 172654 con fecha 3 de junio de 2020 (generado como resultado de las observaciones preliminares de esta auditoría, comentadas durante el trabajo de campo). Los servidores bajo esta situación son:

Servidor	Software	Dir IP	Servicio que soporta
sigaprod-cluster2	sigaprod-cluster2	172.16.101.133	Sistema SIGA
Sivic_prod	Sivic_prod	172.16.101.90	Sistema SIVIC
Registro_Distrital	Registro_Distrital	No recibida	Proceso de publicación de actos administrativos
Emlaze	Emlaze	172.16.103.70	ERP que lleva la trazabilidad de la producción de la imprenta, contiene módulos de talento humano
ServerInfra.alcaldia	ServerInfra.alcaldia	192.101.4.18	Sistema de gestión contractual, sistema de presupuesto, facturación (cades y supercades)
Liquidador_producción	Liquidador_producción	172.16.101.36	Liquidador de nómima
Firma Digital	Firma Digital	172.20.1.250	Firma digital para líderes de la oficina OTIC
SG-Drupal01	Infraestructura en donde se alojan los sitios web de	10.100.1.4	Sitios web de Internacional, Víctimas Bogotá y Archivo Bogotá.
SG-WebApp01		10.100.1.5	
SG-WebApp02		10.100.1.6	

Servidor	Software	Dir IP	Servicio que soporta
SG-Nginx01	Internacional, Víctimas Bogotá y Archivo Bogotá.	10.100.1.36	
SG-Nginx02		10.100.1.37	
SG-DB01		10.100.1.4	
SG-DB02		10.100.1.5	

- Un (1) servidor Windows que soporta el Registro Distrital de la Imprenta de Bogotá, no cuenta con la Dirección IP identificada por la OTIC, debido a que el servidor se encuentra por fuera de la red de datos administrada por la OTIC, razón por la cual no se evidenció inclusión del servidor en los procesos de monitoreo realizados por la OTIC.

  De acuerdo con lo informado por el área de la Imprenta, el servidor se encuentra ubicado físicamente en la sede Archivo de Bogotá con dirección IP 10.101.93.60 y soporta el sistema de información del Registro Distrital y las publicaciones de los extractos de contratos que se realizaron hasta el año 2012.

2. Equipos de Red:

Para 226 equipos de red (Switches Aruba, Controladoras WiFi, Routers y Switches de Cades y dependencia), se observaron las siguientes situaciones:

- La totalidad de Switches Aruba que son 19 y la totalidad de controladoras Wi-Fi que son 5, se están monitoreando con la herramienta Nagios.

- 124 de 176 equipos Router y Switches, no están siendo monitoreados por la herramienta Nagios; para estos 123 equipos, se identifican diez (10) conexiones que soportan servicios Core del negocio. Para los equipos restantes, no es factible identificar cuáles equipos de red son o no críticos para la operación de la Entidad.

- Analizadas las direcciones IP principales de los Cades y Supercades (archivo Equipos_Red.xlsx, entregado por la OTIC – columna CORE), se evidenció que 19 (73%) de 26 conexiones de Cades no están siendo monitoreadas por Nagios.

- Para dos (2) de una muestra de cuatro (4) equipos de red, si bien se encuentran monitoreados en la herramienta Nagios, no se tienen configuradas alertas automáticas para remitir oportunamente el aviso a los ingenieros sobre una caída o falla en el equipo. Los equipos son: Sw_Aruba_DataCenter Liévano SW 3810M y Archivo de Bogota (AB) – DataCenter.

Recomendación:

Es importante que desde la OTIC se puedan identificar los servidores y equipos de red que soportan los servicios críticos de la entidad, verificar y asegurar que se encuentran configurados en la herramienta de monitoreo Nagios, permitiendo emitir alertas en caso de errores o indisponibilidad de los servidores de forma oportuna, previniendo de manera oportuna una falta de conexión a la red de la entidad, o detectando oportunamente fallas que pudiesen afectar los servicios hacia el ciudadano.

4. Administración de las Bases de Datos

Observación No. 5:

No se cuenta con un inventario de Bases de Datos actualizado que, permita identificar la versión del motor de BD que tiene la entidad implementada y el Sistema de Información que soporta, lo que implica que puedan existir Sistemas de Información en la Entidad que no cuenten con una adecuada gestión y administración de su Base de Datos.

En el procedimiento Administración y Gestión Base de Datos, no se tiene definida una actividad para la programación de restauraciones de bases de datos bajo variables de criticidad, disponibilidad de recursos, tipo de base de datos, entre otros, que permita asegurar la restauración de la totalidad de bases de datos críticas o sensibles durante un período definido, lo que puede ocasionar pérdida de información por daño de los datos resguardados o por falla del medio de almacenamiento.

Recomendación:

Mantener actualizado el inventario de Servidores y Sistemas de Información de la Entidad, de manera que se pueda establecer la totalidad de servidores con los respectivos Sistemas de Información que soporta y las versiones de los sistemas operativos y bases de datos correspondientes, permitiendo asegurar que todas las Bases de Datos que soportan los principales sistemas de Información y servicios de la Entidad están siendo administrados y gestionados de manera adecuada.

En coordinación desde la OTIC y de ser necesario con las áreas de negocio, definir los criterios para programar las restauraciones periódicamente de las Bases de Datos y definir los criterios de cubrimiento y alcance según criticidad de la información y disponibilidad de recursos, asegurando el cubrimiento de la totalidad de bases de datos sensibles de la entidad durante un periodo de tiempo determinado (se sugiere 1 año).

Observación No. 6:

Para una muestra de catorce (14) Sistemas de Información, de treinta y nueve (39) existentes en el PETI (OT-043 Plan Estratégico de Tecnologías de Información PETI), se observó que no se han realizado actualizaciones de los motores de las bases de datos ni aplicación de parches de seguridad, lo cual genera riesgos de vulnerabilidades con afectación de la integridad de la información y posibles fallas debido a que no se cuenta con soporte por parte del proveedor de las bases de datos.

Se resalta lo informado por la OTIC, respecto a que no se han realizado estas actualizaciones debido al riesgo que existe de que las aplicaciones no funcionen y se requiere planificar un proyecto para la migración de los motores de las bases de datos con que cuenta la Entidad a las versiones vigentes del mercado.

Los sistemas de información de la muestra son:

Id PETI	Sistema de Información	Motor Base de Datos	Versión motor BD
1	Tablero de Control Alcalde	Postgres	9.3.10
3	Sistema de contratación a la vista - CAV-2	Oracle	11g
4	Sistema de contratación a la vista - CAV-3	Oracle	11g
5	Sistema Distrital de Quejas y Soluciones - SDQS	Postgres	9.3.16
7	Centro de Documentación del Archivo de Bogotá - WINISIS	BD no administrada por la OTIC*	
8	Sistema Integrado de Gestión del Archivo y Correspondencia - SIGA-	Oracle	11g
12	Sistema de información de Personas Jurídicas SIPEJ	BD no administrada por la OTIC*	
24	Intranet	MySQL	5.5.48
27	Sistema de Información para el Archivo de Bogotá – SIAB	Oracle	9.3.10
28	Sivic Sistema de información de víctimas del Distrito Capital	Postgres	9.3.6
29	Sistema Automático de Turnos - SAT	Postgres	9.3.10
30	Administración de Elementos de Consumo - SAE	Oracle	11g
35	Sistema de Personal y Nómina - PERNO	Oracle	11g
36	Libro Mayor - LIMAY	Oracle	11g

***** Bases de Datos no son soportadas por la OTIC, razón por la cual en esta área no se conoce la base de datos ni versión correspondiente.

Recomendación:

Teniendo en cuenta el alto impacto de realizar migración a las versiones vigentes de los motores de bases de datos y los riesgos de no contar con actualización de parches de seguridad, se recomienda que la OTIC realice un análisis y evaluación técnica para planear e implementar un proyecto asociado a la migración y actualización de los motores de base de datos.

5. Administración de Copias de Respaldo y Restauración

Observación No. 7:

Para una muestra de cuatro (4) Sistemas de Información de treinta y nueve (39) relacionados en el PETI, y 10 fechas (diarios, semanales y mensuales), se evidenciaron las siguientes situaciones que implican posibles pérdidas de información y/o dificultad para recuperarla en caso de una contingencia:

- El servidor “ALCAPPCAV2.alcaldia bogota.gov.co” que soporta la aplicación Sistema de Contratación a la Vista CAV-2, no está siendo respaldado. De acuerdo con lo indicado por la OTIC, no se ha recibido el requerimiento del área funcional Servicio a la Ciudadanía, para incluir este servidor dentro de los que se respaldan periódicamente como parte de los procedimientos de la OTIC.

- La copia de respaldo mensual del 30 de noviembre de 2019 para el servidor "dbracsg01.alcaldia bogota.gov.co", que soporta la base de datos de varios aplicativos (Sistema de contratación a la vista - CAV-2, Sistema de Información para la Administración del Riesgo, Administración de Elementos de Consumo – SAE, Libro Mayor – LIMAY), falló y no se encontró evidencia de la toma nuevamente de la misma.

Recomendación:

Identificar los servidores y activos de información sensibles y de mayor criticidad para la entidad, evaluando criterios objetivos para determinar cuáles de los servidores están siendo respaldados y para cuáles no procede, según los criterios definidos, asegurando que todos los servidores y activos sensibles y de mayor criticidad sean respaldados de forma adecuada.

Observación No. 8:

No se observó una programación periódica de restauraciones de cintas de respaldo que permita asegurar la ejecución trimestral de pruebas de restauración de la información establecida en el procedimiento, como tampoco una planeación que permita determinar la frecuencia con la cual opera la restauración de las bases de datos de información crítica de la Entidad, los recursos requeridos y la cobertura con la que se realizan copias de respaldo para todos los servidores activos en la Entidad, así como la identificación misma de estos servidores, ni una relación completa de la totalidad de servidores de la entidad (población) que permita asegurar el cubrimiento completo de los datos y activos de información de mayor criticidad de la entidad.

Estas situaciones o debilidades de control, posibilitan el riesgo de indisponibilidad de información relevante y/o crítica para la Entidad, a causa de daños en los medios magnéticos o equipos donde residen las copias de respaldo de la información del negocio y que pudiese dañarse con el transcurrir del tiempo o pudiese no ser leída en las nuevas herramientas de backup por ser información respaldada en medios magnéticos antiguos.

Recomendación:

En coordinación entre los diferentes Profesionales de la OTIC (Administrador de copias de respaldo, Administradores de Servidores y Administrador de las Bases de Datos), asegurar de manera inmediata, la planificación de restauraciones periódicas, toma de backups y almacenamiento de los activos de Información sensibles o críticos, y garantizando que todos los servidores de la entidad que gestionan información sensible o crítica cuenten con su programación centralizada de backups bajo la herramienta de copias de respaldo Data Protector administrada por la OTIC.

6. Análisis de Vulnerabilidades para Sistemas Operativos, Bases de Datos y Sitios Web

Observación No. 9:

Se evidenciaron análisis de vulnerabilidades realizados a tres (3) sitios Web de la entidad: Soy10 Aprende, Bogotá Te Escucha y Registro Distrital, por solicitud de las áreas funcionales del negocio, sin contar con una planificación basada en un análisis de criticidad de los servicios de la Entidad para definir cuáles requieren o no este tipo de pruebas de identificación de vulnerabilidades.

Si bien, para el segundo semestre del año 2020 se observa, como parte del Plan de Implementación del Modelo de Privacidad y Seguridad de la Información, una propuesta para ejecutar los Análisis de Vulnerabilidades, el mismo aún no se encuentra aprobado ni formalizado.

Se resalta que una de las actividades del mencionado plan es “Realizar análisis comparativo de servidores y sistemas de información que cuentan con escaneo de vulnerabilidades frente a los faltantes por realizar este proceso”, en donde se identificarán los servidores a los que no se les ha hecho este tipo de pruebas.

Observación No. 10:

Analizados los tres informes de análisis de vulnerabilidad, se evidencian resultados que requieren un plan de atención para cerrar las vulnerabilidades técnicas de seguridad encontradas y clasificadas como críticas, graves o moderadas; sin embargo, no se evidencian planes de remediación aplicados a dos (2) de ellos, y al cierre de la auditoría (12 de junio de 2020) aún no se contaba con un plan de remediación para el cierre de las vulnerabilidades encontradas, lo que significa que persisten los riesgos de accesos no autorizados, posible indisponibilidad del servicio y pérdida o robo de información:

Sitio	Nodo	Sistema Operativo	Nombre Servidor	Fecha	Plan de Remediación
Bogotá Te Escucha	172.16.101.220	Linux 3.11	sdqs-app-cluster1	19/06/2019	No
SOY10 Aprende	172.16.101.100	CentOS Linux 07/06/1810	gamificacion.alcaldia bogota.gov	17/05/2020	Si
Sistema de Información del Registro Distrital	172.16.101.61	Linux 3.11	registrodistrital.secretaria general.gov.co	24/03/2020	No

Recomendación Observaciones No.9 y No.10:

Desde las responsabilidades del Oficial de Seguridad en la OTIC, diseñar y formalizar un plan de análisis de vulnerabilidades, que aparte de pruebas a Sitios Web solicitadas por las áreas funcionales, se realice un análisis tanto de los sitios Web de mayor criticidad como de los servidores que soportan los sistemas y la información de mayor criticidad para la Entidad, definiendo priorización para la ejecución de este tipo de análisis; incluyendo en el plan la ejecución de pruebas de vulnerabilidades para los Sistemas Operativos y las Bases de Datos, análisis significativos que permiten identificar falencias de configuración en los servidores y aplicar parches de seguridad, minimizando riesgos de ataques, indisponibilidad de los sistemas, pérdida o robo de información, entre otros.

7. Mantenimiento Preventivo de Equipos de Cómputo y Servidores

Observación No. 11:

7.1 Equipos de Escritorio, Portátiles, Pantallas, Cámaras

Analizada una muestra de 35 equipos de cómputo de diferentes dependencias (portátiles, computadores de escritorio, pantallas), se observó que para ocho (8) de ellos (correspondiente al 23%) no se les realizó el mantenimiento programado, por las siguientes razones:

- Dos (2) pantallas se encontraban instaladas a más de 1,5 metros de altura, y de acuerdo con lo informado por la OTIC, el contrato con el proveedor MicroData, no tiene clausulado para trabajo en alturas, por lo cual no se realizó el mantenimiento.

- Siete (7) computadores (escritorio, CPU, portátil) que no tienen evidencia del mantenimiento realizado. Las placas de los equipos bajo esta condición son: 54536,30709, 30758, 24918, 32658, 32661, 9642.

- Un (1) computador de placa 24557 tiene formato de evidencia de mantenimiento, sin datos ni firma del usuario que dé cuenta de la ejecución satisfactoria del mantenimiento.

- Para dos (2) de los equipos de cómputo con placa 72133 y 72127, no se evidenció el formato soporte de ejecución del mantenimiento realizado por el proveedor Uniples, debido a que se encuentra físicamente bajo llave en oficina OTIC y debido a la emergencia sanitaria COVID-19 no pudo ser remitido para su revisión.

7.2 Servidores Físicos

A la fecha del cierre de la Auditoría (12 de junio de 2020) no se recibieron soportes que permitieran evidenciar mantenimiento para los servidores físicos. De igual manera, para los equipos de red se informó que no requieren de este mantenimiento porque se encuentran en garantía o porque el proveedor realiza el cambio del equipo o de la parte dañada en caso de falla, sin embargo, no se recibió evidencia que respalde esta condición.

Recomendación:

Definir acciones a seguir para los casos en que el técnico no puede realizar el mantenimiento a los equipos de cómputo, ya sea por su ubicación en altura o porque el usuario no se encuentra. Se sugiere que la OTIC en coordinación con la Subdirección de Servicios Administrativos para que el día en que se realice la visita de mantenimiento, los equipos de altura se ubiquen en un sitio accesible al técnico, y para los casos en que no se encuentra el usuario, avisar al jefe de la dependencia para que se autorice el mantenimiento o se reprograme.

Asegurar que se cuente con un plan de mantenimiento anual para los Servidores Físicos y equipos de red, para estos últimos, en caso que existan algunos que no estén cubiertos por la garantía de cambio del equipo o de la parte en caso de daño o falla, lo cual disminuye el riesgo de fallas inesperadas en los servidores o equipos de cómputo que puedan generar indisponibilidad de los servicios.

8. Administración de requerimientos y casos de soporte en la Mesa de Servicio

Observación No. 12:

Se evidenciaron 10 categorías (campo: Tipo Solicitud) de los registros de solicitudes de la herramienta GLPI, que están categorizadas en tipos de solicitud que no tienen definido un ANS:

Categorías GLPI sin correspondencia en los ANS definidos	Cant. Registros
ADMINISTRATIVAS > MANTENIMIENTO DE EQUIPOS > Aires Acondicionados	1
Base de Datos > Base de Datos	5
Clasifica no	12
Cuentas de Usuario	1
Equipos de Cómputo	1
Impresoras	1
INFRAESTRUCTURA > Configuración y/o Soporte red inalámbrica	40
Otros Equipos	2
SISTEMAS DE INFORMACIÓN	1
SISTEMAS DE INFORMACIÓN > Sistema de Información SIVIC	7
TOTAL REGISTROS GLPI	**71**

Observación No. 13:

De 19.449 casos de soporte registrados en la Mesa de Servicio entre julio 2019 y abril 2020, se identifican 9.745, correspondientes al 50%, que no cumplen con los ANS establecidos (entre 0,25 y 64 horas según la categoría del servicio). De los cuales 6.592, presentan inoportunidad en su solución entre 1 y 284 días, y 3.153 casos entre 1 y 24 horas, generando inoportunidad en la atención del servicio (tiempo transcurrido entre la fecha de registro y la fecha de solución), ocasionando un inadecuado servicio al cliente interno y por consiguiente una mala imagen sobre el servicio ofrecido por la OTIC en la atención a las demás dependencias. A continuación, se relacionan los diez (10) casos con mayores días de inoportunidad en su solución:

ID	Fecha Apertura	Fecha solución	tipo solicitud	Días
137109	2019-07-02	2020-03-17	Impresoras > Asistencia en impresión, capacitación y configuración	258
137482	2019-07-04	2020-01-29	INFRAESTRUCTURA > Permisos a carpetas compartida	208
139332	2019-07-19	2020-03-17	Impresoras > Asistencia en impresión, capacitación y configuración	241
139742	2019-07-23	2020-03-03	INFRAESTRUCTURA > Otros Servicios de Infraestructura	222

ID	Fecha Apertura	Fecha solución	tipo solicitud	Días
139914	2019-07-24	2020-03-03	Servicios Especiales > Solicitudes NO categorizadas	223
141196	2019-08-05	2020-03-04	INFRAESTRUCTURA > Otros Servicios de Infraestructura	211
141198	2019-08-05	2020-05-18	SISTEMAS DE INFORMACIÓN > Sistema de Información SIVIC > Reportes Solicitados	284
141336	2019-08-05	2020-03-04	Equipos de Cómputo > Asistencia equipos de cómputo y capacitación	211
141339	2019-08-05	2020-03-04	INFRAESTRUCTURA > Otros Servicios de Infraestructura	210
141893	2019-08-12	2020-03-03	INFRAESTRUCTURA > Instalación, Configuración y/o deshabilitar puntos de red	203

Recomendación

Fortalecer el proceso de monitoreo, seguimiento y medición de los tiempos de cumplimiento para la solución de los casos de la mesa de servicio de acuerdo con los ANS definidos, de manera que se detecten oportunamente desviaciones y se tomen las acciones correctivas necesarias encaminadas a dar cumplimiento a los ANS y a dar un servicio oportuno al usuario en cumplimiento a los Acuerdos de Nivel de Servicio establecidos con el proveedor de la Mesa de Servicio.

9. Mapa de Riesgos y Controles en el Proceso

Observación No. 14:

Verificada la matriz de riesgos del proceso, se observó que los controles definidos en la misma no son consistentes con los puntos de control de los procedimientos del mismo, lo que afecta el ambiente de control del proceso, al no haber claridad frente a los controles que deben aplicarse en su gestión.

Respecto a los nueve (9) controles definidos en el mapa de riesgos del proceso, se observó que frente a los dos (2) riesgos identificados de: 1) Errores (fallas o deficiencias) en la administración y gestión de los recursos de infraestructura tecnológica y 2) Exceso de las facultades otorgadas durante la Administración y/o gestión de los recursos de la Infraestructura tecnológica de la Secretaria General, no hay diferenciación de los controles que apliquen indistintamente a cada uno de los riesgos, los nueve (9) controles definidos mitigan directamente el riesgo de “Errores (fallas o deficiencias) en la administración y gestión de los recursos de infraestructura” y no directamente al de “Exceso de las facultades otorgadas durante la Administración y/o gestión de los recursos de la Infraestructura tecnológica de la Secretaria General”.

Asimismo, se definen dos (2) controles corresponden a las auditorías a cargo de la OCI, sin que se cuente con actividades de control a cargo del propio responsable del proceso, como encargado en “primera línea” de su óptimo funcionamiento.

Los controles definidos hacen parte de la dinámica diaria de la operación del proceso, sin embargo, requiere fortalecimiento en controles claves de monitoreo como, por ejemplo:

- Depuración periódica de usuarios activos en los Sistemas de Información, Bases de Datos y Servidores.

- Monitoreo periódico sobre los Activos de Información críticos para asegurar que están siendo respaldados.
- Revisión mensual o trimestral de cumplimiento de los ANS en la oportunidad de atención de requerimientos en la Mesa de Servicio.
- Asegurar que todos los equipos informáticos hacen parte del cronograma de mantenimientos preventivos o que no lo requieren por estar en periodo de garantía.

Recomendación:

Con el acompañamiento de la Oficina Asesora de Planeación es importante actualizar lo más pronto posible el mapa de riesgos del proceso, para asegurar la consistencia del mismo frente a los controles aplicados y los establecidos en los procedimientos. Así mismo, considerar la implementación de controles para prevenir eventos de riesgos tales como accesos no autorizados a los Sistemas de Información del Core del Negocio, incumplimiento de ANS en la atención de incidentes y requerimientos tecnológicos, pérdida de información por fallas o daños de los medios de almacenamiento, entre otros.

En instancia del subcomité de autocontrol o las actividades cotidianas de seguimiento al proceso, 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: accesos no autorizados a los sistemas de información, fallas en los equipos de cómputo, daño o destrucción de activos de información.

Plan de Mejoramiento

Producto de la evaluación practicada y resultado del análisis del informe preliminar, la Oficina de Tecnologías de la Información y las Comunicaciones, la Dirección del Sistema Distrital de Servicio a la Ciudadanía y la Oficina Asesora de Planeación, definieron acciones de mejora dirigidas a subsanar tanto las observaciones identificadas como las oportunidades de mejora formuladas, 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