BOGOTÁ | SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

Radicado No. 20201300187933
Fecha: 2020/09/24 10:38:11 AM
Anexos: INFORME FINAL AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN Folios: 1
Asunto: INFORME FINAL AUDITORÍA TECNOLOGÍA
Destinatario: HUGO ACERO VELASQUEZ
Radicador: SILENIA NEIRA TORRES

MEMORANDO

Para:	HUGO ACERO VELASQUEZ DESPACHO SECRETARIO DE SEGURIDAD
De:	SILENIA NEIRA TORRES
Fecha:	Jueves 24 de septiembre de 2020
Asunto:	INFORME FINAL AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN VIGENCIA 2019-2020

Respetado Doctor:

Atentamente, me permito informarle que de conformidad con el Plan Anual de Auditoría aprobado para la vigencia en curso y de conformidad con lo establecido en el Decreto 1008 de 2018, política Gobierno Digital, el Documento CONPES 3854 de 2016, las Normas ISO27001, el Decreto 413 del 30 de septiembre de 2016, artículo 3, literal X, artículo 19, literal F y artículo 26 y demás normatividad, la Oficina de Control Interno realizo la auditoría de gestión de tecnología de la información y sistemas de información de la SDSCJ.

De conformidad con el procedimiento de auditoria establecido para el efecto, se allega el Informe Final Auditoría Tecnología de la Información vigencia 2019-2020.

Con base en los resultados arrojados por el ejercicio auditor, se enviará por correo electrónico, la plantilla con las observaciones correspondientes para la formulación del plan de mejoramiento, el cual debe realizarse en un término de cinco (5) días hábiles a partir de la comunicación de la presente. Para dicha estructuración de acuerdo al procedimiento establecido se contara con el apoyo metodológico de la Oficina Asesora de Planeación.

Sin otro particular, me suscribo gratamente.

Cordialmente,

Radicado No. 20201300187933
Fecha: 2020/09/24 10:38:11 AM
Anexos: INFORME FINAL AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN Folios: 1
Asunto: INFORME FINAL AUDITORÍA TECNOLOGÍA
Destinatario: HUGO ACERO VELASQUEZ
Radicador: SILENIA NEIRA TORRES

SILENIA NEIRA TORRES
OFICINA DE CONTROL INTERNO

Anexos: INFORME FINAL AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN

Copia:
ISABEL.RAMIREZ - PARA SU INFORMACION SE ALLEGA EL INFORME FINAL DE AUDITORIA TI
ISABEL CRISTINA RAMIREZ VILLEGAS

NATALIAA.MUNOZ - PARA LOS FINES PERTINENTES SE ALLEGA EL INFORME FINAL DE AUDITORIA TI
NATALIA ALEJANDRA MUNOZ LABAJOS

DIANA.SANCHEZM - PARA LOS FINES PERTINENTES SE ALLEGA EL INFORME FINAL DE AUDITORIA TI
DIANA LUCIA SANCHEZ MORALES

NOHORA.VILLABONA - PARA LOS FINES PERTINENTES SE ALLEGA EL INFORME FINAL DE AUDITORIA TI
NOHORA TERESA VILLABONA MUJICA

SONIA.ROMERO - PARA LOS FINES PERTINENTES SE ALLEGA EL INFORME FINAL DE AUDITORIA TI
SONIA STELLA ROMERO TORRES

HENRY.VILLAMARIN - PARA LOS FINES PERTINENTES SE ALLEGA EL INFORME FINAL DE

Radicado No. 20201300187933
Fecha: 2020/09/24 10:38:11 AM
Anexos: INFORME FINAL AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN Folios: 1
Asunto: INFORME FINAL AUDITORÍA TECNOLOGÍA
Destinatario: HUGO ACERO VELASQUEZ
Radicador: SILENIA NEIRA TORRES

AUDITORIA TI
HENRY HUMBERTO VILLAMARIN SERRANO

Proyectó: SILENIA NEIRA TORRES

INFORME FINAL
AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN

DIRECCIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN

SECRETARIA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

SEPTIEMBRE DE 2020

TABLA DE CONTENIDO

TABLA DE IMAGENES

1 ANTECEDENTES

Dando cumplimiento al Decreto 413 de 2016, Artículo 3°, literal x, la SDSCJ lidera, orienta y coordina la implementación de las tecnologías de la información y la comunicación estratégica para el fortalecimiento de la Seguridad, Convivencia y la Justicia en el Distrito Capital.

En ese contexto y según el Decreto 1008 de 2018, se establecen los lineamientos generales de la política de Gobierno Digital de MIPG, los cuales deben cumplir las entidades que conforman la administración pública en el país tanto del orden nacional, como territorial y local.

Los componentes de la Política de Gobierno Digital son las líneas de acción que orientan el desarrollo y su implementación a fin de lograr sus propósitos; TIC para el Estado que tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades de ese mismo orden, a través del uso de las Tecnologías de la Información y las Comunicaciones y TIC para la Sociedad la cual fortalece la relación entre el Estado y la sociedad permitiendo la apertura y el aprovechamiento de los datos públicos, el desarrollo de productos y servicios sistematizados de valor público y el empoderamiento de la ciudadana en el diseño de políticas y normas. Son habilitadores transversales de la Política de Gobierno Digital, la Seguridad de la Información, Arquitectura Empresarial y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de sus propósitos.

En virtud de lo anterior, la Oficina de Control Interno, de conformidad con el Plan Anual de Auditoria (PAA), aprobado por el Comité Institucional de Coordinación de Control Interno para el año 2020, realizó la evaluación a la gestión de la tecnología y sistemas de información que operan en la SDSCJ. Las conclusiones del ejercicio auditor se detallan en los siguientes apartes.

2 OBJETIVO GENERAL

- Evaluar el estado de la implementación de la Política de Gobierno Digital, la seguridad digital y los sistemas de información empleados por la SDSCJ frente a los recursos disponibles en la entidad para el cumplimiento de sus objetivos estratégicos.

3 OBJETIVOS ESPECIFICOS

- Evaluar el estado de avance de la implementación de Gobierno Digital, la seguridad digital y políticas relacionadas en el marco del MIPG y Ley de Transparencia.
- Evaluar el modelo de seguridad y privacidad de la información, mecanismo y lineamientos para el manejo adecuado de la información en la entidad.
- Revisión y evaluación de los sistemas de información de la SDSCJ; SICAPITAL (Predis, Opget, Pagos, Limay, Sisco), Siap y los aplicativos propios; Lico, Sidijus–Sicas, Cope y Progressus, desde su funcionalidad, interfase y procedimientos asociados.
- Verificar el cumplimiento de la normativa aplicable relacionada con el objetivo de la auditoria.

- Evaluar las metas del Plan de Desarrollo de la entidad para el periodo 2019 – 2020, relacionadas con el proyecto de inversión 7515 Desarrollo y Fortalecimiento, así mismo la integralidad de las nuevas metas con el Plan de Desarrollo a implementarse a partir del segundo semestre de 2020.
- Evaluar la accesibilidad a la web institucional de la Secretaría.
- Evaluar la matriz de riesgos de seguridad digital, de gestión y de corrupción del proceso relacionada con el objetivo de la auditoría.

4 METODOLOGÍA

La metodología se basó en consultas, análisis de datos, observación, inspección, revisión y confirmación, además, de otras técnicas de auditoría mundialmente aceptadas:

- Análisis de la información recibida de la Dirección de Tecnología y Sistemas de Información.
- Revisión en la intranet de los documentos del proceso de Gestión de Tecnologías de la Información.
- Verificación con el instrumento del MinTIC del avance en la implementación de la política de Gobierno Digital.
- Revisión con el instrumento Modelo de Seguridad y Privacidad de la Información MSPI, del avance en la implementación de la seguridad y privacidad de la información de la entidad.
- Verificación del cumplimiento de las metas TIC en el Plan de Desarrollo de la entidad al 2020, incluyo la evaluación a la gestión contractual desarrollada para el proyecto de inversión 7515
- Revisión de la seguridad y accesibilidad de la información en la Web de la entidad.
- Revisión de la implementación de los controles y los eventos de riesgo de seguridad digital. Evaluación de las matrices de riesgos de seguridad digital, de gestión y de corrupción relacionadas con el proceso objeto de auditoría.
- Aplicación de las pruebas de auditoria de acuerdo con los objetivos específicos propuestos; evaluación de las aplicaciones en las oficinas donde las administran y manejan.

5 ALCANCE

- Evaluar la política de Gobierno Digital, el Modelo de Seguridad de la Información y los sistemas de información seleccionados conforme a los objetivos trazados, durante la vigencia de 2019 y hasta al 30 de abril de 2020.

6 NORMATIVIDAD Y CRITERIOS APLICABLES

- Decreto 413 del 30 de septiembre de 2016, por medio del cual se establece la estructura organizacional y las funciones de las dependencias de la Secretaría Distrital de Seguridad, Convivencia y Justicia y se dictan otras disposiciones.
- Resolución 305 de 2008, por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y *Software* Libre.

- Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Ley 1273, por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado; De la Protección de la información y de los datos.
- Resolución 004 de 2017, por la cual se modifica la Resolución 305 de 2008 de la Secretaría Distrital General.
- Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales.
- Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Conpes 3854 de 2016, Seguridad Digital, consiste en modernizar al país y reaccionar oportunamente ante los riesgos de posibles peligros, en cuanto a infraestructura e información digital.
- Resolución 541 de 2017, por la cual se adopta la política de seguridad de la información y se definen lineamientos para uso, actualización y aplicación de la Secretaría.
- Resolución 645 de 2018, por la cual se adopta la política de seguridad de datos personales de la Secretaría.
- Resolución 851 de 2019, por la cual se adopta la política de seguridad de la información y se definen lineamientos para uso, actualización y aplicación de la Secretaría.
- Manual de Seguridad y Privacidad de la Información MA-GT-01.
- Normas Web NTC 5854, por medio del cual se establecen los requisitos de accesibilidad que son aplicables a las páginas web.
- Manual de Gobierno Digital. Implementación de la Política Gobierno Digital, Min TIC.
- Normas NTC-ISO/IEC 27001, la cual promueve la adopción de un enfoque basado en procesos para establecer, implementar, revisar, operar, hacer seguimiento, mantener y mejorar el Sistema de Gestión de Seguridad de la Información de una organización.

7 FORTALEZAS

- La WEB de la SDSCJ cumple a cabalidad los requisitos de accesibilidad de la Norma Técnica Colombiana (NTC) 5854, con el nivel de conformidad A.
- Los aplicativos, la información y los servicios tecnológicos están protegidos con la implementación de la seguridad perimetral que los monitorea en tiempo real.
- La autenticación centralizada mediante contraseñas seguras, el encriptamiento de la información durante su transferencia, la implementación de llaves criptográficas para ingresar a servidores y equipos también brinda seguridad a la información de la entidad.
- Los 11 contratos del Proyecto de Inversión 7515, Mejoramientos de las TIC para la Gestión Institucional, vigencia 2019 y 2020 asociados al cumplimiento de las metas TIC del Plan de Desarrollo de la Secretaría, y revisados por esta auditoría cumplieron sus objetivos y metas propuestas.
- La administración de usuarios y de todos los módulos de SICAPITAL está centralizada en la DTSI, utilizando una herramienta para copiar o duplicar perfiles de usuarios de acuerdo con las funciones

a realizar por cada funcionario o contratista, lo cual garantiza seguridad de la información y minimiza el riesgo de acceso no autorizado a los aplicativos.

- La auditoría de la base de datos SICAPITAL se lleva acabo con el usuario SHD en la DTSI, en el log se registran todos los movimientos que se aplican en las tablas. A nivel superior de Oracle, también se lleva una auditoría detallada de las acciones en la base de datos. La integridad y seguridad de la información está protegida con este sistema de auditorías.
- Las interfaces o conexión entre los sistemas de información de la entidad funcionan adecuadamente, los aplicativos comparten información en línea para lograr sus metas.
- En los módulos de SICAPITAL no se eliminan los usuarios, se inactivan basados en el reporte de novedad (retiro) por parte del usuario líder funcional, actividad realizada por la DTSI, lo que garantiza la integridad de las bases de datos y la trazabilidad histórica de las operaciones realizadas por cada usuario en la base de datos.
- El sistema de personal SIAP está concebido a la medida para las entidades del Distrito, se ha ido adaptando a los requerimientos por cambios de normatividad y por necesidades de la SDSCJ.
- SIAP cuenta con interoperabilidad con otros sistemas de la entidad como ORFEO, el módulo de contabilidad LIMAY de SICAPITAL, y tiene habilitadas algunas vistas en la INTRANET.
- El módulo PREDIS cuenta con reportes estándar a nivel Distrital, con base en lineamientos de la Secretaría de Hacienda Distrital.
- Los módulos OPGET/PAGOS brindan apoyo óptimo en el control y administración de las ordenes de pagos de la entidad.
- El módulo LIMAY atiende eficientemente la necesidad de información financiera de la entidad y está concebido a la medida para las entidades del Distrito, se ha ido adaptando a los requerimientos por cambios de normatividad y por necesidades de la SDSCJ.
- El módulo COPE, aplicativo Web, responde a los lineamientos del Gobierno Distrital “Promover el uso y aprovechamiento de las TICs para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores”.
- La plataforma COPE permanece operativa 24/7, excepto durante las ventanas de mantenimiento, comparte e integra datos desde RNMC.
- El sistema LICO, aplicativo Web, ofrece resultados óptimos en cuanto a la liquidación de comparendos y registros de cursos de actividad pedagógica.
- En el sistema LICO, la fórmula matemática con la que se liquidan los comparendos está blindada contra cualquier tipo de manipulación.
- En la versión No.2 del sistema PROGRESSUS se implementó un módulo para la estrategia de participación ciudadana.
- El sistema SIDIJUS-SICAS registra, atiende y orienta de manera óptima a los usuarios en las Casas de Justicia y los remite a las diferentes entidades operadoras de justicia, a través del Centro de Recepción e Información (CRI) para promover el acceso a la justicia en la ciudad de Bogotá.

8 OBSERVACIONES

8.1 COMPONENTE AVANCE POLÍTICA GOBIERNO DIGITAL.

8.1.1 POLITICA GOBIERNO DIGITAL

El Decreto 1008 de 2018 establece los lineamientos generales de la política de Gobierno Digital. El nuevo objetivo de esa política es promover el uso y aprovechamiento de las tecnologías de la

información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores que generen valor público en un entorno de confianza digital.

La política de Gobierno Digital se implementa a través de dos líneas de acción que orientan su desarrollo: TIC para el Estado y TIC para la Sociedad; así como de tres habilitadores transversales, que son los elementos que proporcionan la base de la política: Arquitectura, Seguridad de la Información, y Servicios Ciudadanos Digitales.

Imagen 1. Esquema de Gobierno Digital. Fuente Gobierno Digital

MEDICIÓN DEL AVANCE DE LA POLÍTICA GOBIERNO DIGITAL

De acuerdo con las directrices del Ministerio de las TIC el seguimiento y evaluación del avance de la Política de Gobierno Digital se realiza, entre otros, con indicadores de cumplimiento, con base a los criterios de evaluación y seguimiento definidos por el Consejo para la Gestión y Desempeño Institucional.

Estos Indicadores miden el cumplimiento de los habilitadores transversales de la política; *Arquitectura y Seguridad de la Información*.

8.1.2 HABILITADOR TRANSVERSAL - ARQUITECTURA.

AVANCE EN LA IMPLEMENTACIÓN DEL PETI, VIGENCIA 2019 Y 2020. SISTEMAS DE INFORMACIÓN.

8.1.2.1. RETRAZO EN LA IMPLEMENTACIÓN DEL PLAN ESTRATÉGICO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES (PETI), EN CONTRAPOSICIÓN CON LO INDICADO EN EL DECRETO 1008 DE 2018, LO QUE AFECTA LA OPERACIÓN DE ALGUNOS PROCESOS Y GENERA DESCONCIERTO RESPECTO DEL AVANCE REAL DEL PETI PARA LA VIGENCIA 2019.

El auditor evidencio que no se puso en marcha al 100% el sistema de información de bienes, a diciembre de 2019, a esa fecha se encontraba en estado de afinamiento y con la data en proceso de migración, situación que contradice lo manifestado en el instrumento de Gobierno Digital con relación al avance en un 100% del PETI.

Esta condición y estado conllevo a que la entidad continuara con los procesos y controles de bienes con las herramientas que venía utilizando y perdiendo la oportunidad de escalar a una tecnología más avanzada, de igual forma, exponiéndose a pronunciamientos negativos por parte de los entes de control.

Igualmente, el ejercicio auditor corroboró que, a comienzos del año en curso, se concertaron compromisos entre la DTSI y la Dirección de Bienes para terminar de migrar la data faltante de los módulos del sistema y para garantizar la puesta en producción del aplicativo, pero solo hasta mayo de 2020, se evidencio que el SIB comenzó a operar con 4 módulos, aplazando los restantes a julio de 2020.

Los auditados expresan que para la vigencia 2020 el PETI, ha alcanzado un porcentaje de avance del 70%, con la ejecución de proyectos, celebración de contratos y otras actividades en los 6 componentes del PETI hasta esa fecha. El equipo auditor procede a corroborar la información, en el documento allegado por la DTSI: "***Alineación PETIC a 2020 V.5 20200731-1***", una vez revisadas las evidencias correspondientes, se concluye que cumplen con lo registrado por esa Dirección en la pregunta PR03 del instrumento de Gobierno Digital, vigencia 2020.

Frente a lo anterior, el artículo 2.2.9.1.3.4 del Decreto 1008, establece que el responsable de liderar la implementación de la Política de Gobierno Digital es el director, jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, de la respectiva entidad.

Corrobora el criterio anterior, el Decreto 413 en el artículo 26, literal B que establece "A*poyar el uso de las TIC y la gestión del conocimiento****".***

RESPUESTA DEL AUDITADO

Con el ánimo de poner en contexto la salida a producción del sistema de Bienes se deben tener en cuenta los siguientes aspectos fundamentales:

> *"El sistema de Bienes se publicó en ambiente de producción en diciembre de 2019 con la totalidad de los módulos en funcionamiento así:*
>
> *COMODATOS*
> *ADMINISTRACIÓN Y RECLAMACIÓN DE SEGUROS*
> *SEMOVIENTES*
> *INFRAESTRUCTURA*
> *MANTENIMIENTO*
> *COMBUSTIBLE*
> *APOYO TIC*
> *CASOS*

Lo anterior permite verificar que el 100% del sistema de Bienes quedó habilitado en el ambiente de producción para que el área usuaria, la Dirección de Bienes, como dueña y responsable de parametrizar y cargar la información de los bienes entregados en comodato a las agencias, iniciará la operación del sistema. Es importante mencionar que la primera versión en producción quedó publicada en agosto de 2019 (Ver acta de cierre del proyecto), y en diciembre de 2019 se realizó una actualización de la versión en producción. Adicionalmente y con el propósito de apoyar el uso y apropiación del sistema, en enero de 2020 se realizó un plan de trabajo con la Dirección de Bienes para el cargue de la data y realización de actividades pendientes (ver acta 20200116 - Acta Seguimiento proyecto bienes), en donde se puede observar que el sistema estaba en producción y cuáles eran las actividades pendientes a esa fecha; así mismos, en el acta (20200122 - Acta Seguimiento BISEC- SI BIENES) se evidencia que nuevamente se realiza un plan de trabajo para obtener el cargue de la data y poder realizar la salida oficial a producción. (ver planes de trabajo para cumplimiento de la Dirección de Bienes).

Es de anotar que, el sistema de Bienes cuenta con la funcionalidad para el cargue de data por parte de los usuarios finales, en la opción administración de datos/configuraciones avanzadas.

a. *Partiendo del hecho que la carga y parametrización inicial de la data es una tarea que está en cabeza de la Dirección de Bienes, según consta en las actas, la Dirección de Tecnologías y Sistemas de la Información ha realizado actividades de acompañamiento y monitoreo con el fin de asegurar que la información necesaria para la operación del sistema cumpla con las condiciones mínimas requeridas. En este mismo sentido vale la pena mencionar el estado actual del cargue de la data al 31 de agosto donde se evidencia que aún hay un remanente de información pendiente por cargar (ver acta 31082020 Reunión SEGUIMIENTO BIENES):*

Comodatos: 100%
Semovientes: 90%
Infraestructura: 80%
Movilidad - Mantenimiento: 80% Apoyo tecnológico: 80%
Combustible: 95%

b. *La Dirección de Bienes envió comunicación a la Dirección de Tecnologías y sistemas de la Información, en la cual nos informa que acordó la concertación de un plan de mejoramiento para entregar el 100% de la data cargada para el día 30 de septiembre. (Se anexa plan de trabajo concertado y respuesta entregada a la Oficina de Control Interno por parte de la Dirección de Bienes, en el marco de la auditoría realizada a esa Dirección).*

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada PETI /8.1.2.1 EVIDENCIAS PROYECTO BIENES, que se ubica en el siguiente enlace:

https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FPETI

En el siguiente enlace https://cutt.ly/9fbb5Ge está disponible el instrumento de seguimiento al Plan Estratégico de TI con corte a 30 de junio del 2020. Por cada uno de los componentes y proyectos que están planteados en la matriz se documentaron los logros obtenidos y las posibles dificultades encontradas en la consecución de las metas.

Con este soporte se evidencia que para las metas establecidas en el PETI se ha dado cumplimiento y seguimiento a cada una de ellas, y se demuestra que las soluciones tecnológicas que soportan los procesos y procedimientos de la Secretaria han operado prestando los servicios para lo que fueron concebidas.

De otra parte, con el fin de lograr un mayor cumplimiento a los compromisos adquiridos para la vigencia 2020 por parte de la Dirección de Tecnologías y Sistemas de la Información, actualmente nos encontramos ejecutando algunas acciones y estructurando planes de trabajo en los frentes de: Gobierno de TI, Sistemas de Información, Servicios Ciudadanos Digitales, Servicios Tecnológicos y, Uso y Apropiación como insumo para la formulación del Plan Estratégico de TI para el próximo cuatrienio, el cual estará orientado a la planificación de acciones y proyectos que contribuyan a la de transformación digital de la Entidad.

En virtud de lo expuesto, respetuosamente manifestamos al Equipo Auditor no estar de acuerdo con la observación realizada y por ende solicitamos sea retirada del informe final.

RESPUESTA OCI

Para brindar respuesta al equipo auditado, es necesario aclarar, que de hecho, el Sistema de Información de Bienes – SIB quedó en estado funcional y listo para entrar en producción a finales de 2019 pero NO entro a funcionar o no se dejó en plena producción cada uno de los módulos del sistema, lo cual solo se evidenció, en parte, hasta mayo de 2020, es decir, NO se cumplió por parte de la Dirección de Bienes y la Dirección de Tecnológica y Sistemas de Información la meta trazada a finales de 2019, para lo cual fijaron un cronograma de actividades a principios de este año, "***20200122 - Acta Seguimiento BISEC- SI BIENES***" pero nuevamente, el objetivo no se logró y fue postergado para una nueva fecha. En dicha acta se evidencia que las actividades contempladas recaían bajo la responsabilidad de ambas direcciones.

En las actas con fechas del 29 de mayo y 18 de junio de 2020, allegadas a la OCI por parte de la DTSI y la Dirección de Bienes, se evidencio, en la primera, que solo entre el 19 y 27 de mayo los ingenieros de la DTSI lograron poner en producción los módulos de Comodatos, Combustible, Administración de Seguros, Semovientes y Casos, quedando así oficialmente estos cinco módulos en funcionamiento, e igualmente, se afirma por los participantes de las dos direcciones, en la segunda acta, que: "***Hoy 18 de junio aún se encuentra en depuración y actualización la data de los módulos de Infraestructura, Movilidad y Apoyo tecnológico, no ha sido dejado en funcionamiento porque se está en la labor de depuración y actualización de la data***", en esta acta se estableció el compromiso que al 3 Julio estos últimos módulos quedaran en funcionamiento. Dado lo anterior, se corrobora lo

anterior, en el documento que también allegaron a la OCI titulado "***Cronograma de Actividades del sistema BISEC -Bienes Secretaria- (Dynamics 365)***", donde se afina un derrotero para lograr el 100% en producción del SIB, a partir del mes de mayo y hasta el 3 de julio de los corrientes, la mayoría de las actividades en ese cronograma quedaron bajo la responsabilidad de los ingenieros de la DTSI. Se concluye y evidencia que el SIB no quedó habilitado en producción a finales de 2019. Se mantiene la observación con relación al incumplimiento en el avance de un 100% del PETI a 2019.

En cuanto al avance de la ejecución del PETI a junio 2020, la DTSI allegó el documento "***Alineación PETIC a 2020 V.5 20200731-1***", revisadas las evidencias correspondientes, cumplen con lo registrado por esa dirección en la pregunta PR03 del instrumento de Gobierno Digital, vigencia 2020. Dicho lo anterior, se reestructura la redacción que brinda sustento a la observación, retirándose el aparte inicial del informe final de auditoría. Los demás aspectos deben verificarse a través del plan de mejoramiento que debe formularse para el efecto.

CAPACIDADES DE ARQUITECTURA EMPRESARIAL VIGENCIA 2019 y 2020.

8.1.2.2. DEBILIDAD EN LA IDENTIFICACIÓN, DESARROLLO Y EJECUCIÓN DE LAS CAPACIDADES NECESARIAS PARA REALIZAR EJERCICIOS DE ARQUITECTURA EMPRESARIAL EN CONTRAPOSICION CON LO INDICADO EN EL DECRETO 1008 DE 2018, GENERANDO RIESGOS EN CADA UNO DE LOS COMPONENTES DE LA ARQUITECTURA MISIONAL DE LA ENTIDAD.

Durante el ejercicio auditor se recibió respuesta del proceso; ***"Se encuentra pendiente la identificación de las capacidades necesarias para realizar ejercicios de Arquitectura Empresarial, hacer uso de una metodología de Arquitectura Empresarial para el diseño y planeación de las iniciativas de tecnologías de información".***

Con esta apreciación, la auditoría corroboró que la entidad no cuenta con un modelo de arquitectura empresarial definido y estructurado en todos sus componentes; misional, sistemas de información, procesos, datos y servicios tecnológicos, solo se evidencia avances en cada uno de ellos, lo que podría conllevar a fallas y poner en riesgo el buen funcionamiento de la estructura organizacional de la entidad.

Lo anterior no está en concordancia con el Decreto 1008 de 2018, artículo 2.2.9.1.2.2. Manual de Gobierno Digital que indica que, para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital.

El Manual en el Numeral 3 Ejecutar la política, 3.3 Lineamiento de los Habilitadores, Arquitectura, establece "*este habilitador busca que las entidades apliquen en su gestión un enfoque de arquitectura empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI".*

RESPUESTA DEL AUDITADO

Si quien bien es cierto que la Secretaría durante la vigencia 2019 adelantó unas acciones preliminares tendientes a contar con un Modelo Base de Arquitectura Empresarial, para la vigencia 2020 se determinó priorizar acciones particulares en frentes como: documentación de los lineamientos definidos en cada uno de los componentes del modelo de gestión y gobierno de

TI establecidos en la Política de Gobierno Digital, tal y como lo reconoce el Equipo Auditor en la sección de FORTALEZAS. Adicionalmente desde la creación de la Secretaría, la Dirección de Tecnologías y Sistemas de Información ha venido realizando avances en el tema, tal y como se relacionan a continuación:

- **Componente Estrategia de TI:**

Nombre de soporte	Enlace de consulta soporte
Plan estratégico de TI	https://cutt.ly/Efv7I5m
Gobierno de TI	https://cutt.ly/nfv7vDr

- **Componente de Gobierno de TI:** los avances realizados por la Dirección en este componente están asociados con: caracterización del proceso de Gestión de Tecnologías de la Información, formulación de 17 procedimientos y formulación de 3 políticas, formulación de 3 planes y formulación de un manual asociado a seguridad y privacidad de la información, lo antes mencionado se encuentra publicado en la sección de Transparencia y Acceso a la Información Pública del sitio web de la Entidad, específicamente en los enlaces: https://scj.gov.co/es/transparencia/organizacion/procesos-y-procedimientos, y https://scj.gov.co/es/transparencia/planeacion/pol%C3%ADticas-lineamientos-manuales

- **Componentes Información:**

Nombre de soporte	Enlace de consulta
Documento de análisis de estrategia y arquitectura de datos	https://cutt.ly/1fv5F09
Documento metodológico para el aseguramiento de la calidad del dato	https://cutt.ly/2fv5kV4

- **Componente sistemas de información:**

Nombre de soporte	Enlace de consulta soporte
Políticas de desarrollo de software seguro	https://cutt.ly/vfbEFXE
Catálogo de sistemas de información	https://cutt.ly/OfbMK5i
Procedimiento de ciclo de vida de desarrollo	https://cutt.ly/mfv5ZMt

- **Componente de servicios tecnológicos:**

Nombre de soporte	Enlace de consulta soporte
Catálogo de servicios tecnológicos	https://cutt.ly/kfbTTmZ
Inventario IPV6	https://cutt.ly/Qfv5wkD

- **Componente de uso y apropiación:**

Nombre de soporte	Enlace de consulta
Procedimiento de uso y apropiación	https://cutt.ly/3fv7saa
Plan de capacitaciones de uso y apropiación para	https://cutt.ly/mfv7tVk

el año 2019	
Evaluación de satisfacción de usuarios	https://cutt.ly/Lfv46sK

- **Seguridad y privacidad de la información:**

Nombre de soporte	Enlace de consulta
Plan de seguridad de la información	https://cutt.ly/WfbFHvn
Plan de tratamiento del riesgo	https://cutt.ly/0fbFO1m

Si bien es cierto la Dirección de Tecnologías de Sistemas de Información no tiene un documento denominado Plan de Aseguramiento de la calidad de la Información, el aseguramiento de la calidad de los datos es un objetivo inmerso en el procedimiento de Ciclo de Vida de Desarrollo de Software PD-GT 17; en la sección "Descripción del procedimiento" en las actividades número 6 "Realizar diseño detallado" y en la actividad número 7 "Codificar requerimientos", teniéndose como resultado su aplicación, lo consignado en el formato en Excel de aseguramiento de la calidad de cada sistema de información desarrollados en la entidad. En conclusión, se puede evidenciar que el aseguramiento de la calidad del dato se encuentra inmerso en el procedimiento de Ciclo de Vida de desarrollo de software PD-GT 17, tal como lo reconoce la auditoría misma en la sección de FORTALEZAS.

Adicionalmente, la Oficina de Análisis de la Información y Estudios Estratégicos, de manera permanente realiza labores que fortalecen la calidad del dato de cada uno de los sistemas de información que posee la Entidad en ambiente de producción aplicando el Documento metodológico para el aseguramiento de la calidad del dato, con el insumo entregado por la Dirección de Tecnologías y Sistemas de la Información, realizando la evaluación de la especificación de datos registrados en el insumo mencionado. Los resultados de esta evaluación son analizados por la Dirección de Tecnologías y Sistemas de la Información para la toma de las acciones necesarias, corregir las inconsistencias evidenciadas cuando son identificadas y lograr una mejora continua en la puntuación de esta evaluación. El resultado de este proceso se puede evidenciar en el repositorio de la Dirección de Tecnologías y Sistemas de la Información, por ejemplo, en los sistemas LICO, PROGRESSUS Y SUME.

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada PETI, que se ubica en el siguiente enlace:

https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FPETI

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

Durante la ejecución de la auditoria se identificaron avances en ejercicios de arquitectura empresarial para la vigencia 2019, tal como se observa en el documento "***E-F2-AED-20190208 v3***"

con relación a Arquitectura Misional, igualmente, en el documento "***Alineación PETIC a 2020. V.5 20200731-1***", pestaña "***PETIC-2019***", "***Componente 1. Estrategia TI, Diseño e Implementación de Arquitectura Empresarial (AE)***", se evidencian acciones ejecutadas al respecto, pero en el mismo documento en la pestaña "***PETIC-2020***", no se evidencia avance alguno en Arquitectura Empresarial, como se observa en la siguiente imagen:

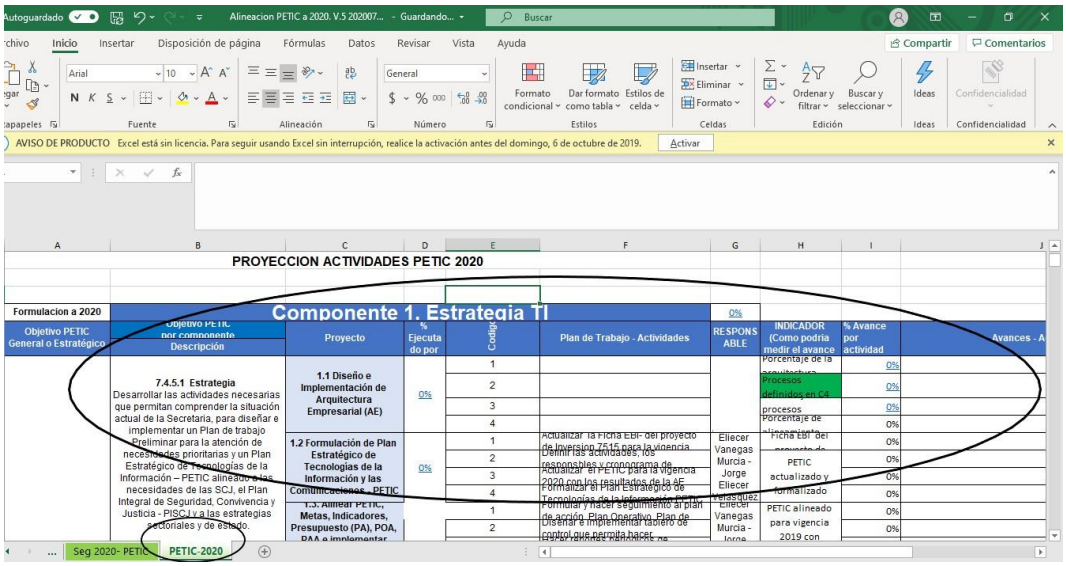


Imagen 2. Documento: Alineación PETIC a 2020. V.5 20200731-1. Fuente DTSI

La mayoría de las evidencias allegadas por la DTSI resultan oportunas para demostrar el avance en la vigencia 2019, pues las actividades representan avances en los componentes *de Gobierno de TI, Gestión de Información, Sistemas de Información, Servicios Tecnológico y Uso y Apropiación,* sin embargo, para la vigencia 2020, aún que se están priorizando acciones de documentación como el Plan de seguridad de la información y Plan de tratamiento del riesgo, no se logra visualizar la implementación de un modelo base e integral de Arquitectura Empresarial, tal como lo exige el ítem PR04 del instrumento de medición de avance en la implementación de Gobierno Digital.

Reiteramos que la respuesta del proceso durante el ejercicio auditor sobre esta pregunta para la vigencia 2020; fue, "***Está pendiente la identificación de las capacidades necesarias para realizar ejercicios de Arquitectura Empresarial…"***

En consecuencia, debe mantener la observación, a fin de brindarle tratamiento a través de un plan de mejoramiento que permita verificar de forma sistémica el avance en su implementación para la vigencia que nos ocupa.

CALIDAD DE LOS COMPONENTES DE INFORMACIÓN VIGENCIA 2019 Y 2020.

8.1.2.3. FALENCIA EN LA MEDICIÓN Y DEFINICIÓN DE UN PLAN PARA EL ASEGURAMIENTO DE LA CALIDAD DE LA INFORMACIÓN, INCUMPLIENDO EL DECRETO

413 Y PONIENDO EN RIESGO LOS RESULTADOS DE TODAS LAS OPERACIONES, ACTIVIDADES Y GESTIONES QUE DEPENDAN DE UNA INFORMACIÓN ESTRUCTURADA, CONFIABLE Y ÓPTIMA.

La calidad de la información es transversal a todos los procesos tecnológicos y administrativos; sistemas de información, bases de datos, información contractual en la entidad y demás, sin un plan que la asegure representa un riesgo en la generación de resultados financieros, administrativos, operativos, técnicos y en la toma de decisiones.

Con lo anterior se incumple, el artículo 26, literal f, del Decreto 413, ***"Impartir lineamientos tecnológicos de estándares de seguridad, privacidad y calidad y oportunidad de la información".***

RESPUESTA DEL AUDITADO

Teniendo en cuenta que la calidad de la información es transversal en la Secretaría, la Oficina de Análisis de Información y Estudios Estratégicos (OAIEE) ha liderado desde el 2019 el análisis de la calidad del dato mediante una metodología, operativa y sistemática, para realizar el aseguramiento de la calidad a las bases de datos. Con esta metodología se pretende:

1. *Entender y documentar la calidad y confiabilidad de los datos.*
2. *Descubrir en los datos los problemas de calidad o detectar las inconsistencias durante los procesos de preparación y carga hacia el Data WareHouse(DWH).*
3. *Asegurar la armonización, estandarización e integración de los datos comunes en las diferentes operaciones estadísticas.*
4. *Especificar las reglas de transformación y validación que deben aplicarse a los datos, para asegurar el nivel de calidad que se requiere en una migración hacia el DWH.*
5. *Cuantificar y documentar los tipos de defectos en los datos.*

Para seguir ésta metodología, la Dirección Tecnologías y Sistemas de la Información genera el formato de calidad mencionado en el procedimiento PD-GT-17 Ciclo de Vida de Software el cual fue desarrollado y entregado por la OAIEE. Una vez este formato, que está relacionado dentro del procedimiento, es diligenciado y entregado nuevamente a la OAIEE, esa Oficina continúa con los siguientes pasos, los cuales permitirán generar un ciclo de mejora continua para producir datos con mayor calidad, que minimizan el riesgo de generar resultados erróneos para la toma de decisiones.

1. *Especificación de reglas de validación.*
2. *Traducción informática de las reglas de validación*
3. *Ejecutar el proceso de evaluación de la calidad de las bases de datos.*
4. *Análisis de resultados de la evaluación de la calidad de las bases de datos*
5. *Informe de hallazgos y recomendaciones.*

Durante el 2019 e inicios del 2020 se desarrollaron estas actividades para los sistemas de SIDIJUS –SICAS, LICO, COPE y PROGRESUS.

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada Sistemas de Información, que se ubica en el siguiente enlace:

https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FSistemasdeInformaci%C3%B3n

RESPUESTA OCI:

Se evidencia en la documentación allegada, que la DTIS ha adelantado conjuntamente con la Oficina de Análisis de Información y Estudios Estratégicos acciones muy valiosas frente a la calidad del dato mediante una metodología, operativa y sistemática, para realizar el aseguramiento de la calidad a las bases de datos para los sistemas de SIDIJUS –SICAS, LICO, COPE y PROGRESUS a 31 diciembre del 2019, pero no ha definido, documentado, ni implementado un plan integral de calidad de la información en la entidad. No se evidencia ninguna documentación al respecto.

De hecho, la respuesta del proceso a esta pregunta del instrumento de medición del avance de Gobierno Digital para la vigencia 2020, fue: "***Se encuentra pendiente realizar la medición de la calidad de la información***" y "***no se había establecido el Plan de Aseguramiento de la Calidad de la Información***". Dado lo anterior, debe mantenerse la observación, a fin de que se establezca un plan de mejoramiento que permita evidenciar el registro de los avances en la implementación del plan integral de calidad de la información.

CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN VIGENCIA 2019 Y 2020.

8.1.2.4. DEBILIDAD EN LAS FUNCIONALIDADES DE ACCESIBILIDAD QUE INDICA LA POLÍTICA DE GOBIERNO DIGITAL, EN LOS SISTEMAS DE INFORMACIÓN DE ACUERDO CON LA CARACTERIZACIÓN DE USUARIOS, EN CONTRAPOSICIÓN CON LO INDICADO EN EL DECRETO 1008 DE 2018 Y AFECTANDO LOS CONTENIDOS DE LOS SERVICIOS DIGITALES QUE DEBEN GARANTIZAR UNA COMUNICACIÓN ADECUADA Y CON CALIDAD.

La entidad no cumple con el diseño integral en el desarrollo de sus proyectos y por el momento no incorpora los principios de diseño de servicios digitales; accesibilidad y usabilidad de acuerdo con la caracterización de usuarios, ciudadanos y grupos de interés de la entidad.

La falta de pruebas de accesibilidad y usabilidad con los usuarios y su caracterización para acceder a los contenidos de las páginas web, portales web y sistemas de información web, genera un riesgo en la efectividad y eficiencia de los servicios e información que se brindan a través de estos medios y afecta los resultados de impacto y calidad esperados.

Frente a lo anterior, el Decreto 1008 de 2018, artículo 2.2.9.1.2.2. Manual de Gobierno Digital indica que, para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital.

El Manual en el numeral 3 Ejecutar la Política, 3.2 Lineamientos TIC para el Estado y TIC para la Sociedad, Principios de Diseño de Servicios Digitales: Accesibilidad y Usabilidad, establece **"*De acuerdo con la caracterización de usuarios, ciudadanos y grupos de interés de la entidad, la infraestructura existente debe garantizar que las páginas web, portales web y sistemas de información web con sus respectivos contenidos, cuenten con características técnicas y funcionales que permitan al usuario percibir, entender, navegar e interactuar adecuadamente".***

RESPUESTA DEL AUDITADO

Para dar respuesta a la afirmación donde nos indican "La entidad no cumple con el diseño integral en el desarrollo de sus proyectos y por el momento no incorpora los principios de diseño de servicios digitales; accesibilidad y usabilidad de acuerdo con la caracterización de usuarios, ciudadanos y grupos de interés de la entidad.", se debe tener claro qué servicios se están prestando a través de las soluciones tecnológicas implementadas, cuál es el objetivo que se está cumpliendo y cuáles fueron las condiciones en las que se desarrollaron, con el fin de evaluar las experiencia de usuario en su ejecución.

En lo que respecta con los aplicativos PREDIS, OPGET, PAGOS, LIMAY, y SISCO que hacen parte de SI CAPITAL, es importante mencionar que éstos fueron adquiridos a través de un convenio interadministrativo con la Secretaria Distrital de Hacienda, y el sistema de información SIAP fue adquirido a través de un convenio suscrito con la Secretaria Distrital de Gobierno, soluciones sobre las cuales se adoptaron las funcionalidades, características de diseño y estándares seguridad definidos por las entidades mencionadas, cumplimiento sus lineamientos y necesidades del momento, sin estar vigente lo indicado en el Decreto 1008 de 2018., época para la cual no existía el Manual de Gobierno Digital, donde se establece las mejores prácticas a tener en cuenta con respecto a usabilidad y accesibilidad.

Por otra parte, las modificaciones que se han realizado sobre dichas soluciones obedecen a cambios en la normatividad y necesidades operativas de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Estos sistemas tienen un uso exclusivo de ciertas áreas, dada la experticia que se requiere para el análisis y uso de los datos que se consolidan allí. Adicionalmente, desde hace varios meses se ha estado a la espera de los lineamientos que sobre el ERP SiCapital se impartan por parte de la Secretaría Distrital de Haciendo a propósito de la implementación del nuevo ERP BogData, que podría llevar a la migración paulatina a dicho nuevo ERP por parte de todas entidades del Distrito, razón por la cual no se ha considerado invertir esfuerzos en cambios al diseño sobre el ERP actual.
En lo que respecta con las soluciones, LICO, SIDIJUS-SICAS, COPE y PROGRESUSS se crearon a partir de los requerimientos realizados por las áreas funcionales y las pruebas finales de aceptación de estos sistemas fueron realizadas por cada grupo funcional, validando el cumplimiento de los requerimientos solicitados y la accesibilidad a la herramienta y solo cuando el usuario funcional dio aceptación, se pasaron a producción los sistemas o sus respectivas modificaciones.

Dado que en esta observación también se contempla el sitio web, es importante reiterar la fortaleza que el Equipo Auditor evidenció, indicando que cumple a cabalidad los requisitos de accesibilidad de la Norma Técnica Colombiana (NTC) 5854, con el nivel de conformidad A.

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada Sistemas de Información, que se ubica en el siguiente enlace:

https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FSistemasdeInformaci%C3%B3n

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

De acuerdo con los Lineamientos y Recomendaciones para el Diseño e Implementación del Sistema de Información y Aplicativos web, "***la accesibilidad web significa que personas con algún tipo de discapacidad van a poder hacer uso de la web, en concreto, al hablar de accesibilidad web se está haciendo referencia a un diseño web qué va a permitir que estas personas puedan percibir, entender navegar e interactuar con la web aportando a su vez contenidos. Algunos tipos de discapacidad; visuales, auditivos, físicos, cognitivos, neurológicos y del habla"***.

En este contexto, la Web de la Secretaría ha logrado el nivel A, el mínimo, y cumple con todos los criterios de conformidad de este nivel de accesibilidad, tal como lo evidenció el grupo auditor.

Sin embargo, en lo que respecta a los aplicativos misionales, LICO, SIDIJUS-SICAS, COPE y PROGRESUSS, independientemente del cumplimiento de los requerimientos solicitados por los usuarios funcionales a la DTSI, es indispensable definir la caracterización de usuarios para desarrollar funcionalidades de accesibilidad que indica la Política de Gobierno Digital.

La respuesta del proceso informa que "***Esta caracterización y las mejoras se realizaran durante la vigencia 2020***". Dado lo anterior, se hace absolutamente necesario, mantener la observación para estos aplicativos tipo Web, a fin de brindarle tratamiento a través del respectivo plan de mejoramiento.

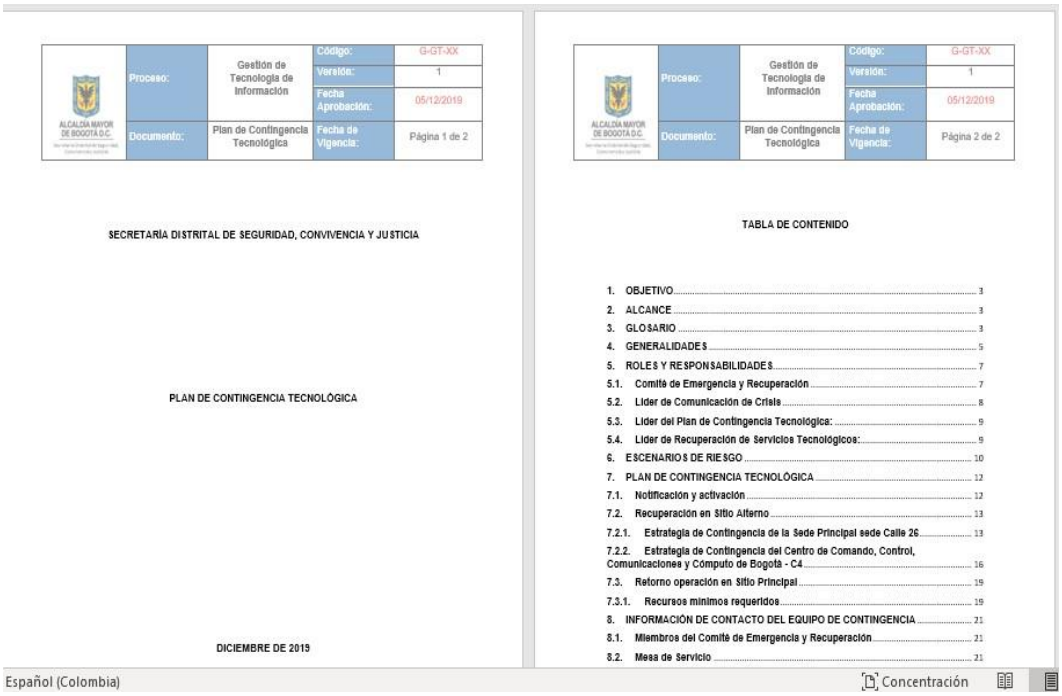
OPERACIÓN DE SERVICIOS TECNOLÓGICOS VIGENCIA 2019 Y 2020.

8.1.2.5. DEBILIDAD EN LA CONFORMACIÓN DE UN PLAN DEFINITIVO, CODIFICADO Y APROBADO DE CONTINUIDAD DE LOS SERVICIOS TECNOLÓGICOS, INCUMPLIENDO LA RESOLUCIÓN 851 DE 2019, LO QUE REPRESENTA UN RIESGO Y DIFICULTAD PARA LA RECUPERACIÓN DE LA OPERACIÓN ANTE DESASTRES TECNOLÓGICOS.

Conforme a lo establecido en la Política de Seguridad de la Información, artículo 17 Seguridad en la Gestión de la Continuidad del Negocio, ***"La SDSCJ deberá disponer de un plan de continuidad del negocio y a través de la DTSI de un plan de recuperación ante desastres tecnológicos – DRP, con el fin de mantener la funcionalidad, confidencialidad, integridad y disponibilidad de los recursos tecnológicos misionales que sean considerados críticos para la continuidad de la operación en la entidad de manera aceptable".***

No contar con una gestión oportuna y eficiente de continuidad del negocio, expondría a la entidad, a incurrir en improvisaciones que puede generar pérdida de información trascendental para la entidad y riesgos asociados con la disponibilidad e integridad de la información, ante situaciones del azar apremiantes y que no brindan posibilidad de respuesta inmediata.

Sin un plan de continuidad de los servicios tecnológicos aprobado, implementando pruebas y verificaciones de la seguridad de la información y acorde a las necesidades de la organización, determinando los riesgos asociados a la infraestructura y servicios tecnológicos, la entidad está en riesgo en caso de una catástrofe o falla general de toda la plataforma tecnológica.



ALCALDÍA MAYOR DE BOGOTÁ D.C.	Proceso:	Gestión de Tecnología de Información	Código:	G-GT-XX
			Versión:	1
			Fecha Aprobación:	05/12/2019
	Documento:	Plan de Contingencia Tecnológica	Fecha de Vigencia:	Página 1 de 2

SECRETARÍA DISTRITAL DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

PLAN DE CONTINGENCIA TECNOLÓGICA

DICIEMBRE DE 2019

ALCALDÍA MAYOR DE BOGOTÁ D.C.	Proceso:	Gestión de Tecnología de Información	Código:	G-GT-XX
			Versión:	1
			Fecha Aprobación:	05/12/2019
	Documento:	Plan de Contingencia Tecnológica	Fecha de Vigencia:	Página 2 de 2

TABLA DE CONTENIDO

Imagen 3. Borrador Plan de Contingencia Tecnológica. Fuente DTSI

RESPUESTA DEL AUDITADO

El nivel de madurez tecnológico alcanzado en la Entidad actualmente se refleja en la consolidación de toda la plataforma tecnológica y con el propósito de alcanzar un mayor nivel, la Dirección de Tecnologías y Sistemas de la Información trabaja en la actualidad en la formulación del plan de continuidad de TI para el cuatrienio del 2020 al 2024, el cual se proyectará contemplando los requerimientos de servicio, recursos y presupuesto asignado.

Como complemento a lo anterior, la Dirección cuenta con el procedimiento implementado del comité de cambios, el cual tiene como objetivo definir las actividades de planeación, evaluación, aprobación, implementación y documentación de la gestión de cambios tecnológicos que permita controlar el ciclo de vida de estos, con el fin de reducir el impacto y minimizar la interrupción de los servicios.

En este sentido y siguiendo lo que contempla el plan en elaboración, las principales aplicaciones y herramientas tecnológicas de la entidad están alojadas en la nube, bajo esquemas de alta disponibilidad, monitoreo y escalamiento.

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada Servicios Tecnológicos, que se ubica en el siguiente enlace:

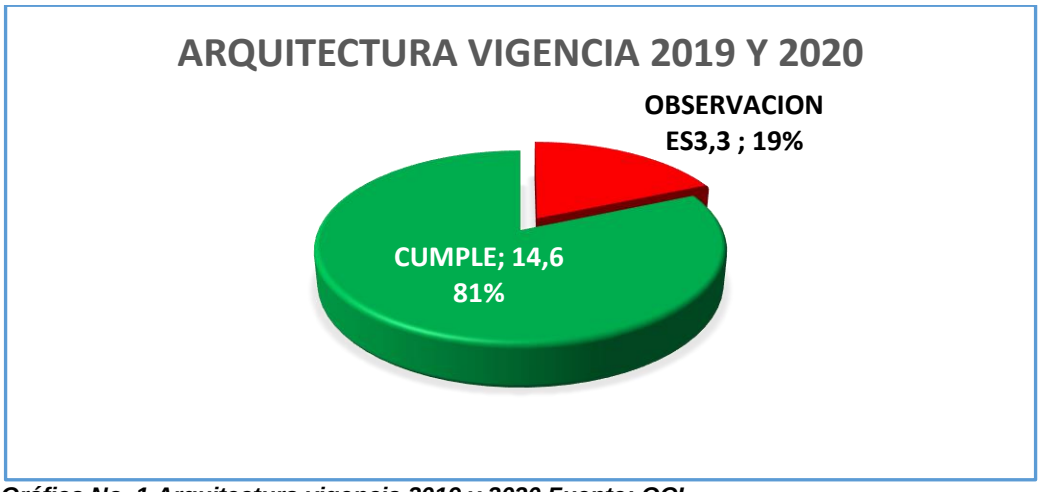
https://scjgovcol.sharepoint.com/:f:/s/DireccionTIC/Eo4rGPiFlAVBt51gl1mDNmgBGoAa77PURHtAh1iLCSySYg?e=TGpyaV

RESPUESTA OCI:

El proceso auditado no allega una evidencia significativa que respalde el cumplimiento de la pregunta formulada en el instrumento de medición del avance de Gobierno Digital para la vigencia 2019 y 2020 "***Documentó e implementó un plan de continuidad de los servicios tecnológicos mediante pruebas y verificaciones acordes a las necesidades de la organización",*** nuevamente hace referencia al documento ***"Plan de contingencia Tecnológica SCJ",*** el cual no está codificado y aprobado por la instancia correspondiente y debe actualizarse, igualmente, allega el procedimiento ***"Gestión de Cambios de TIC PD-GT-2 ",*** que si bien es significativo para garantizar los cambios tecnológicos y controlar el ciclo de vida de estos, con el fin de reducir el impacto y minimizar la interrupción de los servicios, no representa un proceso integrado de contingencia de continuidad del negocio y los servicios tecnológicos.

Es evidente, tal como lo expresa la Dirección de Tecnologías y Sistemas de la Información, en la actualidad se trabaja en la formulación del Plan de Continuidad de TI para el cuatrienio del 2020 al 2024. En tal medida, debe mantenerse la observación a fin de verificar su tratamiento.

Ahora bien, con relación al avance en la implementación del componente Arquitectura de la política de Gobierno Digital, el equipo auditor, concluye el siguiente avance:



Gráfica No. 1 Arquitectura vigencia 2019 y 2020 Fuente: OCI

En el instrumento de avance de Gobierno Digital, se verificaron 18 criterios del habilitador transversal *Arquitectura* tanto en la vigencia 2019 como en la 2020, se evidenciaron 14,6 de conformidad y 3,3 con observaciones, presenta un avance del 81% en cada vigencia, el cual corresponde a nivel ALTO de avance.

8.1.3 HABILITADOR TRANSVERSAL SEGURIDAD DE LA INFORMACIÓN.

GESTIÓN DE RIESGOS Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN VIGENCIA 2019 Y 2020.

8.1.3.1. DEBILIDAD EN LA GESTIÓN DEL RIESGO Y EN LA CONFORMACIÓN E IMPLEMENTACIÓN DE UN PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, INCUMPLIENDO LO ESTABLECIDO EL DECRETO 612 DE 2018, EXPONIENDO A LA ENTIDAD A BAJAS PONDERACIONES CUANDO SE EVALUÉ EXTERNAMENTE ESTE CRITERIO.

Los auditados manifestaron que se estructura el formato F-FD-513, Registro de Activos de Información mediante el cual se empieza diligenciar y registrar los activos de cada proceso junto con la Guía de Gestión de Activos de Información G-FD-1, se elabora el borrador de la Matriz de riesgos de Seguridad Digital en la cual una vez se identifiquen los activos se procederá con la administración de los riesgos.

Con la respuesta anterior, el auditor evidencio que no se cuenta con una matriz de riesgos de seguridad digital, por lo cual no se ha ejecutado la Gestión de Riesgos de Seguridad Digital.

Por otra parte, el ejercicio auditor solicitó el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y se recibió respuesta del proceso así: ***"El Plan de Tratamiento de Riesgos el cual se encuentra en este momento en actualización. Está en proceso de implementación ya que se está construyendo con los diferentes líderes de proceso y líderes operativos los activos de información y de esta manera construir los riesgos asociados a la seguridad digital de los procesos Institucionales".***

Se evidencia que la entidad no cuenta con el plan de tratamiento de riesgos de seguridad de la información actualizado y publicado, el formato de matriz de riesgos esta sin diligenciar, lo cual puede derivar en insuficiente o deficiente tratamiento y mitigación de los riesgos. Por la falta de controles de estos riesgos, la integridad de la información está expuesta a cualquier incidente o daño.

Frente a lo anterior, el artículo 1 del Decreto 612 de 2018 establece ***"(…) Deberán integrar los planes institucionales y estratégicos que se relacionan continuación y publicarlo en su página web, a más tardar el 31 de enero de cada año (…). Numeral 11. Plan de tratamiento de riesgos de seguridad y privacidad de la información (…)"***

RESPUESTA DEL AUDITADO:

Respecto de esta observación, la Dirección de Tecnologías y Sistemas de la Información manifiesta que, si se cuenta con el Plan de Tratamiento de Riesgos de Seguridad de la Información 2020 publicado en el enlace de Transparencia y Acceso a la Información Pública del

sitio web de la Entidad, en cumplimiento de lo establecido en el Decreto 612 de 2018. Como evidencia de lo antes expresado, se adjunta pantallazo de la publicación. Es de anotar que para este plan se realizó una actualización la cual se encuentra en proceso de trámite de aprobación y divulgación. Se adjunta como evidencia el documento en trámite.

En cuanto a lo observado en relación con un Plan de Divulgación 2019 y 2020, se manifiesta que, si se cuenta con un plan, el cual se adjunta como evidencia.

Las evidencias antes citadas y que soportan lo expuesto se encuentran publicadas en la carpeta denominada Seguridad Privacidad Información, que se ubica en el siguiente enlace: https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FSeguridadPrivacidadInformaci%C3%B3n

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

Teniendo en cuenta la respuesta brindada por el proceso, se determina que, si bien se recibe y verifica el Plan de Tratamiento de Riesgos de Seguridad de la Información publicado en la Web de la entidad y una versión en trámite para su actualización, no se allega documentación que demuestre la implementación del plan y gestión de riesgos de seguridad para la vigencia 2020, tal como lo exige el instrumento de verificación de avance de MSPI.
En consecuencia, con lo anterior, debe mantenerse la observación para verificar su tratamiento a través del plan de mejoramiento.

Fueron de recibo para el equipo auditor las evidencias aportadas con relación al *Plan de Divulgación de Seguridad de la Información 2020*, razón por la cual se retiró el aparte de la versión final del informe de auditoría.

PLAN DE AUDITORIA DE SEGURIDAD DE LA INFORMACION.

8.1.3.2. DEBILIDAD EN LA FASE DE VERIFICACION DEL CICLO PHVA DEL SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, INCUMPLIENDO LAS NORMAS NTC-ISO/IEC 27001.

Los auditados informaron que, en el marco de la consultoría de la Alta Consejería de TIC, se realizó una verificación de la gestión de la seguridad y privacidad de la información al interior de la entidad, adicionalmente, se han realizado pruebas de vulnerabilidad a la infraestructura tecnológica de la entidad y que se tiene programada una auditoría interna de seguridad digital para el año 2020.

Entendiendo el significado y valor de las actividades manifestadas, el auditor solicitó a la DTSI el plan de auditoria de seguridad de la información y la respuesta del proceso fue "*No se tiene".*

El plan de auditoría es la formulación de un esquema que forma parte de la estrategia o enfoque, que se sigue para llevar a cabo la auditoría, es la descripción de las actividades y de los detalles que se van a examinar en ella.

No contar con el plan de auditoria de seguridad de la información, denota inobservancia de lo definido en el numeral *6 Auditorías internas* de las normas NTC-ISO/IEC 27001 y falencias en las actividades de *VERIFICAR* del ciclo *PHVA*, lo cual puede afectar la oportunidad en la verificación del cumplimiento y mantenimiento de los controles y seguimiento de la seguridad de la información y limitar la mejora continua del sistema. El avance en los requisitos para la vigencia 2019 y 2020, se detalla a continuación:

RESPUESTA DEL AUDITADO

Si bien dentro de los Retos que se establecieron en el año 2019 se estipulo que se iba a desarrollar una auditoria Interna al Modelo de Seguridad y Privacidad de la Información MSPI para el 2020, revisado el nivel de madurez del Modelo, no se consideró pertinente adelantarlo en esta vigencia. Es importante mencionar que, de acuerdo con la Guía Nº. 15 del Modelo de Seguridad y Privacidad de la Información MSPI Guía Auditoria MINTIC del 6 de mayo de 2016, la base de la auditoria de seguridad recae en los principios que sirven como lineamiento en el desarrollo de esta, la cual permite proporcionar resultados confiables, objetivos, pertinentes y suficientes para que la organización pueda tomar las decisiones acerca de lo avanzado. Por tal motivo el Plan de Auditoria debería ser realizado por la Oficina de Control Interno de la Entidad y no por el Oficial de Seguridad de la Información apelando al principio de integridad e independencia descrito en dicha guía: "Integridad: El profesionalismo del auditor se debe llevar a cabo a partir de su imparcialidad al MSPI, diligencia y responsabilidad, demostrando su competencia durante el ejercicio de la auditoria.

Presentación ecuánime: El resultado de la auditoria (hallazgos, conclusiones e informes) deben reflejar la veracidad y exactitud de la información que se presentó durante el desarrollo de la auditoria.

Debido cuidado profesional: La habilidad del auditor en formular los juicios de valor razonables y con conocimiento de seguridad durante toda la auditoria.

Independencia: La actuación del auditor se refleja en la independencia, libre de sesgo y conflicto de intereses. La independencia es la base de la imparcialidad y la objetividad del resultado de la auditoria, es así como está se mantiene objetiva durante todo el proceso"

Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

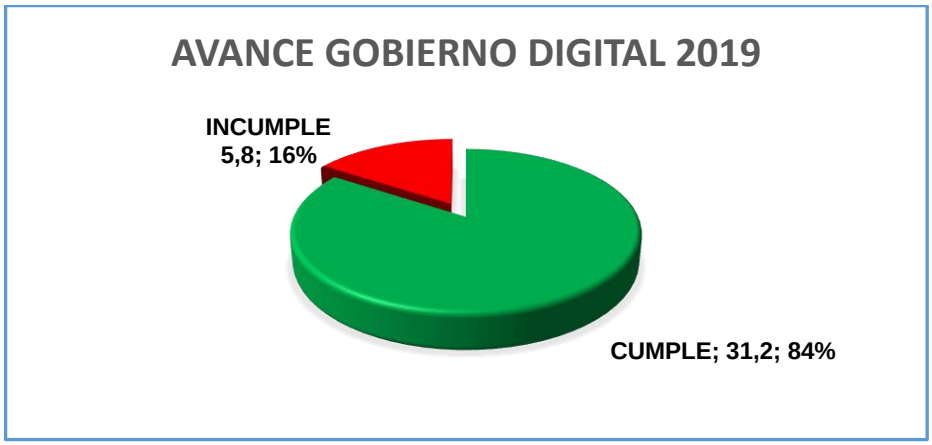
El Manual de Seguridad Digital que es la guía oficial para verificar el cumplimiento y avance de la implementación de la política de Gobierno Digital y en particular lo que concierne a seguridad de la información, en el numeral 4.1 menciona que "***la entidad debe definir indicadores de seguimiento para medir y evaluar el avance del Plan de seguridad y privacidad de la información"*** y en el numeral 5.3. Anexo 3 agrega que "***la entidad diseña, integra y aplica un plan de auditoría de seguridad de la información al plan estratégico de seguridad de la información"***. La ejecución de este último plan, el cual incluye el plan de auditoria de SI, está a cargo de la DTSI.

Además, teniendo en cuenta la respuesta brindada por el proceso auditado "***que se iba a desarrollar una auditoría Interna al Modelo de Seguridad y Privacidad de la Información MSPI para el 2020…***", es evidente que se consideró y analizó realizarla para esta vigencia. Dado lo anterior, se ratifica la observación a fin de realizar el correspondiente monitoreo a través del plan de mejoramiento.

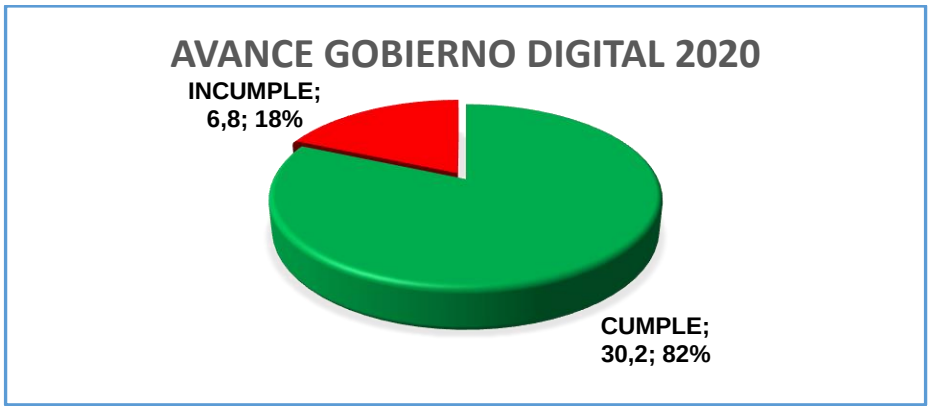
Del habilitador *Seguridad de la Información* se verificaron 13 criterios, para las vigencias 2019 y 2020, se evidenciaron 11 de conformidad y 2 con observaciones, presenta un avance del 85%, nivel ALTO, como se demuestra en la siguiente gráfica:

Gráfica No. 2 Seguridad de la información vigencias 2019 y 2020 Fuente: OCI

De la Política de Gobierno Digital, en general, se verificaron 31 criterios de *Arquitectura y Seguridad de la Información y 6 criterios de Empoderamiento*. En la vigencia 2019, se evidenciaron 31,2 de conformidad y 5,8 de incumplimiento, presenta un avance del 84%, nivel ALTO. En la vigencia 2020, se refleja un avance del 82%, nivel ALTO. El análisis estadístico se refleja con decimales debido a que los criterios están compuestos por preguntas y algunas de ellas cumplen o no cumplen. Veamos la representación gráfica:



Gráfica No. 3 avance gobierno digital vigencia 2019 Fuente: OCI



Gráfica No. 4 avance gobierno digital vigencia 2020 Fuente: OCI

Del habilitador Empoderamiento de los ciudadanos a través de un Estado Abierto de la Política de Gobierno Digital, se verificaron 6 criterios, de los cuales 5,5 presentaron conformidad, el 92%, nivel ALTO. Se deja una *recomendación* con relación al primer criterio de Empoderamiento del instrumento GD, “publicaciones en la sección "Transparencia y Acceso a la Información Pública" del sitio web oficial de la SDSCJ.

8.2 COMPONENTE MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.2.1 SEGURIDAD DE LAS OPERACIONES. COPIAS DE RESPALDO.

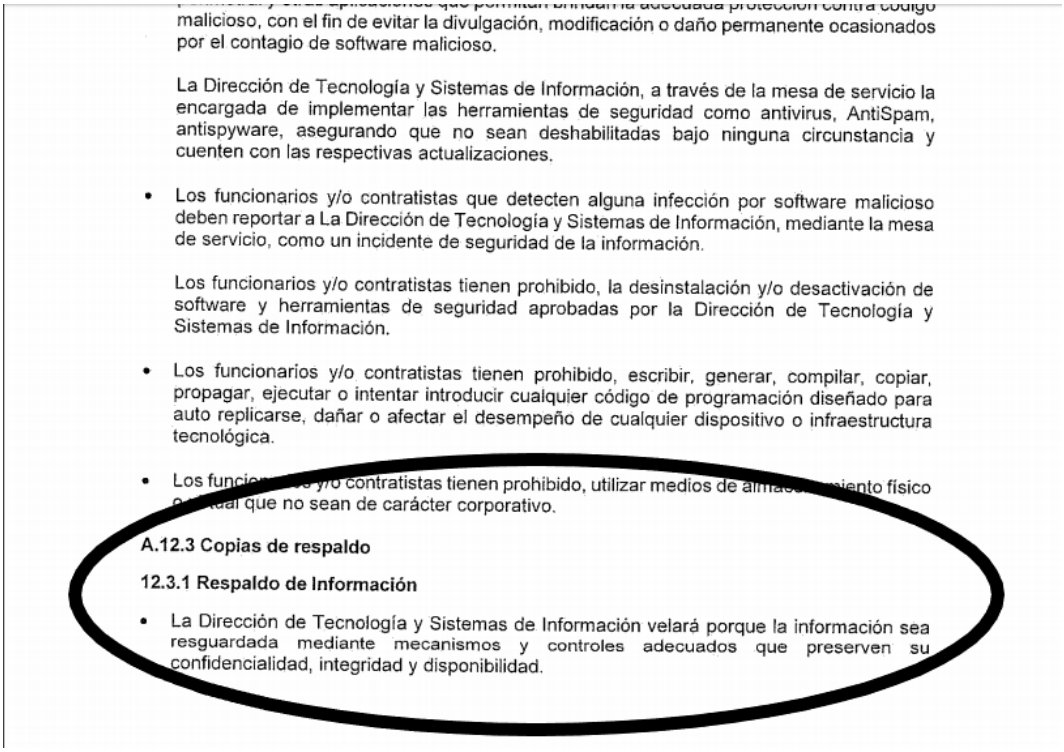
8.2.1.1. DEBILIDAD EN LA RETENCIÓN DE LOS BACKUPS DE LAS BASES DE DATOS HISTÓRICAS, INCUMPLIÉNDOSE EL ESTÁNDAR ISO 27001, QUE DEFINE EL DOMINIO SEGURIDAD DE LAS OPERACIONES, ENTRE OTROS, CON EL *BACKUP*, QUE TIENE COMO PROPÓSITO PROTEGER A LAS ORGANIZACIONES CONTRA LA PÉRDIDA DE INFORMACIÓN.

Actualmente se realiza un levantamiento de copias en la nube, cuya capacidad máxima de vigencia corresponde a los últimos tres (3) meses, expirado el termino, debe regrabarse el

contenido de la copia de seguridad y así sucesivamente. En ese marco, la capacidad pareciera muy limitada e insuficiente para garantizar un esquema de recuperación de información y retención de archivos, el cual debe establecer la entidad de acuerdo con la criticidad y complejidad de la información.

Al no contar con ciclos de mantenimiento de copias de mayor permanencia en la nube, la entidad corre un riesgo inminente al requerir información de bases de datos históricas que son imposible de recuperar por no estar retenida en las copias de respaldo en la nube.

En la misma vía, el Manual de Seguridad y Privacidad de la Información MA-GT-01, numeral a.12 seguridad de las operaciones, Ítem a.12.3 copias de respaldo, 12.3.1 respaldo de la información, establece:



malicioso, con el fin de evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso.

La Dirección de Tecnología y Sistemas de Información, a través de la mesa de servicio la encargada de implementar las herramientas de seguridad como antivirus, AntiSpam, antispyware, asegurando que no sean deshabilitadas bajo ninguna circunstancia y cuenten con las respectivas actualizaciones.

- Los funcionarios y/o contratistas que detecten alguna infección por software malicioso deben reportar a La Dirección de Tecnología y Sistemas de Información, mediante la mesa de servicio, como un incidente de seguridad de la información.

Los funcionarios y/o contratistas tienen prohibido, la desinstalación y/o desactivación de software y herramientas de seguridad aprobadas por la Dirección de Tecnología y Sistemas de Información.

- Los funcionarios y/o contratistas tienen prohibido, escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Los funcionarios y/o contratistas tienen prohibido, utilizar medios de almacenamiento físico que no sean de carácter corporativo.

A.12.3 Copias de respaldo

12.3.1 Respaldo de Información

- La Dirección de Tecnología y Sistemas de Información velará porque la información sea resguardada mediante mecanismos y controles adecuados que preserven su confidencialidad, integridad y disponibilidad.

Imagen 4. Lineamientos copias de respaldo. Fuente Manual de Seguridad de la Información

RESPUESTA DEL AUDITADO:

Como lineamiento base para la realización de los backups a las bases de datos de la Secretaría, cuenta la criticidad de los sistemas de información lo que a su vez determina el tiempo de retención. Actualmente se cuenta con los siguientes esquemas de retención de backups:

Esquema 1: Mecanismos o tácticas de backups para bases de datos:

1. *Servicio de BackUp Oracle Cloud dataset (Full backup mensual incremental) con retención dos meses.*

2. *Backup local RMAN dataset (Full backup semanal incremental) con retención de tres meses.*
3. *DataPump local (Full backup diario) retención tres meses.*

Esquema 2: Mecanismos o tácticas de backups para servidores de aplicación:

1. *Blockstorage backup unidades asociadas (tipo bronce Copias de seguridad incrementales mensuales y copia de seguridad full backup anual) retención 5 años*
2. *Bakcup de servidores (tipo bronce Copias de seguridad incrementales mensuales y copia de seguridad full backup anual) retención 5 años*
3. *Backup directorios de software de aplicación (tipo backup product cada 30 días) retención 1 mes.*

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada Seguridad Privacidad Información, que se ubica en el siguiente enlace:
https://scjgovcol.sharepoint.com/:f:/s/DireccionTIC/EtIYF6Tm08VAt7MkzxsJLVABBRjj1mO0LeeeK3pOFDHl8Q?e=dgB1CF

RTA OCI:

Es de anotar, que la observación está dirigida a ampliar el tiempo de retención de las bases de datos de la entidad, de hecho, se evidencia en el esquema de retención de backups suministrado por la DTSI, en el numeral 1: Mecanismos de backups para bases de datos, que la retención de backups es de 2 a 3 meses, se corrobora que para garantizar una recuperación de información y retención de archivos más efectiva y prolongada, la entidad debe establecer, de acuerdo a los recursos disponibles y a la criticidad de la información, una mayor retención de backup de datos, más que todo, mensuales en los servicios NFS storage y Block storage.

Teniendo en cuenta el documento allegado "***informe dimensionamiento nube Oracle scj***", se observa que aun así "***La infraestructura actual soporta en forma eficiente el uso de almacenamiento en memoria RAM, Procesamiento y almacenamiento activo",*** en el documento se recomienda un crecimiento de almacenamiento en los servicios NFS storage y Block storage.

Por lo anteriormente manifestado, debe mantenerse la observación con relación a la retención de backup de bases de datos de la Secretaría, para verificar las acciones de mejora formuladas a través del plan de mejoramiento.

8.2.2 CRIPTOGRAFÍA. POLITICA DE CONTROLES CRIPTOGRÁFICOS.

8.2.2.2. (Esta observación fue desestimada por el auditado) SE ELIMINO DEBILIDAD EN LA DOCUMENTACIÓN DE LOS PROCESOS CRIPTOGRÁFICOS, INCUMPLIENDO LA RESOLUCIÓN 851 DE 2019, POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA SDSCJ, LO QUE PERMITE LA APLICACIÓN DE VARIOS CRITERIOS, POTENCIALIZANDO LA MATERIALIDAD DE RIESGOS EN LA SEGURIDAD DIGITAL.

RESPUESTA DEL AUDITADO

En concordancia con la Guía de Gestión de Activos de Información con código G-FD-1 del 29 de agosto de 2019, en su numeral ítem Clasificación de la información, la entidad cuenta con la siguiente clasificación de la Información:

Información pública
Información pública clasificada
Información pública reservada
Información sensible

De acuerdo con la clasificación establecida, en la Secretaría, toda la información, exceptuando la pública, se cifra o se le aplican llaves criptográficas para su manejo, transmisión o envió. Se adjunta el documento de manejo de cifrado en las aplicaciones, en donde se evidencia la forma y tipo de encriptado.

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada Seguridad Privacidad Información, que se ubica en el siguiente enlace: https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FSeguridadPrivacidadInformaci%C3%B3n

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada

RESPUESTA OCI:

Revisada la evidencia allegada por la DTSI, "***Manual de configuración políticas de firewall para conexión o inspección de tráfico encriptado v2",*** se evidencia la existencia de una política de firewall que ayuda validar conexiones bajo tráfico cifrado punto a punto y análisis de tráfico SSL en la entidad, con un alcance de "***Validación de tráfico SSL que realizan los funcionarios de la entidad cuando interactúan con portales web, aplicaciones y descarga de archivos. Así como la trasmisión de información por medio de canales MPLS de manera cifrada punto a punto usando algoritmos de cifrado por medio de la implementación de las VPN Site to Site"***.

Dado lo anterior, se acepta la objeción presentada y en consecuencia se retira el aparte que brinda sustento a la observación del informe final de auditoría, se conserva la redacción de la observación, por garantizar la trazabilidad de la Oficina de Control Interno.

8.2.3 SEGURIDAD FÍSICA Y DEL ENTORNO.

8.2.3.1. DEBILIDAD EN LA SEGURIDAD EN OFICINAS, RECINTOS E INSTALACIONES Y ÁREAS DE CARGA, DESPACHO Y ACCESO PÚBLICO, INCUMPLIENDO LO ESTABLECIDO EN EL MANUAL DE SEGURIDAD DE LA INFORMACIÓN, Y AUMENTANDO LAS POSIBILIDADES DE MATERIALIDAD DE RIESGOS.

- Debilidad en el formato de control de acceso físico a Data Center y/o centro de cableado, el cual no está codificado, ni aprobado por la instancia correspondiente.

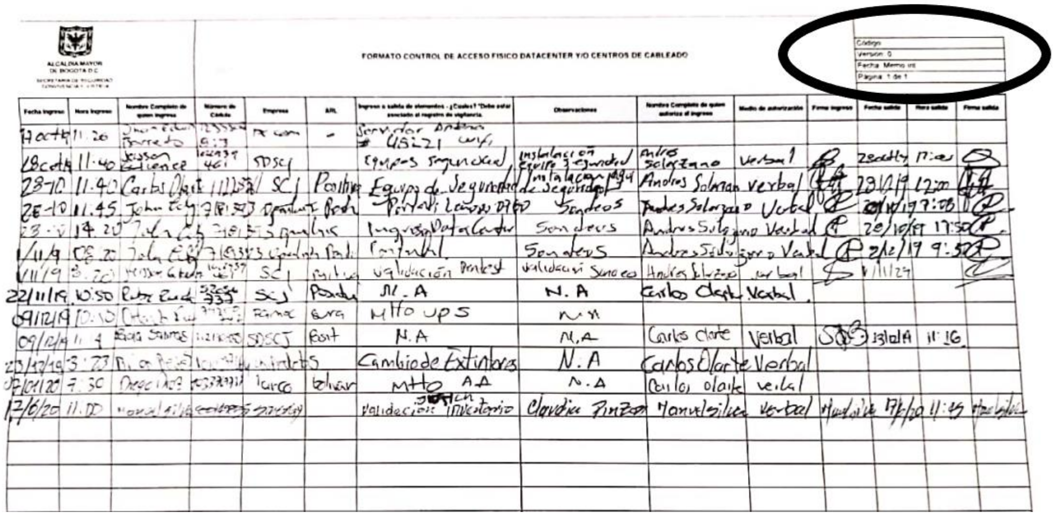
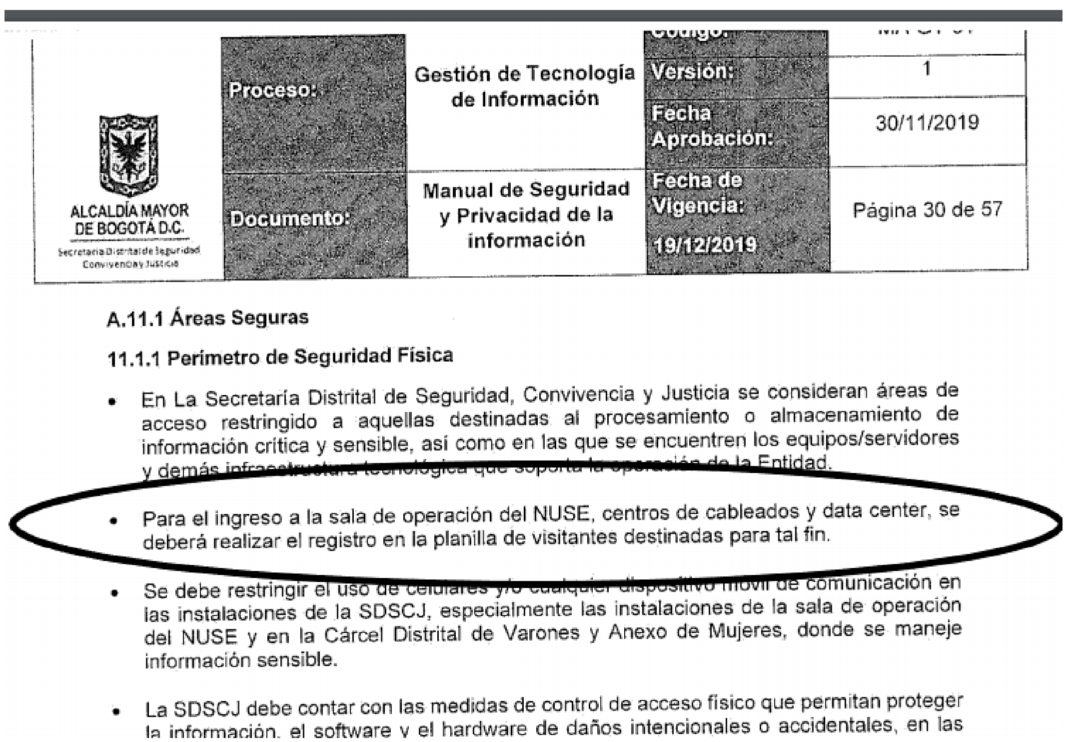


Imagen 5. Formato registro ingreso Data Center. Fuente DTSI

Se aprecia en la imagen No. 4, que el formato carece de código, versión, fecha de aprobación y de vigencia, datos que son los que evidencian la formalidad del documento.



ALCALDÍA MAYOR DE BOGOTÁ D.C. Secretaría Distrital de Seguridad Convivencia y Justicia	Proceso:	Gestión de Tecnología de Información	Código:	
			Versión:	1
			Fecha Aprobación:	30/11/2019
	Documento:	Manual de Seguridad y Privacidad de la información	Fecha de Vigencia: 19/12/2019	Página 30 de 57

A.11.1 Áreas Seguras

11.1.1 Perímetro de Seguridad Física

- En La Secretaría Distrital de Seguridad, Convivencia y Justicia se consideran áreas de acceso restringido a aquellas destinadas al procesamiento o almacenamiento de información crítica y sensible, así como en las que se encuentren los equipos/servidores y demás infraestructura tecnológica que soporta la operación de la Entidad.
- Para el ingreso a la sala de operación del NUSE, centros de cableados y data center, se deberá realizar el registro en la planilla de visitantes destinadas para tal fin.
- Se debe restringir el uso de celulares y/o cualquier dispositivo móvil de comunicación en las instalaciones de la SDSCJ, especialmente las instalaciones de la sala de operación del NUSE y en la Cárcel Distrital de Varones y Anexo de Mujeres, donde se maneje información sensible.
- La SDSCJ debe contar con las medidas de control de acceso físico que permitan proteger la información, el software y el hardware de daños intencionales o accidentales, en las

Imagen 6. Lineamientos registro a Data Center. Fuente Manual de Seguridad de la Información

Tal y como se observa en la imagen que antecede, es deber de la SDSCJ, garantizar la formalidad de los documentos que se utilizan en cuartos restringidos como proteger y brindar los controles necesarios para las áreas determinas como seguras para su operación.

RESPUESTA DEL AUDITADO

La Dirección de Tecnología y Sistemas de la Información cuenta dentro de sus controles con los registros de acceso al centro de datos para los años 2019 y 2020 actualizados, tal como se puede evidenciar en los formatos adjuntos, sin embargo, como plan de mejora a la solicitud para el registro del control de acceso al centro de datos de la Entidad, se formalizará el formato en mención en el Sistema de Gestión de la Seguridad de la Información de la Secretaría y se dará continuidad al registro de los visitantes que ingresan al centro de datos.

Archivo: "Planilla Registro Centro de Datos 15052020.pdf"

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada ServiciosTecnologicos, que se ubica en el siguiente enlace: https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FSeguridadPrivacidadInformaci%C3%B3n

RESPUESTA OCI

De recibo, lo informado por parte del equipo auditado, en consecuencia, se mantiene la observación para verificar su tratamiento.

- Debilidad en los controles para el ingreso de materiales a las instalaciones de la SDSCJ, pues no se evidencia ninguna directriz, que defina los controles de seguridad para esta gestión, tampoco se evidencia con algún protocolo, si el material entrante se inspecciona para determinar si es manipulado durante el viaje.

RESPUESTA DEL AUDITADO

Referente a las áreas de despacho y carga, el Manual de Seguridad de la Información en el numeral 11.1.6 contempla "La SDSCJ debe establecer los controles apropiados para las áreas de despacho y carga, con el fin de no permitir el ingreso de personal no autorizado a las instalaciones de la entidad". La observación planteada hace referencia a controles para el ingreso de materiales a las instalaciones de la Secretaría, dichos materiales deben corresponder a los bienes de la Secretaría. Al respecto, el proceso de Gestión de Recursos Físicos y Documental cuenta con el instructivo I-FD-1 "Acceso Instalaciones SDSCJ", el cual tiene el objetivo de controlar el acceso y salida de visitantes, bienes y documentos de las instalaciones de la Secretaria de Seguridad, Convivencia y Justicia.

Con relación a lo mencionado en la observación, el instructivo anteriormente citado en el numeral 4.2.1 INGRESO Y SALIDA DE BIENES DE LA SEDE ADMINISTRATIVA DE LA SDSCJ, indica los lineamientos para los servidores y/o contratistas que por necesidad de sus actividades requieran ingresar o retirar bienes al servicio de la Entidad, mediante trámite dirigido a la Dirección de Recursos Físicos y Gestión Documental, con copia al jefe inmediato incluyendo la información

de quien ingresa o retira los bienes, la justificación del requerimiento y la información del bien, indicando explícitamente en dicho instructivo que la responsabilidad sobre dichos bienes recae en el servidor y/o contratista que realizó la solicitud.

Dado lo anterior, la observación referente a que "No es responsabilidad del EDIFICIO T7-T8 de la empresa de vigilancia, la salida o entrada de equipos o elementos varios al área de oficinas…" no indica falta de lineamientos claros, dado que el instructivo I-FD-1 Acceso Instalaciones SDSCJ, el cual incluye los lineamientos y la responsabilidad respecto al ingreso y salida de los bienes de la Secretaría. En lo que corresponde al área de carga, el manual del usuario edificio T7-T8 da los lineamientos para el manejo de carga, los cuales incluyen los controles como la solicitud a la administración del edificio, la asignación de personal ascensorista, asignación de ascensor de carga, asignación de estacionamiento de vehículos únicamente por el tiempo necesario para el cargue y descargue de mercancía, aviso al personal de seguridad y mantenimiento del Centro Empresarial.

Las evidencias de las mismos ya fueron entregadas previamente, y se encuentran disponibles en los enlaces relacionados a continuación:

Instructivo I-FD-1 Acceso Instalaciones SDSCJ:

https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FMSPI%20%2D%20Evidencias%202020071 7%2FRecursos%20F%C3%ADsicos%20A11%20Seguridad%20y%20A%2E8%20Activos%2FA11%20%2D%20SEGURIDAD%2FA%2E11%2E2%2E6

Manual Usuario Edificio T7-78:

https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FMSPI%2D%20evidencias%20requerimiento%2020200803%2FA%2E11%2E1%2E6

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

Dado que la nueva evidencia suministrada por la DTSI, "***Instructivo I-FD-1 Acceso Instalaciones SDSCJ***", se evidencia que se está controlando el acceso y salida de visitantes, bienes y documentos de las instalaciones de la entidad y registra los lineamientos y la responsabilidad respecto al ingreso y salida de bienes de la Secretaría, además, señala los requisitos de ingreso y salida de bienes de la bodega de la entidad y el traslado e ingreso/salida de elementos tecnológicos, cumple con el requisito establecido en el instrumento MSPI con relación a "***establecer que el material que ingresa se registra de acuerdo con los procedimientos de gestión de activos al entrar al sitio***". Se retira el aparte de la observación, en el informe final de auditoría.

8.2.4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. DOCUMENTO DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

8.2.4.1. DEBILIDAD EN LOS PROCESOS Y DIRECTRICES PARA MANEJAR LAS DESVIACIONES Y LAS EXCEPCIONES EN LA APLICACIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN, INCUMPLIENDO LAS DIRECTRICES ESTABLECIDAS POR EL MINTIC, EN EL INSTRUMENTO MSPI, LO QUE PUEDE GENERAR RIESGOS DE MATERIALIDAD EN LA INFORMACIÓN DE PROPIEDAD DE LA SDSCJ.

Las malas prácticas que se pueden suscitar en la aplicación de esa política conllevarían a que los empleados y el personal exógeno relacionado con la entidad desatendieran y violaran la confidencialidad e integridad de la información.

Lo anterior denota incumpliendo de las directrices del Min Tic, ítem AD.1.1 ***"Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la Dirección, publicada y comunicada a los empleados y a las partes externas pertinentes, referente a los procesos para manejar las desviaciones y las excepciones."***

Corrobora el criterio anterior, el Decreto 413 en el artículo 26, literal I," *Implementar políticas de seguridad de la información".*

RESPUESTA DEL AUDITADO:

Partiendo del hecho de que se definen como "Desviaciones" las malas prácticas realizadas por los colaboradores de la Entidad o personal exógeno, en la Secretaría éstas son tratadas de una de las siguientes maneras.

1. *Socialización y Divulgación de la Política General y Especificas del MSPI*
2. *Acuerdos y cláusulas de Confidencialidad en contratos.*

Respecto de las excepciones, cabe mencionar que la Entidad cuenta con el Directorio Activo y con el procedimiento Control de Acceso a plataformas PD-GT-12 del 30 de agosto de 2019, en donde se establecen los requisitos y perfiles de usuarios que pueden acceder a las plataformas de la SDSCJ

Es de precisar que el Decreto 413 en el artículo 26, literal I expresa textualmente "Implementar políticas de seguridad informática y de la plataforma tecnológica de la Secretaría, definiendo los planes de contingencia y supervisando su adecuada efectividad", lo cual indica que se habla del concepto "Seguridad informática" el cual es completamente diferente en su desarrollo y aplicación de acuerdo a la norma NTC ISO 27001:2013 al concepto de "seguridad de la información"
Desviación (Seguridad informática): Perdida posible de Integridad
Desviación (Seguridad de la información): Malas Practicas

Se adjunta el pantallazo de la Política de Seguridad de la Información 2019 publicada en el sitio web de la Entidad, además se adjunta la carpeta de sensibilizaciones 2019 y 2020 y el procedimiento de Control de Acceso a Plataformas PD-GT-12

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada SeguridadPrivacidadInformación, que se ubica en el siguiente enlace: https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FSeguridadPrivacidadInformaci%C3%B3n

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RTA OCI:

La respuesta brindada por parte de la DTSI es pertinente con relación al tratamiento de las desviaciones y las excepciones en materia de seguridad de la información, pero éstas no figuran ni son explícitas en la Política de Seguridad y Privacidad de la Información, se reitera que no se evidencia específicamente "***los procesos para manejar las desviaciones y las excepciones***" en el Manual de seguridad y privacidad de la información MA-GT-01. Se mantiene la observación para garantizar su tratamiento a través del plan de mejoramiento.

8.2.5 GESTIÓN DE ACTIVOS.

PROPIEDAD DE LOS ACTIVOS Y MANEJO DE ACTIVOS.

8.2.5.1. DEBILIDAD EN LA DEFINICIÓN DE LAS RESTRICCIONES Y CLASIFICACIONES DE ACCESO A ACTIVOS IMPORTANTES DE LA ENTIDAD Y EN EL MARCADO DE TODAS LAS COPIAS DE MEDIOS, INCUMPLIENDO EL MANUAL DE SEGURIDAD DE LA INFORMACIÓN

- Debilidad en la definición y revisión periódica de las restricciones y clasificaciones de acceso a activos importantes de la entidad lo que incrementa la materialidad de riesgos de seguridad digital.

Tal y como lo dejo definido, el Manual de Seguridad de Información, Numeral A.9 Control de Acceso, ítem a.9.1.1 Política de Control de Acceso, la SDSCJ, deberá implementar los controles tantos físicos como lógicos, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información de la entidad.
La organización y estructura de controles documentados para el acceso y restricción a activos importantes de la entidad minimizaría el riesgo de alteraciones, pérdidas o manipulaciones de estos.

En el desarrollo del ejercicio auditor, no logro evidenciar, un procedimiento o un instructivo que restrinja el acceso a activos de la entidad, lo cual puede generar riesgos asociados a la confidencialidad e integridad de la información.

RESPUESTA DEL AUDITADO

La Entidad cuenta con el procedimiento PD-GT-8 Administración de usuarios que incluye lineamientos para la asignación de los permisos definidos según el rol a cumplir dentro de la entidad, con los cuales se gestionan los accesos o restricciones a los activos de información de manera general. Dicho procedimiento incluye entro otros la gestión del retiro del personal, eliminación de usuarios en aplicativos, eliminación de cuentas de correo electrónico, eliminación de usuarios en directorio activo, con los cuales se mitigan riesgos de seguridad sobre los activos de información.

En este sentido, la Dirección de Tecnologías y Sistemas de la Información, dispone del equipo técnico y las soluciones de software y hardware que permiten la gestión de las restricciones sobre los activos de información, teniendo los controles necesarios para la separación de funciones mediante la gestión de usuarios, roles y permisos dentro de las plataformas de la Entidad.

Si bien es cierto que la Entidad cuenta con los mecanismos para la gestión de los accesos y restricciones sobre los activos, es necesario realizar la actualización de dicha documentación que incluya la revisión periódica de los accesos, y aspectos de virtualidad, documentación electrónica y digital como:

- *Documentos electrónicos: Si el documento contiene información reservada o de uso interno, se debe indicar el nivel de clasificación al menos en la portada del documento; si contiene información secreta, se debiera indicar dicho nivel de clasificación tanto en la portada como en cada una de las páginas.*
- *Correo electrónico: se indica el nivel de clasificación en la primera línea del cuerpo del correo electrónico.*
- *Soporte de almacenamiento electrónico (discos, tarjetas de memoria, etc.): se debe indicar el nivel de clasificación sobre la superficie de cada soporte.*
- *Documentación de FileServer, Archivos compartidos, Virtual Drives dentro y fuera de los recursos tecnológicos de la entidad.*
- *Plataformas de Colaboración: que permiten Compartir archivos, datos, noticias y recursos, trabajo colaborativo en línea.*
- *Reuniones Virtuales*

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada SeguridadPrivacidadInformación, que se ubica en el siguiente enlace: https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FSeguridadPrivacidadInformaci%C3%B3n

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

Si bien el procedimiento PD-GT-8, Administración de usuarios, gestiona los accesos o restricciones a los activos de información digital de la entidad, es indispensable contar con una

guía o procedimiento que defina controles físicos a activos importantes, tal como se observa en este dominio del instrumento MSPI, "***Los activos mantenidos en el inventario deben tener un propietario y se deben fortalecer los controles***" y considerando que el proceso auditado confirma que es necesario realizar la actualización de la documentación para incluir la revisión periódica de los accesos, y aspectos de virtualidad, documentación electrónica y digital, se ratifica la observación para garantizar su tratamiento en el plan de mejoramiento.

- Debilidad en el marcado claro de todas las copias de medios.

Situación que puede ocasionar desorganización y problemas de identificación de las copias de medios donde reposa información importante, poniendo en riesgos su seguridad oportunidad, confidencialidad e integridad.

Frente al Numeral A.8 Gestión de Activos, Ítem A.8.2 Clasificación de la Información del Manual de Seguridad de Información, establece: "***La SDSCJ deberá establecer los mecanismos necesarios para el adecuado etiqueteado de la información de acuerdo con el nivel de clasificación asignado teniendo en cuenta los tipos de información descritos en la Guía de Gestión de Activos de Información G-FD-1".***

La Guía menciona en el numeral 6 Etapas del Inventario de Activos de Información, Ítem 6.1 Diligenciamiento del Formato de Activos de Información, en el sub ítem 6.1.6 Clasificación y Custodia de la Información, identifica, entre otros, si el activo requiere de etiqueteado.

RESPUESTA DEL AUDITADO

En búsqueda de asegurar que la información de la entidad reciba el nivel apropiado de protección, se desarrolló una estructura para clasificar y etiquetar la información en el SharePoint de la Dirección, sobre lo cual se adjunta la evidencia.

Por otra parte, de acuerdo con la Norma NTC ISO 27001:2013 en su numeral A.8.2 Clasificación de la Información, se expresa que se hace necesario desarrollar los lineamientos pertinentes para el etiquetado de la información que no reside en la nube de Oracle, de acuerdo con el esquema adoptado por la Entidad en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada. Aun así, es de aclarar que la Secretaría no utiliza medios físicos de almacenamiento externo para propósitos de respaldo.

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada *SeguridadPrivacidadInformación*, que se ubica en el siguiente enlace: https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FSeguridadPrivacidadInformaci%C3%B3n

En virtud de lo expuesto, respetuosamente manifestamos al Equipo Auditor no estar de acuerdo con la observación realizada y por ende solicitamos sea retirada del informe final.

RESPUESTA OCI:

Si bien el proceso auditado afirma que "***La Secretaría no utiliza medios físicos de almacenamiento externo para propósitos de respaldo***", durante el ejercicio auditor se evidencio que "***El procedimiento y lineamiento de etiquetado de activos y medios se encuentra en construcción en fase temprana, por ende aún no se cuenta con el control***" y que "***Actualmente la DTSI viene estructurando un plan de trabajo para la actualización y/o elaboración de documentos asociados al dominio de Gobierno TI, en el mencionado plan se contemplará la elaboración del Procedimiento de Etiquetado de Activos de la Información***". A la fecha de finalización de la auditoría, no se presentó evidencia que permita verificar el procedimiento y lineamiento de etiquetado de activos y medios. Por las razones expuestas debe mantenerse el aparte en la observación.

8.2.6 RELACIONES CON LOS PROVEEDORES. GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES.

8.2.6.1. DEBILIDAD EN EL SEGUIMIENTO, REVISIÓN Y AUDITORÍA REGULAR A LOS PROVEEDORES PARA EVALUAR EL CUMPLIMIENTO DE COMPROMISOS RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN, INCUMPLIENDO LA RESOLUCIÓN 851 DE 2019, LO QUE REPRESENTA UNA FALENCIA EN LOS CONTROLES ADMINISTRATIVOS Y RIESGO DE MATERIALIDAD RESPECTO DE LA FUGA DE INFORMACIÓN.

De conformidad con lo establecido en la Política de Seguridad de la Información, artículo 16 control de acceso, literal f, respecto a los controles en las relaciones con los proveedores, la SDSCJ, definirá mecanismos de control que aseguren que la información a la que tenga acceso un tercero cuente con un nivel de protección adecuado y que estos cumplan con las políticas y procedimientos de seguridad de la información establecidos.

Luego del ejercicio auditor, no logro evidenciarse que la entidad realice seguimiento y control a la información que acceden los proveedores, en consecuencia, la privacidad y seguridad de la información se pone en riesgo y puede ser vulnerable por los proveedores que pueden incurrir a acciones indebidas que afectaría la información de la entidad.

RESPUESTA DE AUDITADO

En concordancia con la NTC-ISO 27001:2013, que en la normativa asociada al Anexo A literal A.15 RELACIONES CON PROVEEDORES numeral A.15.1.1 Política de Seguridad de la Información, es de aclarar que el supervisor del contrato debe solicitar por escrito la creación de usuario indicando expresamente los accesos requeridos a las aplicaciones, para el correcto desarrollo de las actividades contractuales que va a desarrollar el proveedor. Respecto a los servicios que están en Nube se tiene restricciones de nivel de red segmentada y control de acceso por medio del Firewall, además se tiene asociado para los servicios de correo electrónico y herramientas de colaboración un espacio de alojamiento que permite controlar los servicios

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada SeguridadPrivacidadInformación, que se ubica en el siguiente enlace: https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2F

Documentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FSeguridadPrivacidadInformaci%C3%B3n

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

Con la respuesta brindada por el proceso de Gestión de Tecnología de la Información, si bien el supervisor del contrato define los accesos a la información requeridos para el desarrollo de las actividades del proveedor, se reitera, tal como se evidenció durante el ejercicio auditor, que no se demuestran actividades específicas de seguimiento, control, revisión y auditoría a la información que acceden los proveedores, dirigidas a verificar y validar el cumplimiento de los compromisos respecto a la seguridad de la información, se mantiene la observación.

8.2.7 DATACENTER

CONDICIONES DE MOBILIARIO Y ÁREA.

8.2.7.1. DEBILIDAD EN LAS CONDICIONES DE SEGURIDAD DEL CUARTO DE PROCESAMIENTO DE DATOS, INCUMPLIENDO EL MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MA-GT-01 Y EXPONIENDO A LA ENTIDAD A HECHOS GRAVES QUE AFECTARIAN NOTABLEMENTE LOS EQUIPOS DE LA DATA CENTER.

El auditor evidencio que los aires acondicionados están dentro del centro de datos con tuberías y ductos expuestos y a la vista, no están asegurados, ni adecuadamente aislados y protegidos.

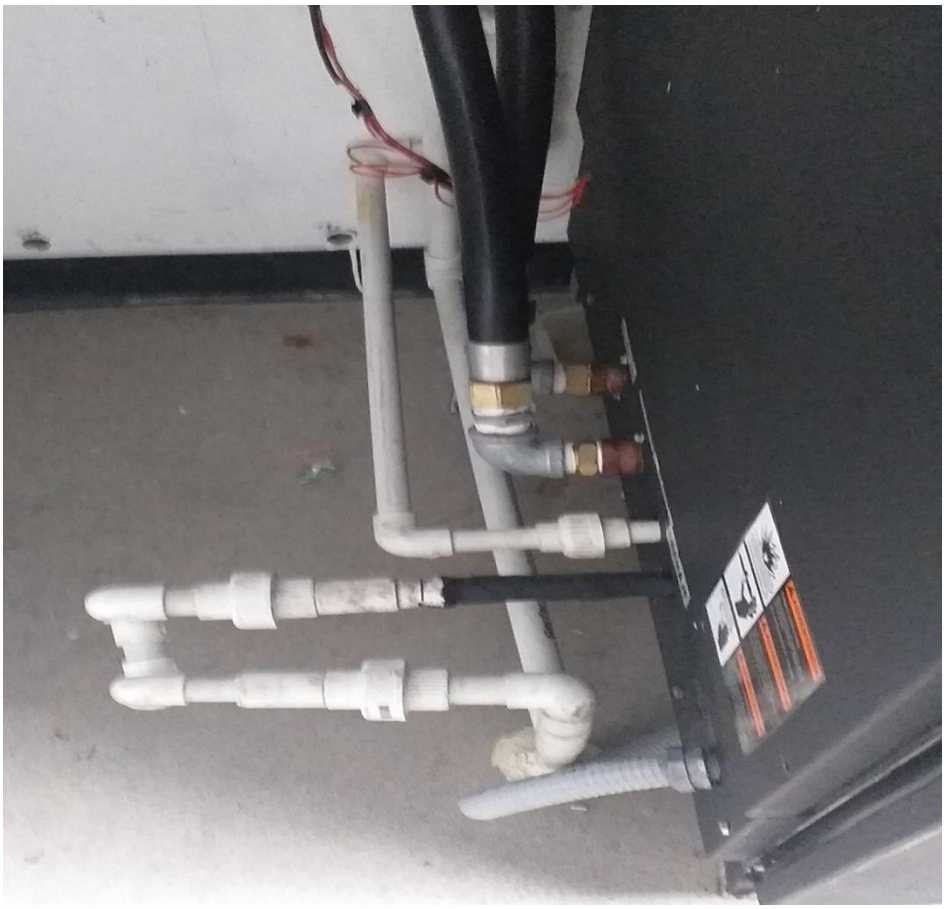


Imagen 7. Tubería expuesta en el Data Center

Sin el cumplimiento de los requisitos ambientales en el Data Center se corre el riesgo de una ruptura de tubería ocasionando serios daños a todos los equipos de cómputo y de comunicaciones, inclusive, puede provocar afectaciones eléctricas graves que podría acarrear consecuencias muy delicadas en el funcionamiento de parte de la infraestructura tecnológica de la entidad.

Frente a este hecho, el Manual indica en el Numeral A.11 Seguridad Física y del Entorno, Ítem 11.14 Protección contra amenazas externas y ambientales ***"La SDSCJ debe cumplir con los requisitos ambientales (temperatura, humedad, otros), en las instalaciones de procesamiento de información, con el fin de responder de manera adecuada ante incidentes como incendios e inundaciones entre otros".***

RESPUESTA DEL AUDITADO

Actualmente en lo que se puede evidenciar con las fichas técnicas de los aires acondicionados, no se cuenta con el cruce de tubería hidráulica (conducción de agua potable, aguas negras, aguas lluvias) sobre el área del Datacenter, se adjunta las fichas técnicas mencionadas en el enlace.

Sin embargo, se realizará la gestión con la Dirección de Recursos Físicos para que minimice la exposición de la tubería que impida un posible acceso a la misma.

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada *Servicios Tecnológicos*, que se ubica en el siguiente enlace: https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FServiciosTecnol%C3%B3gicos

RESPUESTA OCI:

Se evidencia con la respuesta de la DTSI que es indispensable minimizar la exposición de la tubería que impida un posible acceso a la misma para que esas conexiones y ductos del sistema de aire acondicionado estén seguros y protegidos con el fin de evitar posibles afectaciones a los equipos tecnológicos del Data Center.

En el material allegado se evidencian las características y dimensiones, entre otros, de las conexiones del Sistema de Aire Acondicionado y Refrigeración. Por lo anterior debe mantenerse la observación a fin de brindar tratamiento a través del plan de mejoramiento.

8.3 COMPONENTE SISTEMAS DE INFORMACIÓN

8.3.1 MÓDULOS OPGET, LIMAY, SISCO, SIAP Y PROGRESSUS.

8.3.1.1 DEBILIDAD EN LA GENERACIÓN DE CONSULTAS, REPORTES Y LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN, INCUMPLIENDO LA LEY 1712 DE 2014 Y EL MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MA-GT-01, LIMITANDO LA FUNCIONALIDAD DE LA FUENTE DE CONSULTA, OCASIONANDO REPROCESOS QUE EN TODO CASO DIFICULTAN LA GESTIÓN ADMINISTRATIVA Y GENERANDO POSIBLES RIESGOS EN LAS CONTRASEÑAS DE LOS USUARIOS.

Durante la verificación de la funcionalidad de los módulos mencionados, se evidencio:

- Debilidad en la generación de consultas y reportes en los aplicativos OPGET, LIMAY, SISCO, SIAP Y PROGRESSUS.

El contenido de los reportes generados por los aplicativos es limitado, el formato de los informes es restringido a PDF, no es reutilizable, afectando la oportunidad y celeridad de la información de salida, indispensable para las gestiones administrativas y la toma de decisiones eficientes.

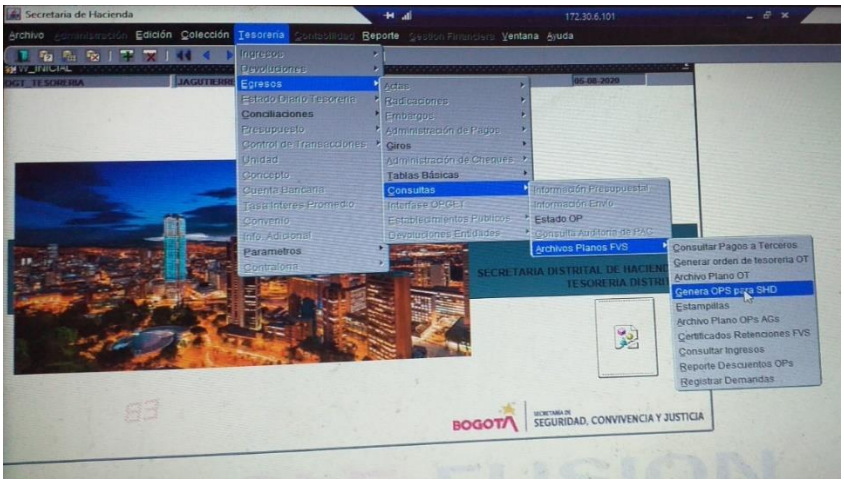


Imagen 8. Opción Tesorería -> Consultas. Fuente Aplicativo OPGET

En el entendido que los aplicativos generan reportes fijos o estáticos y archivos planos a partir de una variedad de consultas, no disponen de generación de reportes a partir de una parametrización robusta y suficiente para satisfacer requerimientos a la medida y aumentar el uso y aprovechamiento de la información. Un número importante de informes de salida deben ser solicitados a los administradores de los aplicativos en la DTSI.

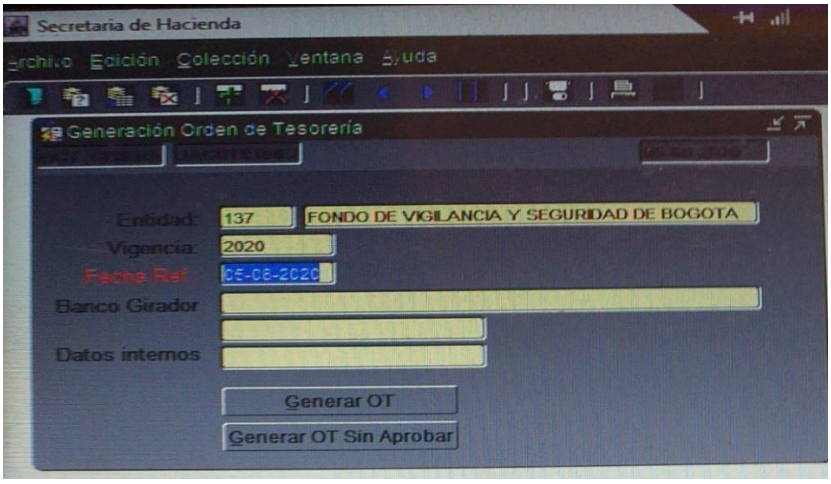


Imagen 9. Opción Tesorería -> Consultas -> Generación Orden de Tesorería. Fuente OPGET.

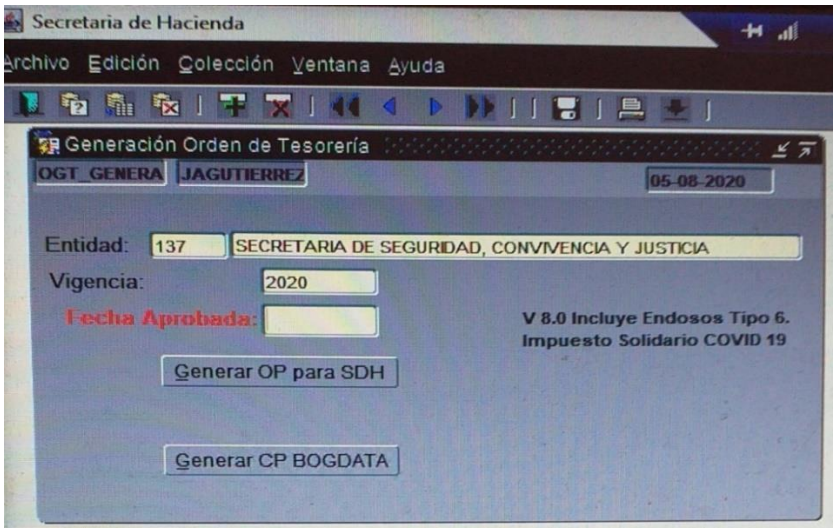


Imagen 10. Opción Tesorería -> Consultas -> Generación OPS para SHD. Fuente OPGET

Tal como se observa en la imagen No. 8, la parametrización está limitada solo a los datos de Entidad, Vigencia y Fecha Aprobada, impidiendo seleccionar datos de salida como rangos de fechas, filtros por usuarios, diferentes formatos CSV, DOC, XLS, PDF, TXT y demás que sean requeridos.

Ahora bien, respecto al Sistema de Información SIAP, se evidenció en el desarrollo de la auditoría, que este no permite descargar información en formatos reutilizables, incumpliendo el principio de la calidad de la información.

Los reportes que genera SIAP, en algunas oportunidades pueden utilizarse, para responder peticiones ciudadanas, la cual es información pública, pero su formato restringido afecta y pone en riesgo la oportunidad y celeridad de la información para las gestiones pertinentes.

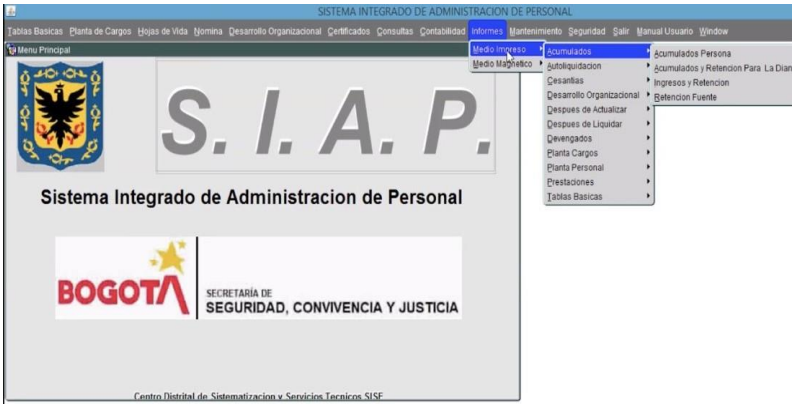


Imagen 11. Pestaña en cascada para la generación de reportes solo en PDF. Fuente SIAP

Debido a esta limitante de reportes, se afecta la completitud, disponibilidad, integridad, el acceso y oportunidad de la información necesaria para consultas, seguimientos o toma de decisiones.

Para finalizar, el ejercicio auditor evidencio también que en el módulo Progressus las peticiones ciudadanas son relevantes e indispensable en un formato flexible o reutilizable, pero el aplicativo solo permite la generación de reportes en formato PDF.

Frente a lo anterior, la ley 1712 de 2014, respecto al principio de la calidad de la información, dejo establecido ***"Toda la información de interés público que sea producida, gestionada y difundida por el sujeto obligado, deberá ser oportuna, objetiva, veraz, completa, reutilizable, procesable y estar disponible en formatos accesibles para los solicitantes e interesados en ella, teniendo en cuenta los procedimientos de gestión documental de la respectiva entidad".***

RESPUESTA DEL AUDITADO

En lo que respecta a los aplicativos PREDIS, OPGET, PAGOS, LIMAY, y SISCO, que hacen parte del ERP SI CAPITAL, fueron adquiridos a través de convenio interadministrativo con la Secretaria Distrital de Hacienda, y el sistema de información SIAP fue adquirido a través de un convenio suscrito con la Secretaria Distrital de Gobierno, soluciones sobre las cuales se adoptaron las funcionalidades, características de diseño y estándares de seguridad definidos por las entidades mencionadas, cumplimiento sus lineamientos y necesidades del momento, sin estar vigente la ley 1712 de 2014 y el manual de seguridad y privacidad de la información MA-GT-01; Es importante mencionar que el desarrollo de los Sistemas SICAPITAL y SIAP fueron iniciados en 2001 claramente anteriores a la ley y manual antes mencionados, así las cosas los usuarios funcionales utilizan las consultas y reportes que venían definidos en las versiones entregadas.

La Secretaria de Seguridad, Convivencia y Justicia, realizó la implementación de la versión NIC-SP de SICAPITAL en el 2018, trayendo con esta las actualizaciones necesarias para suplir las necesidades de los usuarios finales. Para la vigencia 2019 se realizaron mesas de trabajo buscando dar solución a las mejoras y ajustes solicitados por cada uno de los usuarios funcionales y adicional a eso, se realizó una reunión con la Oficina de Control Interno respecto a los hallazgos hechos a la Dirección Financiera en donde se plantearon las soluciones a los puntos encontrados por dicha dependencia, los cuales fueron implementados y se encuentran en producción. En dichas mesas no fueron solicitadas mejoras a las consultas y los reportes existentes. Es importante mencionar que a la fecha no se tienen solicitudes de mejoras o nuevos desarrollos sobre las funcionalidades, consultas y reportes.

Las soluciones tecnológicas SICAPITAL (OPGET/PAGOS, LIMAY y SISCO) y SIAP se han ido mejorando y modificando según solicitud de los usuarios y la aplicación de los procedimientos internos, el tipo de consultas y reportes generados desde estas soluciones están dados bajo las necesidades propias de los usuarios, y se presentan en formato PDF o archivo plano según requerimiento.

Sumado a lo anterior, en la actualidad la entidad se encuentra a la espera de los lineamientos que la Secretaría Distrital de Hacienda imparta en relación con la implementación del nuevo ERP BogData, los cuales pueden impactar el futuro de las aplicaciones citadas en esta observación, razón por la cual la Dirección de Tecnologías y Sistemas de la Información no ha planeado mejoras generales en estas aplicaciones.

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada SistemasdeInformación, que se ubica en el siguiente enlace:
https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FSistemasdeInformaci%C3%B3n

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RTA OCI:

Los usuarios funcionales manifestaron en las mesas de trabajo realizadas para la revisión de los módulos OPGET, LIMAY, SISCO, SIAP Y PROGRESSUS, la necesidad y pertinencia de generadores de reportes parametrizables y en formatos reutilizables por las razones expuesta en esta observación las cuales son objetivas y perentorias de resolver, más sin embargo, con la implementación del nuevo sistema BogData en la Secretaría Distrital de Hacienda, la funcionalidad y operación de los módulos de SICAPITAL y otros aplicativos de la SDSCJ podrían variar. La observación se mantiene, pero dependerá de la continuidad en servicio de los módulos mencionados.

- Debilidad en la seguridad de las contraseñas para acceder a los aplicativos OPGET/PAGOS, SISCO, SIAP Y PROGRESSUS.

La administración de la base de datos Oracle no está perfilada para obligar a los usuarios que cumplan los criterios de construcción de contraseñas de acuerdo con lo establecido en el Manual de Seguridad de la Información, además, su composición es libre.

Los usuarios auditados de OPGET manifestaron que, si bien sus claves las conforman de manera segura, el sistema les permite configurarlas sin ningún requisito y restricción.

Los auditados del aplicativo SISCO expresaron que las contraseñas que utilizan no contienen caracteres especiales, el sistema no controla la estructura que debe cumplir, ni tampoco exige el cambio periódico de contraseñas.

Los usuarios del sistema SIAP, incluido el usuario administrador de la DTSI, manifestaron que la estructura de la contraseña que utilizan es una combinación de números y letras.

Lo evidenciado en los módulos OPGET, SISCO y en el sistema SIAP genera riesgos asociados a la vulnerabilidad de las claves y de confidencialidad e integridad de la información, tal como está contemplado en el objetivo principal de la Política de Seguridad y privacidad de la Información de la SDSCJ.
Frente a lo anterior, se evidencia un claro incumplimiento del Manual de Seguridad y Privacidad de la Información, en el Numeral A.9 Control de Acceso, ítem 9.3 Responsabilidades de los usuarios, 9.3.1 *que establece* ***"Los funcionarios y contratistas deberán utilizar credenciales seguras de ingreso a los servicios o sistemas de información designados, las cuales deben contener entre 8 y 14 caracteres, números, letras y caracteres especiales".***

Fortalece el criterio normativo anterior, los enunciados al respecto por la Resolución 004 de 2017, ART. 18. Dominios de Control, NORMA NTC-ISO/IEC 27000, Dominio 7 Control de acceso a los datos, medios para impedir accesos no autorizados.

No obstante, hasta aquí lo referido con anterioridad, también el ejercicio auditor evidenció debilidad en el manejo del usuario administrador de SIAP, se identificó, que la titularidad del usuario, funcionaria/contratista de la DTSI, durante los periodos en los que no está activa (vacaciones, otros), se la concede a la ingeniera que la reemplaza en esa función.

Igualmente, el auditor verificó que los usuarios funcionales del módulo PROGRESSUS tienen las contraseñas de otros usuarios, incluyendo la del usuario administrador del sistema. Los usuarios auditados informan que para facilitar y agilizar el trabajo que realiza cada uno de ellos en la aplicación y, por otra parte, para mitigar la carga laboral del administrador del sistema, recurren a este procedimiento laboral irregular que desconoce las funciones y responsabilidades de cada servidor o contratista, lo cual puede conllevar a la desorganización de tareas en el aplicativo y riegos de seguridad de la información.

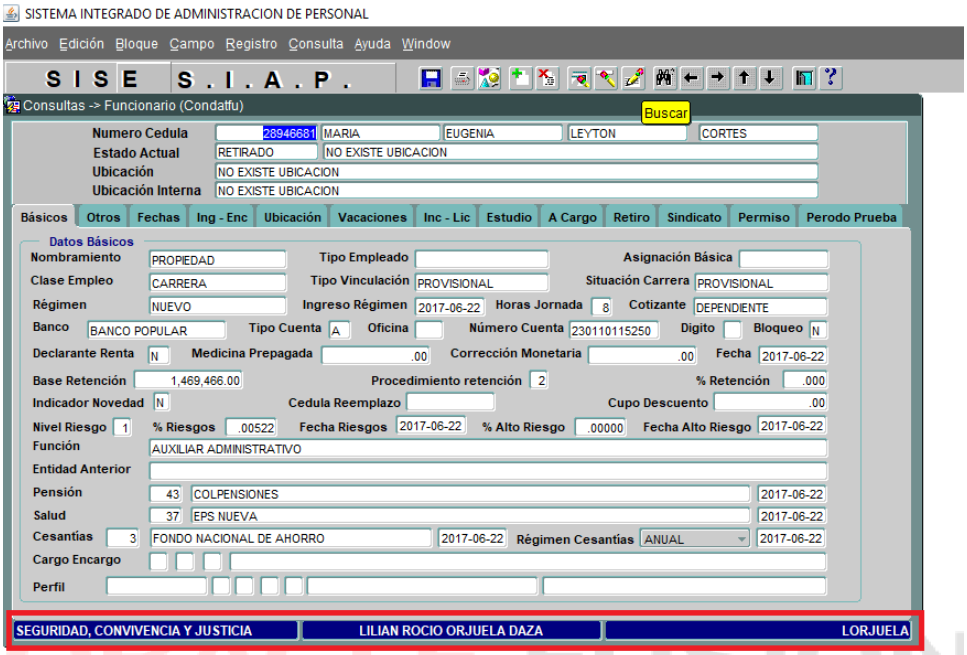
Lo anterior denota, tanto en el sistema SIAP como en PROGRESSUS, incumplimiento de lo establecido en el Manual de Seguridad y Privacidad de la Información MA-GT-01, Numeral A.9 Control de Acceso. ítem 9.3 Responsabilidades de los usuarios Numeral 9.3.1: ***"Los funcionarios y contratistas deberán mantener confidencialidad de sus contraseñas o claves de acceso a los sistemas de información, asegurándose que no sea divulgada en ninguna instancia***".

RESPUESTA DEL AUDITADO

Con respecto a lo establecido en el ítem 9.3 Responsabilidades de los usuarios, numeral 9.3.1: "Los funcionarios y contratistas deberán mantener confidencialidad de sus contraseñas o claves de acceso a los sistemas de información, asegurándose que no sea divulgada en ninguna instancia", se evidencia que el uso inadecuado de las claves y contraseñas para acceder a los sistemas de información es una problemática que corresponde y es responsabilidad directa de las áreas usuarias de los sistemas de información. En este mismo sentido, el hallazgo es real, pero no para la Dirección de Tecnologías y Sistemas de la Información, si no para las áreas usuarias de los sistemas de SIAP (Gestión Humana) y PROGRESSUS (Subsecretaria de Seguridad y Convivencia) que están faltando a al cumplimiento de la política definida para el uso y administración de claves.

Los sistemas de Información SICAPITAL y SIAP fueron entregados con el nivel básico de seguridad que permite la base de datos Oracle y así mismo fueron implementados y configurados en la entidad, por esto, con el ánimo de complementar los niveles de seguridad que provee el motor de base de datos Oracle, en la actualidad se está realizando el análisis que corresponde para proponer una solución que permita la gestión de usuarios y claves en todos los sistemas de información incluyendo aspectos como el acceso a los sistemas por perfil y grupos de usuarios que incluye la política.

Respecto a la clave del usuario que permite dar soporte al sistema SIAP, se creó un usuario a la ingeniera que reemplaza al ingeniero habitual que da este soporte al aplicativo.



Nuevo usuario Soporte Aplicación SIAP

En pantalla se puede evidenciar lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

De recibo, la respuesta y evidencia enviada por el proceso, pues se valida la creación de un nuevo usuario soporte para la aplicación SIAP, subsanando la debilidad formulada, el aparte de la observación se ratifica por el evidente manejo y uso inadecuado de las contraseñas por parte de los usuarios funcionales de los módulos *SISCO, SIAP Y PROGRESSUS* y por la falta de control y restricción de los sistemas de información al no exigir requisitos mínimos de composición de las claves o en su defecto para perfilar y complementar los niveles de seguridad que provee el motor de base de datos Oracle para obligar a los usuarios que cumplan los criterios de construcción de contraseñas.

8.3.2 MODULO DE PRESUPUESTO - PREDIS.

8.3.2.1. DEBILIDADES EN LA NUMERACIÓN CONSECUTIVA Y LA EMISIÓN DE LA FECHA DE LOS CERTIFICADOS DE DISPONIBILIDAD PRESUPUESTAL DE LOS PERÍODOS OCTUBRE 2019 A JUNIO DE 2020 GENERADOS EN EL SISTEMA PRESUPUESTAL, INCUMPLIENDO EL MANUAL DE POLÍTICAS CONTABLES, NUMERAL 7.3.2. REPRESENTACIÓN FIEL, NUMERAL 7.3.4. VERIFICABILIDAD, Y NUMERAL 7.3.7. COMPARABILIDAD, LO QUE OCASIONA INCERTIDUMBRE EN SU EMISIÓN Y POSIBLE

INCUMPLIMIENTO DE LAS CARACTERÍSTICAS CUALITATIVAS DE LA INFORMACIÓN FINANCIERA.

Analizados los reportes de los consecutivos de la Ejecución Presupuestal – Disponibilidades para los meses de octubre de 2019 a junio de 2020 (Unidades Ejecutoras 1 y 2), se observaron 15 saltos en la fecha de emisión de los documentos, es decir, las fechas no guardan un orden cronológico, ocasionando incertidumbre en su emisión (0,96% en promedio de la muestra de auditoría), ni se observó documentos que evidencien el uso y/o anulación de los consecutivos Nos: 996 de 2019 (UE1) ,38 y 41 de 2020 (UE1) y 237 de 2020 (UE2), lo que impide determinar si los mismos fueron utilizados, circunstancias que podrían corroborar la ejecución de dos o más transacciones sensibles en conflicto, lo que podría afectar el estado real de la disponibilidad presupuestal, situación que va en contravía con las características cualitativas de la información financiera claramente definidas en las políticas contables.

Los saltos en las fechas identificados son los que se describen a continuación:

Consecutivos_Disponibilidades_Oct-Dic2019_UE1

* Se observó el consecutivo 996 que no es consecuente con la numeración del período seleccionado.
* Se observaron errores en el consecutivo de las fechas:

Información s/n PREDIS		Observación Control Interno	% registros en el período
No. Disponibilidad	Fecha Documento		
996	7-dic-19	La fecha consecutiva correcta debió ser entre: 01-02-oct-2019	0,42%
1358	16-dic-19	La fecha consecutiva correcta debió ser: 01-oct-2019	

Consecutivos_Disponibilidades_Oct-Dic2019_UE2

* No se observan saltos en la numeración
* Se observaron errores en el consecutivo de las fechas:

Información s/n PREDIS		Observación Control Interno	% registros en el período
No. Disponibilidad	Fecha Documento		
467	3-oct-19	La fecha consecutiva correcta debió ser: 01-oct-2019	2,82%
476	13-nov-19	La fecha consecutiva correcta debió ser entre: 07-09-oct-2019	
484	13-nov-19	La fecha consecutiva correcta debió ser entre: 17-21-oct-2019	
546	30-oct-19	La fecha consecutiva correcta debió ser: 31-oct-2019	
676	30-dic-19	La fecha consecutiva correcta debió ser: 31-dic-2019	
678	30-dic-19	La fecha consecutiva correcta debió ser: 31-dic-2019	

Consecutivos_Disponibilidades_Ene-Jun2020_UE1

* No se observaron los consecutivos: 38, 41 en la numeración del período seleccionado.
* Se observaron errores en el consecutivo de las fechas:

Información s/n PREDIS		Observación Control Interno	% registros en el período
No. Disponibilidad	Fecha Documento		
277	29-ene-20	La fecha consecutiva correcta debió ser: 28-ene-2020	0,44%
281 a 292	30-ene-20	La fecha consecutiva correcta debió ser: 28-ene-2020	
297	30-ene-20	La fecha consecutiva correcta debió ser: 28-ene-2020	
375	30-ene-20	La fecha consecutiva correcta debió ser: 29-ene-2020	
386	30-ene-20	La fecha consecutiva correcta debió ser: 29-ene-2020	
536	28-feb-20	La fecha consecutiva correcta debió ser: 03-mar-2020	

Consecutivos_Disponibilidades_Ene-Jun2020_UE2

* No se observó el consecutivo: 237 en la numeración del período seleccionado.
* Se observaron errores en el consecutivo de las fechas:

Información s/n PREDIS		Observación Control Interno	% registros en el período
No. Disponibilidad	Fecha Documento		
212	28-feb-20	La fecha consecutiva correcta debió ser entre: 03-04-mar-2020	**0,18%**

Imagen 12. Consecutivos disponibilidades. Fuente: Elaboración propia

RESPUESTA DEL AUDITADO

PREDIS emite el control del número del consecutivo de la disponibilidad, pero no maneja el control de las fechas de emisión de la disponibilidad, este control no ha sido solicitado por los usuarios funcionales de la Dirección Financiera de la Secretaría de Seguridad, Convivencia y Justicia, y la opción de creación de la disponibilidad, viene con esta estructura desde la Secretaría de Hacienda Distrital.

La Dirección de Tecnologías y Sistemas de la Información en su procedimiento Gestión de Requerimientos Tecnológicos PD-GT-15, menciona que la definición de nuevas necesidades o requisitos como es el caso de la validación mencionada debe ser solicitada por el líder funcional de la Dirección Financiera con el Formato F-GT-192 Solicitud Solución Tecnológica, a la fecha no se ha recibido dicha solicitud en ese sentido.

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

Teniendo en cuenta lo señalado por la Dirección de Tecnologías y Sistemas de información que en la actualidad en el módulo de PREDIS no se maneja el control de las fechas de emisión de la disponibilidad", se hace necesario vincular al proceso de Gestión Financiera con el fin de manifestar la necesidad de implementar acciones tendientes a evitar que se continúen presentando saldos en la numeración de los consecutivos de los certificados de disponibilidad presupuestal, control que preferiblemente se aconseja sea automático. Dado lo anterior, se mantiene la observación para formular las acciones de mejora correspondientes, vinculando a la Dirección Financiera para gestionarlas.

8.3.3 MODULO SISCO.

8.3.3.1. DEBILIDAD EN LA REVERSIÓN DE TRANSACCIONES, DISPONIBILIDAD DEL MANUAL DE USUARIOS Y NUMERACIÓN AUTOMÁTICA DE LOS CONTRATOS EN EL SISTEMA SISCO, INCUMPLIENDO EL MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS POLÍTICAS CONTABLES, POR LA FALTA DE CONTROLES, LOS CUALES GENERAN RIESGOS EN LA SEGURIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y OPORTUNIDAD DE LA INFORMACIÓN.

- Debilidad en la reversión de transacciones en estado "viable"

El sistema no permite reversar operaciones en estado “viable”, las cuales solo se puede ejecutar con la intervención del administrador del aplicativo de la DTSI.

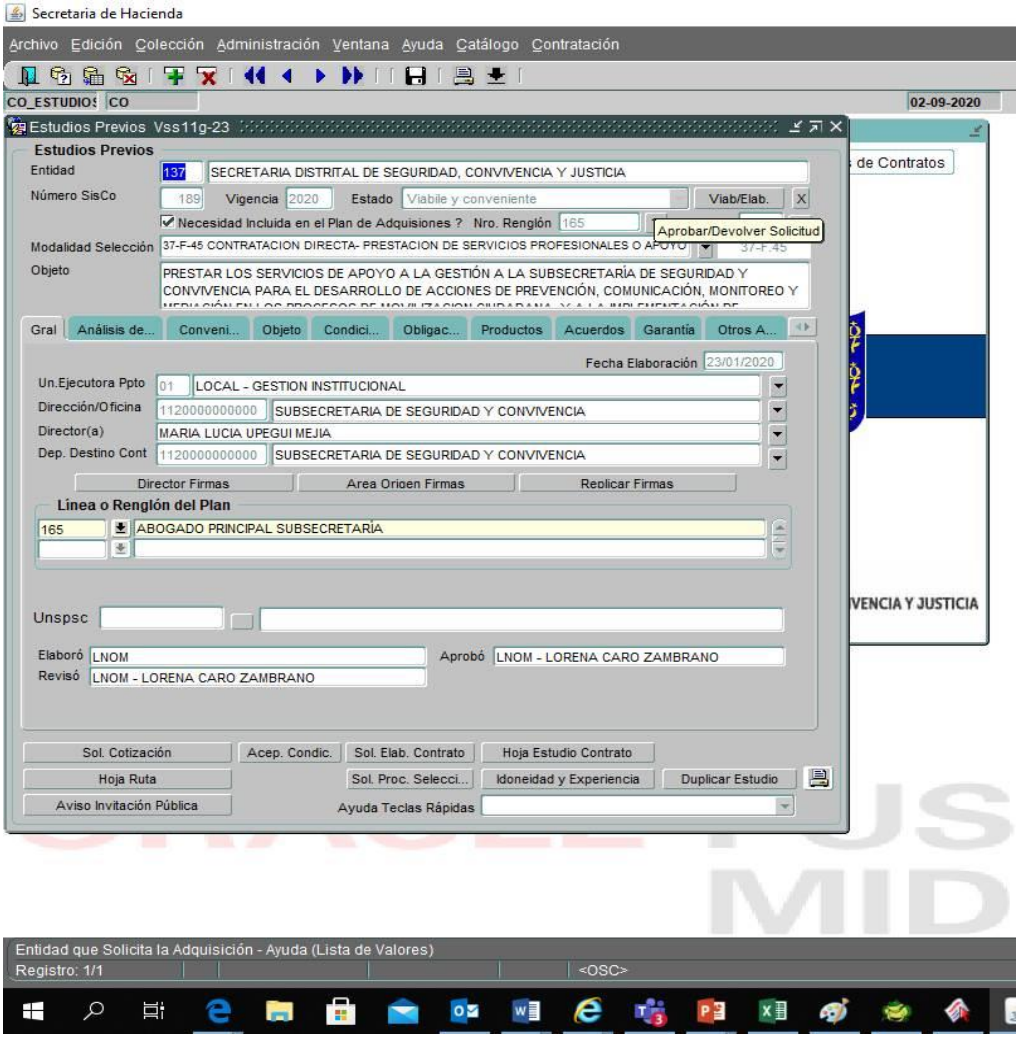
Lo anterior denota incumpliendo a lo establecido en el Manual de Seguridad y Privacidad de la información MA-GT-01, Numeral A.14 Adquisición, Desarrollo y Mantenimiento de los Sistemas, Ítem 14.2.1 Política de Desarrollo Seguro, ***“La DTSI debe aplicar las metodologías apropiadas para proteger los procesos transaccionales de los sistemas de información de la entidad”.***

La falta de completitud de este tipo de operaciones a nivel usuario representa una falencia en la calidad del desarrollo del aplicativo.

Esta condición genera retrasos en las operaciones cotidianas de los usuarios del sistema y verificaciones manuales de las operaciones reversadas por parte del agente tecnológico de la DTSI.

RESPUESTA DEL AUDITADO:

En la actualidad el módulo SISCO, en el único formulario (pantalla) que se viabiliza es en el correspondiente a Estudios Previos, tanto para solicitud contractual como para modificación, permitiendo que el usuario, si tiene el perfil y permiso de realizar esta actividad, lo pueda hacer.



La Dirección de Tecnologías y Sistemas de la Información en su procedimiento Gestión de Requerimientos Tecnológicos PD-GT-15, menciona que la definición de nuevas necesidades o requisitos como es el caso de la validación mencionada debe ser solicitada por el líder funcional de la Dirección Financiera con el Formato F-GT-192 Solicitud Solución Tecnológica; y a la fecha no se ha recibido una solicitud en ese sentido.

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RTA OCI:

Con el propósito de ampliar la explicación de lo evidenciado durante el ejercicio auditor, la observación se refiere a que después de cargar la minuta del contrato, no es posible reversarla, en caso de cometer error, esta operación sí es viable en el formulario de *estudios previos.*

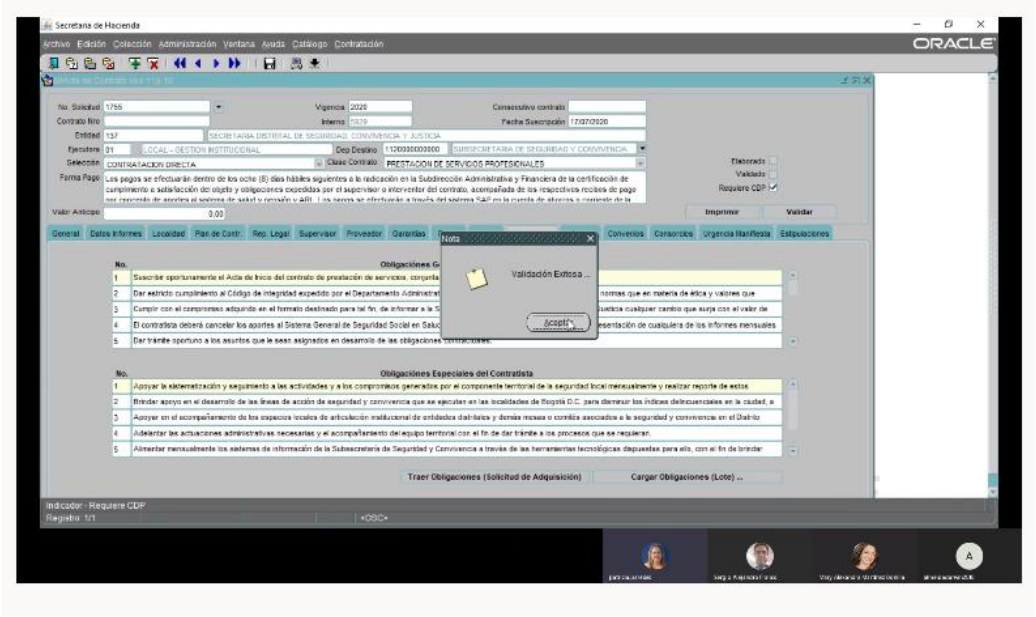


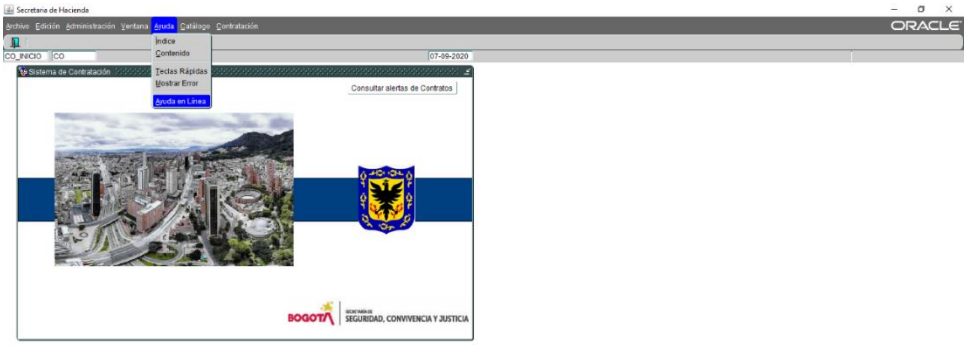
Imagen 13. Formulario Cargue minuta de contrato. Fuente módulo SISCO

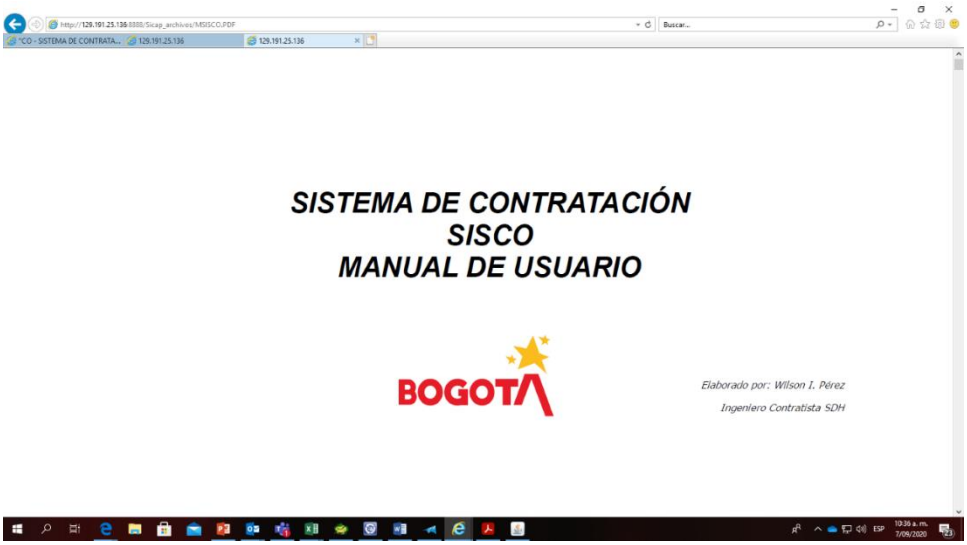
En consecuencia, los usuarios funcionales deben generar un caso en la Mesa de Servicios, para que el responsable del mantenimiento y soporte del aplicativo de la DTSI proceda de conformidad.

Se mantiene la observación instando a que se tomen las acciones necesarias aplicando el procedimiento pertinente por la Dirección Jurídica y Contractual, quien deberá adelantar las acciones que correspondan.

RESPUESTA DEL AUDITADO:

En la actualidad el módulo SISCO cuenta con la ayuda en línea como se puede observar en la siguiente pantalla.





Vale la pena aclarar que la actualización de estos manuales se realiza de manera periódica recopilando nuevas funcionalidades y mejoras realizadas durante el periodo de actualización.

El instructivo de usuario para el módulo SISCO se encuentra en proceso de actualización para incluir las últimas funcionalidades que han sido requeridas por los usuarios finales, la versión que se tiene en la actualidad data del año 2018, documento actualizado sobre el que fue entregado por la Secretaría de Hacienda.

Las evidencias que soportan lo expuesto se encuentran publicadas en la carpeta denominada SistemasdeInformación, que se ubica en el siguiente enlace:

https://scjgovcol.sharepoint.com/sites/DireccionTIC/Documentos%20compartidos/Forms/AllItems.aspx?CT=1594127771572&OR=OWA%2DNT&CID=409d8916%2Df522%2Df337%2D025d%2D2c0684e2d9c1&viewid=ae3ac8fb%2Dc220%2D422f%2Db8e3%2D572b5096e80a&id=%2Fsites%2FDireccionTIC%2FDocumentos%20compartidos%2FAuditoria%202020%2FInformeFinal%2FSistemasdeInformaci%C3%B3n

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

De recibo, lo informado por el equipo auditado, en consecuencia, se retiró el correspondiente aparte de la observación en el informe final de auditoría.

- Debilidad en la numeración automática de los contratos celebrados en la entidad.

El ejercicio auditor constató que, en cada una de las unidades ejecutoras, pese a que el aplicativo si puede realizar la numeración automática, actualmente los consecutivos de los contratos se realizan manualmente, situación que puede generar duplicidad de numeración en la misma unidad ejecutora y factibles reprocesos que afectarían documentos asociados.

Frente a este hecho se puede presentar, posiblemente, incumplimiento de las características cualitativas de la información financiera, que establece las políticas contables, Numeral 7.3.2. Representación Fiel, Numeral 7.3.4. Verificabilidad, y Numeral 7.3.7. Comparabilidad.

RESPUESTA DEL AUDITADO

El sistema si permite manejar el control de numeración consecutiva de contratos, pero por solicitud de la Dirección Jurídica y Contractual y la Dirección de Operaciones, este control esta inactivo desde la vigencia 2018, manifestando que si estas dependencias consideran que se debe activar este control, lo deben solicitar formalmente a la Dirección de Tecnologías y Sistemas de la Información, acorde a lo establecido en el procedimiento Gestión de Requerimientos Tecnológicos PD-GT-15, que hace mención a que la definición de nuevas necesidades o requisitos como es el caso de la validación mencionada, debe ser solicitada por el líder funcional de la solución con el Formato F-GT-192 Solicitud Solución Tecnológica.

A este respecto es importante mencionar que, desde febrero de 2020, la Dirección de Tecnologías y Sistemas de la Información ha adelantado varias actividades de sensibilización y apropiación que buscan que los usuarios hagan un correcto uso del sistema, de manera que en los próximos meses se puedan habilitar de nuevo todos los controles con que cuenta el módulo SISCO y que se encuentra deshabilitados. Esta actividad fue expuesta al señor Secretario y está siendo apoyada por el Subsecretario de Gestión Institucional.

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

Apoyamos la gestión que viene adelantando la DTSI con respecto a habilitar todas las opciones funcionales en el aplicativo SISCO, en ese sentido, el auditor considera que, si es importante realizar la numeración automática de los contratos de las unidades ejecutoras, se insta a que se ejecuten los adecuamientos necesarios en el proceso de contratación a fin de que no se generen reprocesos, ni se debilite la integridad de la información contractual. La observación se mantiene a fin de verificar la implementación de las acciones de mejora por parte de la Dirección Jurídica y Contractual.

8.3.4 SISTEMA DE INFORMACION DE PERSONAL – SIAP.

8.3.4.1. DEBILIDADES EN LA UTILIZACIÓN, VALIDACIÓN Y RESERVA DE INFORMACIÓN EN EL SISTEMA SIAP, LO CUAL DENOTA INCUMPLIMIENTO DE LA RESOLUCIÓN 004 DE 2017, LA NORMA NTC-ISO/IEC 17799:2005 Y DE LA LEY 1266 DE 2008. LO ANTERIOR, DEBIDO A LA NO ATENCIÓN DE CONTROLES ESTABLECIDOS PARA EL EFECTO, LO CUAL GENERA RIESGOS ASOCIADOS A LA SEGURIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y OPORTUNIDAD DE LA INFORMACIÓN.

Realizadas las pruebas pertinentes, en conjunto con los profesionales delegados para el efecto por parte de la Dirección de Gestión Humana y la DTSI, se identificaron las siguientes situaciones:

- Debilidad en la validación de datos en el módulo hojas de vida, opción novedades/ ingresos.

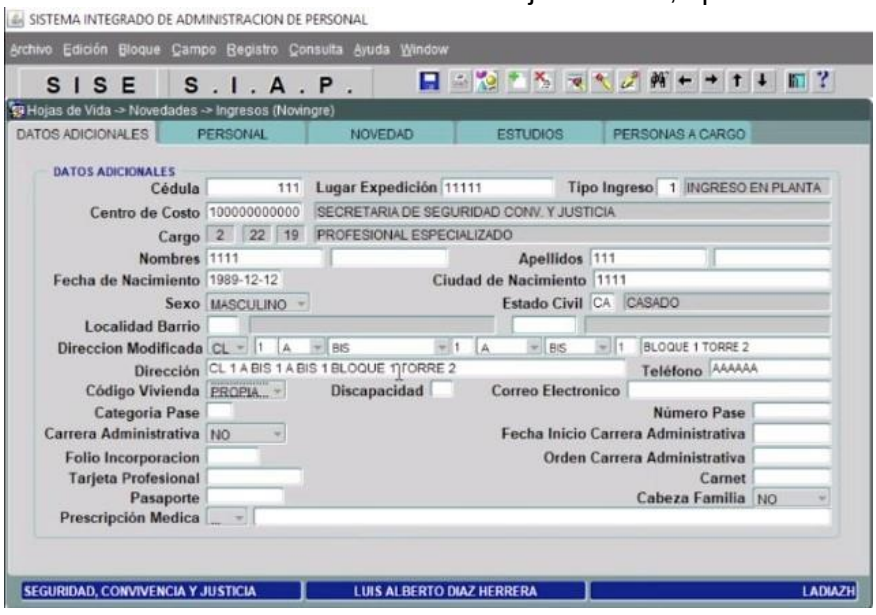


Imagen 14. Módulo Hojas de Vida. Fuente Sistema SIAP

Tal y como se observa en la imagen que antecede, se evidencian campos que no restringen el tipo de dato que deben capturar; *cedula* permite tipo carácter, *lugar de expedición*, acepta números, *nombres y apellidos,* permite números, *ciudad de nacimiento,* registra números.

Estas falencias pueden ocasionar verificaciones adicionales, reprocesos y factible entrega de información incorrecta o indebida, generando riesgos en la calidad e integridad de la información.

Con lo anterior, se incumple lo establecido en la norma NTC-ISO/IEC 17799:2005, los numerales 12.2.1 validación de la input data, ***"Se debiera validar los datos de entrada en las aplicaciones para asegurar que esta data sea correcta y apropiada"*** **y 12.2.2 control del procesamiento interno*, "Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados".***

RESPUESTA DEL AUDITADO

En el módulo Hojas de Vida, opción Novedades/Ingresos, la validación que el sistema realiza es que el campo que es numérico solo reciba números, además controla la obligatoriedad del campo es decir que no permite que el campo se guarde nulo.

La Dirección de Tecnologías y Sistemas de la Información en su procedimiento Gestión de Requerimientos Tecnológicos PD-GT-15, menciona que la definición de nuevas necesidades o requisitos como es el caso de la validación mencionada debe ser solicitada por el líder funcional de la Dirección de Gestión Humana con el Formato F-GT-192 Solicitud Solución Tecnológica, a la fecha no se ha recibido dicha solicitud en ese sentido, toda vez que si los controles mencionados por el auditor son necesarios deben realizar dicha solicitud.

RESPUESTA OCI:

Analizada la respuesta brindada por proceso auditado, se concluye que si bien la Dirección de Gestión Humana es responsable de la administración, operación y manejo con calidad de los datos del aplicativo SIAP, el agente tecnológico, aparte de brindar soporte técnico al sistema de personal, también debe verificar y revisar periódicamente la calidad de la información que se registra y sale del aplicativo, considerando que la DTSI en coordinación con la oficina de Análisis de Información y Estudios Estratégicos (OAIEE) es la que diseña e implementa un plan de calidad de la información. Por las razones expuestas, se ratifica la observación para verificar las acciones de mejora correspondientes.

- Debilidad en las restricciones de acceso a la información reservada.

Durante las pruebas de auditoría, se identificó que, un número importante de usuarios funcionales tienen acceso a la información de hojas de vida, lo cual constituye un riesgo, debido a que algunos datos tienen el carácter de reservado y la información de menores de edad tiene carácter sensible

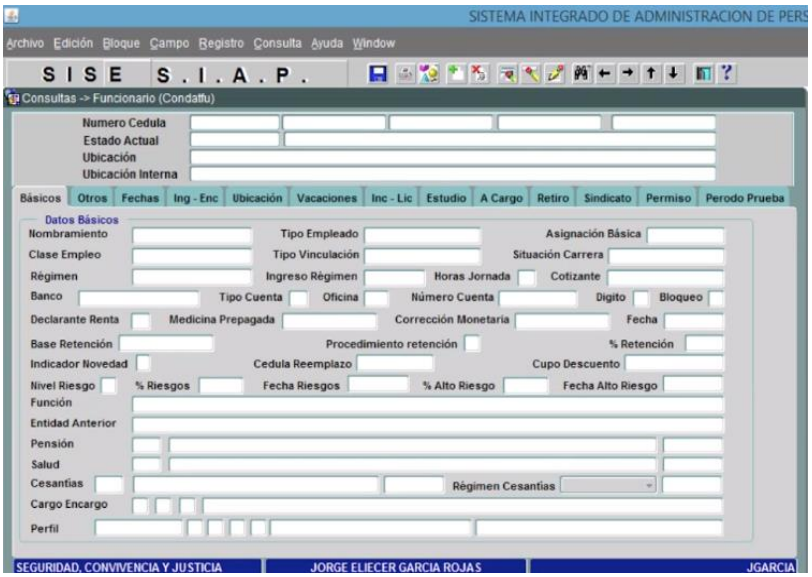


Imagen 15. Módulo Consultas -> funcionarios. Fuente Sistema SIAP

Es claro que, en el ejercicio de las funciones del personal del área de Gestión Humana, deben ingresar a Hojas de Vida, pero es conveniente aplicar protocolos de seguridad de la información, pues esta falta de control genera riesgos asociados a la confidencialidad y privacidad de la información tanto del personal activo como de menores a su cargo.

Frente a lo anterior, la Ley 1266 de 2008, artículo 4, literal G, dejo establecido: ***"Principio de confidencialidad, todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma"*** y la Resolución 645 de 2018, política de protección de datos personales de la SDSCJ.

RESPUESTA DEL AUDITADO

El sistema SIAP permite la creación de usuarios con permisos asociados a cada perfil, los permisos existentes para los usuarios han sido solicitados por la Dirección de Gestión Humana, como dependencia funcional de la solución. Si estos permisos deben ser actualizados, se requiere que el líder funcional solicite dicha actualización.

En este mismo sentido vale la pena aclarar que es el líder funcional de la Dirección de Gestión Humana, quien determina a que usuarios se les asigna privilegios de acceso a las funcionalidades y a la información que posee el Sistema SIAP, esto incluye la información de hojas de vida, en la que algunos datos tienen el carácter de reservado y la contienen la información de menores de edad.

La Dirección de Tecnologías y Sistemas de la Información en su procedimiento Gestión de Requerimientos Tecnológicos PD-GT-15, menciona que la definición de nuevas necesidades o

requisitos como es el caso de la validación mencionada debe ser solicitada por el líder funcional de la Dirección de Gestión Humana con el Formato F-GT-192 Solicitud Solución Tecnológica.

En virtud de lo expuesto, respetuosamente solicitamos al Equipo Auditor no contemplar dentro del informe final la observación realizada.

RESPUESTA OCI:

La administración, operación y otorgamiento de permisos a los diferentes módulos e información en SIAP está a cargo del funcionario que la Dirección de Gestión Humana designe, en este caso del usuario líder funcional del sistema de personal, tal como lo expresa la DTSI, además, esa oficina debe garantizar el cumplimiento del *Principio de confidencialidad de datos personales* de los empleados de la entidad como lo menciona la norma. La observación se mantiene para ser subsanada por la Dirección de Gestión Humana.

8.4. EVALUACIÓN A LA EFECTIVIDAD DE LAS ACCIONES DE MEJORA IMPLEMENTADAS POR EL PROCESO

Teniendo en cuenta que mediante el radicado número 20181300097833 donde se notificó el Informe final de auditoría realizada al proceso de Gestión de Tecnologías de la Información, para la vigencia 2018, se comunicó el siguiente hallazgo:

1.4.1 "Debilidades en el centro de cómputo de la Entidad"

Mediante el Informe Final Auditoria realizada al proceso de Gestión y Análisis de la Información radicado con radicado 20191300095743 para la vigencia 2019, se estableció para el proceso auditado en esta oportunidad, la siguiente observación:

2.2.3.2." Debilidades en la implementación de la política de seguridad de la información, en lo que tiene que ver con: lineamientos y documentación de copias de seguridad y pruebas de restauración, situación que se encuentra definido en el Artículo 15 de la Resolución Interna 541 de 2017 "por la cual se adopta la política de seguridad de la información y se definen lineamientos para su uso, actualización y aplicación", y la norma técnica ISO 27001:2013".

En tal medida debe predicarse que las acciones de mejora establecidas por el proceso no fueron del todo efectivas, pues para el presente ejercicio auditor se configuraron nuevamente las observaciones, tal y como se dejó plasmado en las identificadas con los números:

8.2.1.1. DEBILIDAD EN LA RETENCIÓN DE LOS BACKUPS DE LAS BASES DE DATOS HISTÓRICAS, INCUMPLIÉNDOSE EL ESTÁNDAR ISO 27001, QUE DEFINE EL DOMINIO SEGURIDAD DE LAS OPERACIONES, ENTRE OTROS, CON EL *BACKUP*, QUE TIENE COMO PROPÓSITO PROTEGER A LAS ORGANIZACIONES CONTRA LA PÉRDIDA DE INFORMACIÓN.

8.2.7.1. DEBILIDAD EN LAS CONDICIONES DE SEGURIDAD DEL CUARTO DE PROCESAMIENTO DE DATOS, INCUMPLIENDO EL MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MA-GT-01 Y EXPONIENDO A LA ENTIDAD A HECHOS GRAVES QUE AFECTARIAN NOTABLEMENTE LOS EQUIPOS DE LA DATA CENTER.

9 CONCLUSIONES

9.1 GOBIERNO DIGITAL.

- Se hace necesario revisar las metas alcanzadas en el PETI, vigencia 2019, a fin de asegurar la trazabilidad correspondiente.

- Aplicar en la entidad un enfoque integral de arquitectura empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de Tecnología de la Información y garantizar el aseguramiento de la calidad de la información que es transversal en todos sus procesos internos.

- En los sistemas de información misionales implementar las funcionalidades de accesibilidad de acuerdo con la caracterización de los usuarios y desarrollar un plan de contingencia tecnológica para garantizar la continuidad de los servicios tecnológicos en la entidad y con el fin de mantener la funcionalidad, confidencialidad, integridad y disponibilidad de los recursos tecnológicos y la información.

- Ejecutar el plan y gestión de riesgos de seguridad en la vigencia 2020.

9.2 MSPI.

- Las bases de datos históricas de la entidad deben estar protegidas con una mayor retención de backups.

- Se debe fortalecer el control formal de acceso al cuarto de procesamiento de datos y aislar la tubería del aire acondicionado para evitar incidentes como inundaciones en el Data Center.

- Se hace necesario establecer revisiones periódicas de las restricciones y clasificaciones de acceso a activos de información importantes y formalizar e implementar el procedimiento de etiquetado de activos de la información.

- Es indispensable fortalecer y hacer seguimiento a los compromisos de los proveedores, condiciones indispensables para preservar la seguridad, confidencialidad, integridad y disponibilidad de la información de la entidad.

9.3 SISTEMAS DE INFORMACIÓN.

- *En el módulo PREDIS*, los saltos en el consecutivo de la fecha de emisión de los comprobantes de Disponibilidad Presupuestal de octubre 2019 a junio 2020 ocasionan incertidumbre en la emisión de estos documentos y un posible incumplimiento de las características cualitativas de la información financiera.

- El módulo LIMAY es el receptor final de los datos contables de todos los demás módulos de SICAPITAL.

- En el módulo SISCO, permitir que las transacciones en estado “viable” se puedan reversar para dar celeridad a las operaciones cotidianas de los usuarios y estudiar la viabilidad de la numeración automática de los contratos celebrados en la entidad.

- En el sistema SIAP, se identificó un posible riesgo, asociado a la confidencialidad y privacidad de la información de las hojas de vida.
- En aplicativo LICO no se evidencian quejas del servicio, los pocos errores que se presentan son relacionados con la información entrante del Registro Nacional de Medidas Correctivas.

- El canal de datos que utiliza LICO para conectarse al RNMC es muy seguro, es un servicio Web de comunicación cifrada, se accede a través de código de seguridad.

10 RECOMENDACIONES

10.1 POLITICA GOBIERNO DIGITAL.

- Verificar y establecer con la documentación y evidencias pertinentes el avance real del PETI, en la implementación del sistema de información de la Dirección de Bienes.

- Desarrollar un modelo de arquitectura empresarial integral y llevar acabo la identificación, desarrollo y ejecución de las capacidades necesarias para realizar ejercicios de arquitectura empresarial

- Definir y ejecutar un plan para el aseguramiento de la calidad de la información transversal a todos los procesos tecnológicos y administrativos.

- De acuerdo con la caracterización de usuarios, ciudadanos y grupos de interés de la entidad, implementar las funcionalidades para acceder a los contenidos de los sistemas de información tipo web

- Conformar un plan definitivo, codificado y aprobado de continuidad de los servicios tecnológicos conforme a lo establecido en la política de seguridad de la información, implementando pruebas, con el fin de mantener la funcionalidad, confidencialidad, integridad y disponibilidad de los recursos tecnológicos misionales que sean considerados críticos para la continuidad de la operación en la entidad.

- Continuar con las iniciativas, acciones y proyectos que a la fecha están en curso en la vigencia 2020 de Gobierno Digital, habilitadores Arquitectura y Seguridad de la Información y ejecutar lo que corresponda para lograr un avance del 100% de esa política y cumplir las metas propuestas al término del año en curso.

- Diligenciar la matriz de riesgos de seguridad digital y poner en práctica el plan de tratamiento de riesgos de seguridad de la información.

- Estructurar un plan de auditoria de seguridad y privacidad de la información en concordancia con el ciclo PHVA del sistema de seguridad de la información.

10.2 MSPI

- Establecer una retención de backups de las bases de datos históricas mayor a 3 meses para proteger a la entidad contra la pérdida de información y para garantizar un esquema más robusto de recuperación de información y retención de archivos.

- Formalizar, codificar y aprobar el formato de control de acceso físico a Data Center y/o centro de cableado.

- Definir en la Política de Seguridad y privacidad de la Información y en el Manual correspondiente, los procesos para manejar las desviaciones y las excepciones en la aplicación de la política.

- Precisar las revisiones periódicas de las restricciones y clasificaciones de acceso a activos de información importantes y formalizar e implementar el procedimiento de etiquetado de activos de la información.

- Documentar y ejecutar actividades de seguimiento, evaluación y auditoria a proveedores con respecto al cumplimiento de los compromisos de la seguridad de la información.

- Continuidad del negocio. En el esquema actual de recuperación de la información de las bases de datos en la nube, en caso de una falla mayor del servidor de producción, se demoraría alrededor de 2 horas; crear un ambiente nuevo a otro servidor, cargar el backups de las bases de datos al servidor de contingencia en la nube y actualizar las aplicaciones en cuanto a cadena de conexiones. Con un esquema de servicio más eficiente en la nube, llevando las bases de datos a otro servidor en otra región, se realizaría una transacción de bases de datos online en caso de falla, garantizándose con ello, una disponibilidad inmediata de backups y las aplicaciones seguirían funcionando normalmente, ahora bien, el proceso manual en el nuevo esquema (si llegase a fallar el cambio automático de bases de datos), demoraría unos pocos minutos, mejorándose ostensiblemente el termino de recuperación de la operación.

- Se debe aislar la tubería y ductos del aire acondicionado que están expuestos en el cuarto de procesamiento de datos, Data Center, con en el fin de responder de manera adecuada ante cualquier incidente como inundaciones.

10.3 SISTEMAS DE INFORMACIÓN.

- *Los módulos OPGET, LIMAY, SISCO, SIAP Y PROGRESSUS* deben fortalecer sus informes, contar con generadores de reportes con mayores opciones de parametrización para obtener información de primera mano, filtrada de acuerdo con la necesidad del área, disponible de manera inmediata, flexible, reutilizable, ahorrando tiempo y trabajo en su generación y aumentando el uso y aprovechamiento de la información en la toma de decisiones.

- Definir en la configuración o perfilación de las bases de datos de ORACLE la obligatoriedad de construir las contraseñas a nivel usuario de acuerdo con lo indicado en el Manual de Seguridad de la Información y exigir el cambio periódico de contraseñas, particularmente, en los módulos *SISCO, SIAP y, PROGRESSUS.*

- *Módulo PREDIS*. Revisar las funcionalidades automáticas del sistema presupuestal (control de consecutivos) que permita contar con controles actualizados en la emisión de los CDP, sustentados con los soportes de las transacciones realizadas durante el periodo.

- *Módulo SISCO.* Implementar la reversión de transacciones en estado "viable", para dar celeridad a las operaciones sin necesidad de acudir al ingeniero que da soporte técnico, facilitar por la opción de AYUDAS el manual para los usuarios que permita resolver inquietudes asociadas al manejo del aplicativo, estudiar la posibilidad de implementar el uso de la numeración automática de los contratos emitidos por las dos unidades ejecutoras y concertar este cambio con las otras áreas implicadas en el proceso.

- *Módulo SIAP*. Revisar y ajustar la validación de datos de entrada en el módulo de Hojas de Vida e implementar restricciones específicas de acceso a la información de las hojas de vida, que tiene carácter de reservada y/o datos sensibles.

- *Módulo COPE.* Actualizar el manual del usuario y facilitarlo por la opción de AYUDAS que permita resolver en línea inquietudes asociadas al manejo del aplicativo.

10.4 RECOMENDACIONES GENERALES

- Con relación al habilitador Empoderamiento de los Ciudadanos a través de un Estado Abierto de la Política de Gobierno Digital, es necesario realizar la revisión al estado de la información publicada en la página web oficial para dar cumplimiento a la Ley de Transparencia y Acceso a la Información Pública, a fin de garantizar su actualización y disponibilidad para las partes interesadas.

- Agilizar los trámites con el uso de las TIC, con relación al compromiso de la SDSCJ para la vigencia 2020 en el Plan Anticorrupción y de Atención al Ciudadano – PAAC, en el componente 2 de racionalización de trámites, con el trámite inscrito en el Sistema Único de Información de Trámites – SUIT "Autorización para ingreso como visitante a la Cárcel Distrital de Varones y Anexo de Mujeres.", de las personas privadas de la libertad – PPL.

- Gran parte de una de las paredes del Data Center está terminada en draibol (doble cara), donde está ubicada la puerta de entrada al centro de datos, en la medida que sea posible, entendiendo que las instalaciones de la Secretaría son en calidad de arriendo, construir una pared en material sólido para garantizar la seguridad del Data Center.

- Instalar al interior y en la puerta de acceso del Data Center cámaras de vigilancia estratégicamente ubicadas para obtener un monitoreo y registro continuo y brindar mayor seguridad al recinto de procesamiento de datos.

- En los módulos de SICAPITAL debe implementarse mensajes al usuario funcional en pantalla cuando se interrumpe el servicio por problemas de red, caídas de la conectividad y otros que no tienen que ver con la funcionalidad de los aplicativo, para evitar reclamos y solicitudes inoficiosas a la Mesa de Servicios.

- Continuar con el proceso de la transferencia de conocimientos a partir del agente tecnológico con el fin de brindar un soporte técnico oportuno a y garantizar el funcionamiento de los módulos de SICAPITAL.

- Definir mecanismos de atención para el acompañamiento permanente al grupo de contabilidad responsable de la digitación y consolidación, con el fin de garantizar los resultados esperados.

- En SISCO Implementar mecanismos o reportes de contrarreferencia que permita verificación de los datos de un determinado informe.

- En SISCO y en otros módulos que no lo dispongan, implementar la ayuda, MOSTRAR ERROR, que valide y genere alertas de detección de errores frecuentes para controlar sí al ingresar información o al realizar algún movimiento, el usuario comete algún error, por ejemplo, dejar vacío un campo, el sistema debe informar que se ha presentado una inconsistencia en el ingreso de datos, lo que permite al usuario revisarlo y ajustarlo antes de guardar o procesar datos, así se evitarían inconsistencias e incidentes con la información.

- Acordar con la Policía Nacional, en el marco del Convenio Interadministrativo de Cooperación vigente, un control de calidad en el cobro de multas más efectivo para evitar, que la información recibida del Registro Nacional de Medidas Correctivas en el sistema LICO venga con errores, lo que ocasiona liquidaciones de comparendos equivocadas y que se replican en el módulo de Cobro Persuasivo COPE, generando reprocesos; verificaciones por expediente o por número de cédula, y si persiste el error, solicitudes formales al área de Policía, Grupo Telemática, generando un caso SIGMA.

- El proceso debe diseñar un plan de mejoramiento con acciones de mejora efectivas y sostenibles en el tiempo, pues tal como se indicó en el aparte correspondiente del presente informe, las acciones establecidas por el proceso, que ya habían sido debatidas para

atender observaciones establecidas en ejercicios de auditorías anteriores resultaron ser ineficientes.

Cordialmente,

SILENIA NEIRA TORRES
Jefe Oficina de Control Interno

Proyecto: Juan A. Gutiérrez G.
Auditor OCI