## PERIODO DE EJECUCION

Entre el 24 de noviembre y el 20 de diciembre de 2021, se llevó a cabo evaluación al Data Center Manzana Liévano, cuarto de almacenamiento de medios en el archivo de Bogotá y visita al Centro Alterno de Procesamiento ubicado en el Archivo de Bogotá.

## OBJETIVO GENERAL

Realizar visita al Data Center para establecer la existencias y efectividad de controles de acceso, tomando como marco de referencia mejores prácticas de seguridad, así como evaluar el cumplimiento de la guía GS-037 Guía de Acceso al Data Center, Cuartos Técnicos y Cuartos de Almacenamiento de Medios y del OT-020 Plan de Contingencia TI – DRP.

## ALCANCE

Visita al Data Center ubicado en el Edificio Liévano de la Secretaria General de la Alcaldía de Bogotá. El período de evaluación para la generación de información y toma de muestras de auditoría, corresponderán al periodo comprendido entre 1 de diciembre 2020 y el 30 de noviembre 2021.

## EQUIPO AUDITOR:

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

## METODOLOGIA APLICADA

Para el desarrollo de las pruebas de auditoría se aplicaron las técnicas de auditoría internacionalmente aceptadas tales como indagación, observación, inspección y comprobación selectiva a través de muestreo, entre otros.

## MARCO NORMATIVO:

- Guía GS-037 Guia de Acceso al Data Center, Cuartos Técnicos y Cuartos de Almacenamiento de Medios (2211700-GS-037) Vs 3
- OT-020 Plan de Contingencia TI – DRP (2213200-OT-020) Vs 05
- Caracterización del Proceso Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos (2213200-PO-036 versión 13 del 19 de octubre 2020).
- Mapa de riesgos del proceso con fecha de actualización al 08/09/2021.

## CONCLUSION

Como resultado de las pruebas de auditoría practicadas en las visitas realizadas al Data Center Principal, Cuarto de medios, Centro Alterno de Procesamiento y evaluación del Plan de Contingencia de TI, temas contentivos del proceso Gestión, Administración, y Soporte de Infraestructura y Recursos Tecnológicos a cargo de la OTIC, con el cual se mantiene la disponibilidad de los recursos de tecnología de información y comunicaciones, se concluyó que se encuentran implementados y operando algunos controles asociados a condiciones ambientales en el Data Center como son: sistema de detección y control de incendios, extintores vigentes, mantenimientos periódicos a los Aires acondicionados, existencia de UPS, entre otros.

Así mismo, se cuenta con controles para restricción de acceso físico y lógico al Data Center y físico al Cuarto de almacenamiento de Medios, existencia de un documento de Plan de Contingencia de TI con clasificación de criticidad de los aplicativos y existencia de un Centro Alterno de Procesamiento.

No obstante, se observaron situaciones para las que se requieren acciones correctivas inmediatas y otras susceptibles de mejora, relacionadas con:

- No se cuenta con un plan de contingencia integral y debidamente probado, que garantice la continuidad de la operación de la entidad ante eventos inesperados como desastres naturales, huelgas, motines, etc., generando riesgos de indisponibilidad del servicio e interrupción de la operación de la entidad.
- Adelantar las gestiones para arreglos locativos al Data Center (piso y pared en mal estado)
- Equipos de cómputo y otros elementos que no se encuentran en uso, así como algunos artículos que se encuentran en desorden en la entrada del mismo o en el cuarto contiguo. Así como, estantes para guardar cintas, medios de almacenamiento obsoletos y biométrico para acceso al cuarto de medios en el Archivo de Bogotá.
- Elementos aún bajo responsabilidad del funcionario Oscar Asprilla, anterior jefe de la OTIC, quien ya no labora con la entidad.
- Inexistencia de una herramienta de archivo para controlar la ubicación e identificación de los medios magnéticos respaldados y guardados en el cuarto de medios.
- Diligenciamiento del formato FT-267 para registrar el acceso y actividades realizadas cuando se ingresa al Cuarto de Medios en el archivo de Bogotá.

## OBSERVACIONES Y RECOMENDACIONES PRODUCTO DE LA EVALUACIÓN

Se realizó visita al Data Center principal al Data Center Manzana Liévano, cuarto de almacenamiento de medios en el archivo de Bogotá y visita al Centro Alterno de Procesamiento ubicado en el Archivo de Bogotá para establecer la existencia y efectividad de controles de acceso, condiciones ambientales y almacenamiento de medios que permitan la recuperación ante una contingencia tecnológica.

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

## 1. Plan de Contingencia – Centro de Procesamiento Alterno

### Observación No. 1

Analizado el documento OT-020 Plan de Contingencia DRP, realizada la visita al centro de procesamiento Alterno ubicado en las instalaciones del Archivo de Bogotá y realizada la reunión con el funcionario de la OTIC a cargo de la implementación del Plan de Contingencia Tecnológico, se observó que se cuenta con algunos equipos alternos para la recuperación de bases de datos y configuraciones de equipos de comunicaciones en caso de un evento de contingencia, sin embargo, en la actualidad la Entidad no cuenta con un Plan de Contingencia en funcionamiento debidamente aprobado y probado que garantice la continuidad de las operaciones de la Secretaria General en caso de ocurrir eventos inesperados. A continuación, mencionamos algunos de los aspectos identificados:

- No se cuenta con evidencia de la existencia de un Comité de Contingencia como se indica en uno de los roles definidos en el numeral 6.2.2 Roles específicos, del documento mencionado OT-020 Plan de Contingencia DRP de la Entidad, tampoco se evidencia la implementación de los roles allí definidos como son el de Jefe e OTIC, Oficial de Seguridad de la información, Líder Plan de Contingencia, Coordinador de Infraestructura, Gestores Plan de Contingencia, específicamente relacionado a responsabilidades antes, durante y después de la contingencia.

- En el documento OT-020, numeral 6.2.5 Aplicativos, se observó el inventario de Sistemas de Información clasificados según su criticidad. En este mismo documento, en su numeral 6.2.3 se hace referencia a un link con los equipos de cómputo que hacen parte del alcance del Plan de Contingencia DRP, link que no está disponible y no se recibió respuesta a la solicitud realizada en memorando de apertura de la auditoría 3-2021-31859 del 25 de noviembre.

- No se recibió respuesta referente a los eventos de contingencia presentados durante el período de evaluación, por lo tanto, no es factible concluir respecto a la existencia o no de los mismos, y su gestión en caso de haber ocurrido.

- No se han realizado pruebas a Plan de Contingencia definido en el documento OT-020 – Plan de Contingencia de TI, perteneciente al proceso Gestión Administración y Soporte de Infraestructura y Recursos Tecnológicos publicado en el SIG (Sistema Integrado de Gestión), ni se observa una planeación encaminada a actualizar el Centro Alterno de Procesamiento, poner en funcionamiento un plan de contingencia bajo diferentes escenarios de caídas de servidores, fallas en la infraestructura, pérdida de información e incluso eventos de desastre naturales y/o provocados con dolo o intensión, dificultando o imposibilitando la recuperación efectiva y eficiente de los servicios tecnológicos en caso de presentarse interrupciones en la infraestructura tecnológica.

- No se evidencia la definición de las principales variables a tener en cuenta en un Plan de Contingencias como son el RTO (Recovery Time Objetive) y RPO (Recovery Point Objective) que requieren ser determinadas para cada uno de los Sistemas de Información clasificados como críticos para la entidad o el core del negocio.

- El Centro Alterno de Procesamiento se encuentra ubicado en la misma zona geográfica, cercano al Data Center Principal, lo que conlleva que tenga los mismos riesgos de pérdida de información o indisponibilidad en caso de fallas naturales como terremotos o inundaciones por lluvias, o también ante eventos provocados como huelgas, motines, bombas, etc.

Es indispensable continuar con el proceso de evaluación de escenarios de contingencia, realizar las propuestas de mejoramiento a los niveles directivos de la entidad, con el fin de implementar un plan de contingencia integral que contemple aspectos importantes como: ubicación geográfica del Centro Alterno diferente a la ubicación geográfica del Data Center, definición del RTO (Recovery Time Objetive) y RPO (Recovery Point Objective) para cada uno de los sistemas críticos de la operación, planificación y ejecución de pruebas integrales que permitan a la entidad estar preparada y dar continuidad a la operación y servicio al ciudadano ante eventos inesperados de contingencia tales como: caídas de servidores, fallas en la infraestructura, pérdida de información e incluso eventos de desastre naturales y/o provocados.

## 2. Visita al Data Center Piso 3 Manzana Liévano

Realizada la visita al sitio donde se encuentra ubicado el Data Center principal de la Secretaria General en el piso 3 de la Manzana Liévano, se observó que el Centro de Procesamiento de Información cuenta con controles adecuados de restricción de acceso (puerta metálica y puerta de vidrio con control biométrico por huella), también cuenta con los rack de servidores y equipos de comunicaciones debidamente ordenados, sistema de detección y extinción de incendios, UPS con sus respectivas baterías, y aire acondicionado.

### Oportunidad de Mejora No. 1:

Se encontró en mal estado una parte del piso del Data Center, ya que se observó que algunas baldosas se encuentran levantadas con riesgo de accidente laboral (tropiezo y/o caída) por parte de los colaboradores que ingresan al lugar. Así mismo, se encontró una pared en mal estado.

Durante la etapa de ejecución de la auditoría, la OTIC gestionó el arreglo del piso y con fecha 17 de diciembre (durante el proceso de cierre de esta auditoría) se recibió soporte del cierre del caso GLPI No. 0237215, con el cual se dio solución a la situación encontrada por esta Auditoría en visita realizada el 30 de noviembre de los corrientes. Se sugiere evaluar la necesidad de realizar arreglos locativos a la pared que se encontró deteriorada.

### Recomendación No. 1

Se encontraron algunos artículos en desorden como cajas y toma corrientes en el cuarto contigüo al Data Center, estructuras metálicas dentro del data center y un monitor y CPUs en el suelo a la entrada del Data Center. De acuerdo con la respuesta recibida de la OTIC recibida al informe preliminar se sugiere revisar la ubicación y orden de los elementos indicados.

**Oportunidad de Mejora No. 2**

Se observaron equipos de cómputo que no se encuentran en uso, como un rack de comunicaciones dentro del Data Center, como por ejm los equipos con placa: 56681, 13927, 25203, así como otros equipos sin placa de inventario también en desuso y ochenta y dos (82) elementos a nombre del Ingeniero Oscar Javier Asprilla, quien ya no labora en la entidad desde el 9/05/2021.

Se deben realizar las gestiones con la Subdirección de Servicios Administrativos y el Comité PIGA, para dar de baja los elementos que ya no se utilizan y darles el destino final adecuado según lineamientos ambientales actuales para este tipo de elementos de cómputo.

**3. Visita Centro de Almacenamiento de Medios – Archivo de Bogotá**

**Oportunidad de Mejora No. 3**

Realizada la visita presencial al sitio donde se encuentra ubicado el cuarto de almacenamiento de medios en el piso 3 del Archivo de Bogotá, se observó que el cuarto cuenta con medidas mínimas de control de acceso con puerta metálica con llave física para su ingreso, en el exterior del cuarto se cuenta con extintor para equipos de cómputo y las cintas se encuentran organizadas en cajas de cartón encima de un escritorio. Se observaron las siguientes situaciones susceptibles de mejoramiento:

- Estantería metálica para guardar cintas sin uso.
- Biométrico para control de acceso no se usa.
- No se lleva bitácora de acceso (Formato FT-267), incumpliendo lo establecido en el numeral 3.2 de la guía GS-037 – Guía de Acceso a Data Center, Cuartos Técnicos y Cuartos de Almacenamiento de Medios, donde se debe registrar las actividades realizadas.

Se sugiere revisar las medidas de control de acceso, organización y condiciones de almacenamiento de las cintas de backup en el cuarto de almacenamiento y realizar devolución de los elementos sin uso, definir necesidad de conservar y/o destruir los medios de almacenamiento obsoletos y organizar el cuarto según las necesidades tecnológicas que se requieran.

**Oportunidad de Mejora No. 4**

Respecto a los medios de almacenamiento, se observaron las siguientes situaciones:

- Los backups que se observaron en cintas, no cuentan con una identificación externa y/o interna que permita conocer y restaurar de forma rápida y eficiente una copia de respaldo de un Sistema de Información. Se aclara que las cintas están identificadas externamente según el servidor, pero no se cuenta con una herramienta de archivo que permita consultar tipo de backup, fecha, sistema de información, lugar de ubicación, entre otra información que permita una restauración rápida y eficiente.

- En el cuarto de medios se evidenciaron elementos en desorden (cajas, cables, copias de respaldo en cintas obsoletas, CDs, etc.

- Algunas cintas en formato antiguo (obsoletas) que se encuentran ubicadas en un escritorio del cuarto de medios, sin organización y para su lectura ya no se cuenta con un equipo que permita su consulta, son cintas Sony Ultrium 4, 5 y 6.

Evaluar la posibilidad de incluir como parte de los elementos que se archivan y son controlados por el Sistema de Información del Archivo, los medios magnéticos, de tal forma que, se tenga identificado en detalle la información respaldada, fechas, tiempo de almacenamiento en archivo, ubicación en depósitos, con facilidad de ser consultada y restaurada a partir de los registros existentes en el Sistema de Información del Archivo (Numero de cinta, estante, numero de depósito, año, tipo de información, sistema de información, etc).

**Plan de Mejoramiento**

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

Criterios de clasificación de conceptos derivados de la auditoría.

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

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