

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	1 de 15

INFORME EJECUTIVO

Evaluación Seguridades Lógicas y Físicas al Centro de Cómputo, Cuartos de Comunicaciones y Cuartos de Almacenamiento de Medios

PERIODO DE EJECUCION

Entre el 4 de abril y 17 de mayo de 2024, en cumplimiento del Plan Anual de Auditoría aprobado para el 2024, se realizó evaluación de Seguridades Lógicas y Físicas al Centro de Cómputo, Cuartos de Comunicaciones y Cuartos de Almacenamiento de Medios.

OBJETIVO GENERAL

Establecer la aplicación adecuada de los controles lógicos y físicos en el Data Center, cuartos de comunicaciones y cuartos de almacenamiento de medios; evaluar los controles existentes para la administración del inventario, la instalación/desinstalación y monitoreo de los elementos, en los Data Center y cuartos de comunicaciones; así como la gestión de riesgos respectiva.

ALCANCE

La ejecución pruebas de auditoría sobre el período comprendido de 1 de abril 2023 a 31 de marzo 2024, correspondientes a:

- Registros de control de acceso físico al Data Center, cuartos de comunicaciones y de almacenamiento de medios
- Control de acceso lógico (biométrico)
- Aplicación lista de chequeo para condiciones físicas y ambientales del Data Center:
- Inventario de equipos de cómputo que se encuentran en el Data Center y Cuartos de comunicaciones y demás sitios de procesamiento (según aplique).
- Almacenamiento externo de medios de respaldo.

EQUIPO AUDITOR

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

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195



	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	2 de 15

METODOLOGIA APLICADA

Se realizó solicitud de información a las dependencias OTIC y Subdirección Servicios Administrativos, se analizó el procedimiento para mantenimiento de infraestructura tecnológica y la guía relacionada de acceso al Data Center, cuartos técnicos y cuartos de almacenamiento de medios, y se realizaron pruebas de integridad de la información con el inventario de equipos de cómputo de la entidad (SAI/SAE).

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

De acuerdo con la población, para cada prueba de auditoría a practicar se genera la muestra aleatoria objeto de evaluación con el Papel de Trabajo en Excel respectivo para el periodo objeto de evaluación definido.

MARCO NORMATIVO:

- Procedimientos y Guías SIG:
 - ✓ Caracterización del Proceso Gestión de Servicios Administrativos y Tecnológicos (4233100-CR-033 V10 del 30 de mayo de 2023)
 - ✓ Procedimiento Mantenimiento de la Infraestructura Tecnológica y del proceso Gestión de Servicios Administrativos y tecnológicos (4204000-PR-104 versión 13 del 23 de agosto de 2023).
 - ✓ Guía de acceso a data center, cuartos técnicos y cuartos de almacenamiento de medios (4204000-GS-037 Versión 3 del 20 de junio 2018)
- Manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI (4204000-MA-031) V6 de 25/01/2024.
 - ✓ 12.5.1 Política para Control de Acceso
 - ✓ 12.7.1 Política para seguridad física y del Entorno
 - ✓ 12.7.3 Controles para la seguridad física y del entorno
- ISO 27001:2013:
 - ✓ A.8.1 Responsabilidad por los Activos
 - ✓ A.8.3 Manejo de Medios
 - ✓ A.9 Control de Acceso
 - ✓ A.11 Seguridad Física y del Entorno

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	3 de 15

CONCLUSION

Como resultado de la evaluación realizada a las Seguridades Lógicas y Físicas al Centro de Cómputo, Cuartos de Comunicaciones y Cuartos de Almacenamiento de Medios entre el 1 de abril 2023 y el 31 de marzo 2024, se encontró que, los mecanismos de control existentes para el acceso, mantenimiento de las UPS, AA y equipos de cómputo del Data Center, así como las seguridades para el almacenamiento de cintas, son adecuados para el tipo de Centro de Computo (Tier 2) y brindan un grado de efectividad, encontrado los siguientes aspectos:

- Se cuenta con controles normados en la guía de acceso a data center, cuartos técnicos y cuartos de almacenamiento de medios, que hace parte del procedimiento “Mantenimiento de la Infraestructura Tecnológica y del proceso Gestión de Servicios Administrativos y tecnológicos, del proceso “Gestión de Servicios Administrativos y Tecnológicos (PR-104 V13).
- Se gestionaron las situaciones recomendadas en el informe resultado de la auditoría realizada con vigencia 2021, con relación en arreglos locativos, devolución de equipos de cómputo que no se encontraban en uso, organización y reubicación del cuarto de medios y la organización de la entrada al centro de cómputo.
- El Data Center Principal, el Data Center alterno y el cuarto de medios, cuentan con una adecuada organización, controles de acceso por puerta con cerradura (DC alterno), tarjeta de proximidad y biométrico de huella digital (DC principal), cableado organizado, cintas organizadas y bien dispuestas, temperatura de los sitios adecuada, aire acondicionado, sistema de detección de incendios y extintores manuales con recarga vigente, Circuito Cerrado de Televisión (CCTV) en el Data Center Principal y bitácora para control de acceso de visitantes a los sitios auditados.

Sin perjuicio de lo anterior, producto de las pruebas practicadas se identificaron dos (2) oportunidades de mejora y se formulan algunas recomendaciones que, al ser adoptadas propenderán por fortalecer y mejorar la efectividad de los controles y la dinámica de la operación relacionada con la administración de los Centros de Cómputo Principal y Alterno, y el cuarto de almacenamiento de medios, así:

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	4 de 15

OPORTUNIDADES DE MEJORA

- Se encontró durante la visita de auditoría que, los 27 activos revisados aleatoriamente en el Data Center Principal y al Data Center Alterno, figuran aún a cargo del anterior jefe de la OTIC (Rafael Londoño Carantón y Roberto Rommel DiazGranados Díaz), quien se retiró de la entidad el 1 de febrero de 2024. Así mismo, se analizó si existen equipos de cómputo asignados a funcionarios retirados de la entidad, evidenciando que 433 están a nombre del jefe de la OTIC retirado el 1/02/2024 y 5 a nombre del jefe de la OTIC retirado el 15/07/2023. Por lo tanto, se requiere que desde la OTIC se haga la verificación de la existencia física de dichos elementos, con el fin de actualizar el inventario y realizar la entrega al responsable de los bienes que considere designar en dicha dependencia, asimismo, de manera simultánea adelantar el trámite requerido ante la Subdirección de Servicios Administrativos.

Este mismo sentido, se recomienda a la Subdirección de Servicios Administrativos gestionar con las dependencias correspondientes las acciones correctivas encaminadas a actualizar el inventario de equipos que aún se encuentran a cargo de funcionarios desvinculados de la entidad para que sean reasignados a los responsables de su manejo y control. Las dependencias con esta situación al corte de marzo 2024 son: Oficina de Consejería Distrital de Paz, Víctimas y Reconciliación, Subsecretaría Distrital de Fortalecimiento Institucional, Subdirección e Gestión del Patrimonio Documental del Distrito, Dirección de Contratación, Dirección de Paz y Reconciliación, Dirección de Reparación Integral y Despacho Secretaria General.

- Se identificaron dos (2) Aires Acondicionados (placas de inventario No. 12636 y 12637), ubicados en el centro alternativo de procesamiento que no se encuentran en funcionamiento, a los cuales no se les ha realizado mantenimiento desde el año 2021, y de acuerdo con la respuesta obtenida de la SSA informó que se tiene programado abordar su desmonte en el marco del contrato que se suscriba para el mantenimiento de aires acondicionados, por tal razón, es importante dar celeridad a la gestión para tramitar los requerimientos de darlos de baja, siguiendo los lineamientos establecidos en el procedimiento Egreso o salida definitiva de bienes (PR-236 V8).

Teniendo en cuenta las situaciones mencionadas anteriormente, es importante llevar a cabo las siguientes acciones:

Cra 8 No. 10 - 65
 Código postal 111711
 Tel: 381 3000
 www.bogota.gov.co
 Info: Línea 195



	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	5 de 15

- La OTIC realice prontamente las gestiones correspondientes para efectuar la entrega y reasignación de equipos de cómputo a la jefe actual de la OTIC o a quien se designe, previa confirmación de la existencia física de los activos, que se encuentran asignados a los jefes anteriores de la OTIC, quienes ya no tienen relación laboral con la entidad. Al igual que, realizar los trámites requeridos de la devolución de los Aires Acondicionados del Data Center Alterno, que no están en funcionamiento.
- Implementar la acción correctiva para asignar el responsable de los equipos de cómputo que al corte de la auditoría (31 de marzo de 2024) se encontraban aún a cargo de funcionarios ya retirados de la entidad.
- Dar celeridad a la gestión de dar de baja los dos (2) Aires Acondicionados ubicados en el Data Center Alterno (Sede Archivo de Bogotá), cumpliendo los lineamientos establecidos en el procedimiento Egreso o salida definitiva de bienes (PR-236 V8).

RECOMENDACIONES

- El panel para controlar el equipo de extinción de incendios EVO SYSTEMS con agente NOVEC1230, no está certificado de acuerdo con las normas NFPA 72 y NFPA 2001, y una situación significativa es que el sistema no lleva a cabo la liberación autónoma del agente extintor, generándose un potencial riesgo de no lograr la extinción del fuego oportunamente, en caso de presentarse un conato de incendio. Por lo anterior, y teniendo en cuenta que las capacitaciones en el uso de extintores se realizan a los brigadistas, se recomienda coordinar con la SSA para extender estas charlas a todos los funcionarios de la OTIC, en caso de requerirse su uso.
- Gestionar las acciones encaminadas a asegurar la correcta liberación de manera autónoma del agente extintor y evaluar la pertinencia de llevar a cabo la certificación del panel de control, con el propósito de garantizar su correcto funcionamiento, al igual que, formular acciones para realizar el proceso de formación de los colaboradores de la dependencia en el uso de extintores y del SEDI.
- Desde la SSA consultar con la DTH, la pertinencia de contar con dos extintores en el Data Center Alterno y gestionar la ubicación del extintor faltante en el lugar dispuesto para tal fin, o de lo contrario, reubicar el letrero actual de señalización en caso de no ser requerido, con el fin de contar con los elementos necesarios y suficientes en caso de necesitar su uso en un conato de incendio.

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	6 de 15

- Es necesario evaluar la infraestructura de contingencia con que se cuenta actualmente en la entidad, para el análisis de costo/beneficio y estudiar las diferentes opciones para implementar y/o actualizar un Data Center Alterno y la puesta en marcha del funcionamiento de un plan de contingencia que permita dar continuidad a la operación en caso de falla total o parcial del Centro de Computo Principal y restablecer la operación normal de la plataforma tecnológica, en caso de la ocurrencia de un evento o la materialización de un riesgo de TI que afecte el funcionamiento correcto de los servicios informáticos críticos de la entidad.

RESULTADO DE LAS PRUEBAS PRACTICADAS

A continuación, se describen los principales aspectos como la observación identificada, oportunidades de mejora y las recomendaciones formuladas como resultado de las pruebas practicadas:

1. Normatividad Interna - Procesos, Procedimientos y Guías

Una vez evaluada la normatividad interna publicada en la herramienta de gestión Daruma, se observó que la guía de acceso a data center, cuartos técnicos y cuartos de almacenamiento de medios (GS-037), hace parte de los documentos contentivos del procedimiento “Mantenimiento de la Infraestructura Tecnológica y del proceso Gestión de Servicios Administrativos y tecnológicos” (PR-104), del proceso “Gestión de Servicios Administrativos y Tecnológicos” (CR-033), con los formatos asociados: el FT-743 – Ubicación Física en cuarto de medios y FT-267 Bitácora de acceso a centros de cómputo y cuartos de comunicaciones

Al respecto, de la documentación que define los controles físicos y lógicos para el acceso al Data Center, cuartos de almacenamiento, cuartos técnicos y cuartos de almacenamiento de medios, se encuentra publicada en la herramienta Daruma como los lineamientos establecidos están normados en la guía GS-037 Guía de acceso a data center, cuartos técnicos y cuartos de almacenamiento de medios V3 con fecha de publicación 20/06/2018. Teniendo en cuenta que la fecha de publicación corresponde a las actividades definidas en el año 2018, se recomienda realizar una verificación de lo documentado frente a las actividades realizadas periódicamente, con el fin de asegurar que los controles allí establecidos son eficaces y se encuentran vigentes y/o para la actualización de este documento en caso de considerarse necesario.

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	7 de 15

2. Data Center Principal – Manzana Liévano

En visita realizada el 18 de abril de 2024 al Data Center Principal ubicado en el edificio Manzana Liévano, se observó lo siguiente:

- ✓ Buena iluminación artificial.
- ✓ Acceso con tarjeta de proximidad en la primera puerta de acceso y acceso con biométrico de huella digital para acceso al Data Center, ambos en funcionamiento y con restricción de acceso únicamente a las personas autorizadas que lo requieren para el desempeño de sus funciones.
- ✓ Identificación del sitio con letrero con el nombre “Centro de Cómputo”
- ✓ Equipos y cableado organizado.
- ✓ Circuito Cerrado de Televisión (CCTV) en funcionamiento.
- ✓ Sistema de Detección y extinción de Incendios, el cual funciona para detección, pero no para extinción.
- ✓ Un extintor tipo ABC Multipropósito externo al Data Center, en el hall de ingreso ubicado a la entrada del Data Center, con carga vigente hasta agosto 2024.
- ✓ Estantes para ubicación de cintas debidamente organizados, en el hall antes de ingreso al Data Center.
- ✓ Las cintas se encuentran debidamente etiquetadas con fecha y descripción.
- ✓ Aire Acondicionado para regular la temperatura en el Data Center, en funcionamiento.
- ✓ Cuenta con Bitácora de acceso (formato FT-267 V3, dispuesto para tal fin) para registrar a las personas que ingresan al Data Center (colaboradores o proveedores), se recomienda diligenciar el formato completamente, puesto que se evidenciaron algunos sin diligenciamiento de la hora de salida del funcionario visitante que ingresó.

Se evidenció que se realizaron mantenimientos correctivos y preventivos a los servidores del Centro de Cómputo:

- ✓ Se llevó a cabo mantenimiento correctivo (cambio de board) el día 14/4/2023 para los equipos Dell M1000e. Caso 290296
- ✓ Se llevó a cabo mantenimiento preventivo (anual) y correctivo (SW core) el día 2/4/2023 para los equipos Dell M1000e. Caso 295273
- ✓ Se llevó a cabo actualización de los servidores Windows los días 16/11/2023, 27/2/2024 y 14/3/2024.
- ✓ Se cumple con las condiciones establecidas en el procedimiento en cuanto al “Mantenimiento de la infraestructura tecnológica PR-104”

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	8 de 15

Una vez analizado el archivo recibido de la OTIC (Diagrama de Rack Datacenter Liévano y Archivo de Bogotá.xlsx) con la relación de servidores del Data Center vs los soportes de mantenimiento realizados, se recomienda incluir como parte del instrumento de control (Diagrama Rack Data Center), el detalle de los servidores que tienen garantía, los que están programados para mantenimientos preventivos anuales, y realizar el análisis de riesgo para los que no cuentan con un plan de mantenimiento ni preventivo ni correctivo.

Para la vigencia 2023, se observó la realización de los siguientes mantenimientos a los Aires Acondicionados del Centro de Cómputo Principal en cumplimiento a las condiciones establecidas en el procedimiento “Mantenimiento de la infraestructura tecnológica PR-104”:

- ✓ Se llevaron a cabo un total de seis (6) mantenimientos para dos equipos ubicados en el Edificio Liévano piso 3, tanto preventivos como correctivos.
- ✓ Se llevaron a cabo tres (3) mantenimientos para el equipo con serial 95926, ubicado en el Edificio Lievano P3
- ✓ Se llevaron a cabo tres (3) mantenimientos para el equipo con serial 801001, ubicado en el Edificio Lievano P3

Recomendación No. 1

Una vez analizado el informe general de la inspección, pruebas y mantenimiento efectuado en el mes de noviembre de 2023, al sistema de detección y extinción de incendios Alcaldía de Bogotá (equipo EVO SYSTEMS con agente NOVEC 1230), se identificó que se realizaron actividades como: activación de estaciones manuales, verificación del funcionamiento de la sirena estrobo y el switch de baja presión, las cuales se surtieron con normalidad y resultados satisfactorios.

No obstante, en el mismo reporte se informa que el panel para controlar el equipo no está certificado de acuerdo con las normas NFPA 72 y NFPA 2001, y una situación significativa es que, el sistema no lleva a cabo la liberación autónoma del agente extintor, situación que, aunada a la falta de evidencia respecto a la participación de los funcionarios de la dependencia en capacitaciones en el uso de extintores alternos y en el Sistema de Extinción de Incendios (SEDI).

Durante la visita realizada al Data Center principal, la OTIC informó a la auditora, que se tenía identificada la falla por medio del informe reportado en el mantenimiento realizado en 2023 y que actualmente se encuentra en proceso de contratación para la vigencia 2024.

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	9 de 15

En respuesta recibida de la OTIC al informe preliminar, se menciona que ya se encuentra en proceso de contratación el mantenimiento para el Sistema de Extinción, razón por la cual se solicita registrar esta acción que se viene adelantando, como una acción correctiva en la herramienta Daruma, con el fin de realizar seguimiento posteriormente según las fechas establecidas para la realización del mantenimiento mencionado.

Asimismo, se recomienda formular acciones para llevar a cabo el proceso de formación de los colaboradores de la dependencia en el uso de extintores y del SEDI.

3. Cuarto Medios de Almacenamiento y Data Center Alterno (Sede Archivo de Bogotá)

En visita realizada el 26 de abril de 2024 a la sede del Archivo de Bogotá, donde se encuentra ubicado el Data Center alerno y el cuarto de medios de almacenamiento, se observó:

- ✓ Buena iluminación artificial.
- ✓ Acceso con tarjeta de proximidad en una primera puerta para ingreso al hall compartido entre ambos sitios (Data Center Alterno y Cuarto de medios). Por medio de la tarjeta de proximidad, se otorga acceso únicamente a los funcionarios autorizados.
- ✓ Puerta de acceso con llave mecánica/manual independiente al Cuarto de Cintas Magnéticas y otra independiente al DC Alterno. Las llaves son administradas y se encuentran a cargo de los funcionarios responsables de la OTIC.
- ✓ Identificación de los sitios (Data Center y Cuarto de Cintas Magnéticas) con un aviso de papel impreso con el correspondiente nombre del sitio.
- ✓ Un extintor tipo ABC Multipropósito externo a ambos cuartos, ubicado en el hall cercano a la puerta del cuarto de cintas; asimismo un extintor al interior del Data Center alerno, ambos con carga vigente hasta octubre de 2024.
- ✓ Estantes móviles verticales para almacenamiento de las cintas.
- ✓ Las cintas se encuentran debidamente etiquetadas con fecha y descripción
- ✓ Aire Acondicionado en funcionamiento para regular la temperatura en el Data Center.
- ✓ Cuenta con Bitácora de acceso (formato FT-267 V3, dispuesto para tal fin).

Oportunidad de Mejora No. 1

- Se identificaron dos (2) Aires Acondicionados (placas de inventario No. 12636 y 12637), ubicados en el centro alerno de procesamiento que no se encuentran en funcionamiento, la última fecha de mantenimiento registrada en la bitácora fue del 25/03/2021 y 26/03/2021.

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	10 de 15

Teniendo en cuenta la respuesta al informe preliminar recibida de la SSA, donde informan que ya se realizó análisis de costo/beneficio y que no es viable la inversión requerida para el mantenimiento correctivo, al igual que informó: “...se tiene programado abordar el desmonte de los dos equipos en el marco del siguiente contrato de mantenimiento de aires acondicionados que se suscriba, para su posterior reintegro al almacén”, se mantiene la oportunidad de mejora y se solicita registrar en la herramienta Daruma, el plan de acción correctivo como se mencionó en la respuesta al informe preliminar, con el fin de poder realizar el seguimiento correspondiente como parte del proceso de mejora continua en el proceso de desmonte y dada de baja de los elementos.

Al respecto, se resalta que el sitio del Data Center Alterno, cuenta con un Aire Acondicionado que funciona correctamente por lo que el riesgo de daño de los equipos de cómputo por condiciones de temperatura está debidamente mitigado.

Recomendación No. 2

- En el Data Center Alterno, se observó una señalización de extintor sin estar allí ubicado el aparato. No obstante, se observó que en otro sitio a unos pocos metros de distancia también con señalización si se cuenta con el elemento debidamente ubicado y vigente, por lo anterior, y de acuerdo con la respuesta recibida de la SSA al informe preliminar.

En respuesta recibida de la SSA al informe preliminar, se menciona que: “Respecto al extintor que no estaba en su lugar, es posible que se haya ubicado temporalmente en otro lugar. Por lo anterior, se consultará con el personal del Archivo de Bogotá para buscarlo y ubicarlo en el lugar que corresponde de acuerdo con la señalización” y “con relación a los extintores, la cantidad, ubicación y señalización no la decide la SSA, sino que, se realiza atendiendo las directrices de la Dirección de Talento Humano, de acuerdo con los lineamientos de Administradora de Riesgos Laborales y la normativa vigente de Seguridad y Salud en el Trabajo.”

Dado lo anterior, se recomienda consultar con la Dirección de Talento Humano, los lineamientos de la Administradora de Riesgos Laborales y la normativa vigente de Seguridad y Salud en el Trabajo para definir sobre la necesidad o no de contar con dos extintores, y en tal caso, poner el extintor faltante o de lo contrario reubicar el letrero actual no requerido.

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	11 de 15

- No se observó control de Circuito Cerrado de Televisión (CCTV) para el monitoreo de ingreso al sitio, lo cual es importante en caso de requerirse determinar alguna responsabilidad por pérdida y/o daño de equipos o medios magnéticos, por lo tanto, es necesario coordinar evaluar en conjunto con la SSA la pertinencia de implementar al menos una cámara al interior del DC Alterno, con el propósito de tener control y registro sobre los equipos y en caso de eventualidad o novedad poder establecer responsabilidades ante algún evento de daño, pérdida o robo.
- Asimismo, referente al control de acceso con tarjeta de proximidad al hall por el cual se ingresa a ambos sitios (cuarto de medios y DC Alterno), y teniendo en cuenta que el control de acceso de ambos sitios es con llave física mecánica, se recomienda consultar con la SSA quienes cuentan con copia de las llaves físicas, al igual que consultar quienes tienen acceso en el biométrico, con el fin que desde la OTIC se cuente con un control de monitoreo puesto que ambos sitios tienen equipos e información administrada y bajo responsabilidad de la OTIC.

4. Inventario de Activos (equipos de cómputo, aires acondicionados y Sistema detección y extinción de incendios)

Oportunidad de Mejora No. 2

- De 27 activos (23 equipos de cómputo, 3 Aires Acondicionados y 1 equipo de detección y extinción de incendios), tomados aleatoriamente durante la visita presencial realizada al Data Center Principal y al Data Center Alterno y Cuarto de Medios de Almacenamiento, se observó que el 100% de los seleccionados se encuentran registrados en el inventario de la entidad (aplicativo SAI/SAE); no obstante, se observó que al momento de la auditoría, los 27 activos se encuentran a cargo del anterior jefe de la OTIC, quien se retiró de la entidad el 1 de febrero de 2024.

Una vez recibida la respuesta de la SSA al informe preliminar, se observa que para el elemento identificado con placa 82777 se realizó el ajuste en el sistema de información de inventarios SAI/SAE con respecto a la novedad de ubicación cambiándola del Edificio Liévano al Archivo de Bogotá, tarea realizada como resultado de este informe de auditoría.

Adicionalmente, y con respecto a la ubicación de los elementos según registro en el aplicativo de inventarios vs la ubicación física del elemento, como lo indica la SSA en respuesta al informe preliminar: *“En el marco de la Toma Física de Inventarios se están abordando las actualizaciones de ubicación”*; por lo tanto, se recomienda dar continuidad a las labores que actualmente ya se tienen

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	12 de 15

planeadas y se vienen adelantando en el marco de la toma física de inventarios y actualización de la ubicación física del elemento con relación al registro en el sistema de inventarios SAI/SAE.

Se realizó prueba para verificar equipos de cómputo asignados a otros funcionarios retirados de la entidad, identificando doce (12) exfuncionarios con esta condición; uno de ellos el exjefe de la OTIC retirado el 15/07/2023 y los once (11) restantes de diferentes dependencias retirados con fechas de retiro entre el 23/01/2024 y el 26/03/2024.

En razón a lo anterior, se incumple con las políticas de Seguridad de la Información, los controles definidos en la norma ISO27001:2013 y lo establecido en el procedimiento Movimiento de Bienes (PR-233 V8), así:

- Manual políticas y controles de seguridad y privacidad de la información y políticas de TI V6, que en su numeral 12.4 Gestión de Activos, establece:

“Todos los servidores públicos, contratistas y proveedores deben hacer entrega de los activos de información que se encuentran bajo su custodia al terminar su contrato y/o cada vez que el mismo haga cambio de dependencia o responsabilidades al interior de la entidad.”

- *“Cuando el servidor público o contratista se retire de la Entidad, deberá hacer la respectiva devolución de los activos de información a su cargo donde repose los datos e información que durante su vinculación laboral generó, administró, modificó y custodio para el desarrollo de las funciones y responsabilidades asignadas”*
- ISO 27001:2013 que en el anexo A control A.8.1.4 – Devolución de activos, indica: *“todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.”*
- Procedimiento Movimiento de Bienes (PR-233 V8), numeral 5.Condiciones Generales – título Expedición de la constancia de devolución de bienes y cancelación de servicios (paz y salvo), que dice: *“Los servidores, contratistas o terceros con bienes a cargo deberán entregar la totalidad de sus elementos al jefe de la dependencia o a quien éste designe, según lo señalado en la Resolución 001 de 2019 “Manual de Procedimientos Administrativos y Contables para el Manejo y Control de los Bienes en las Entidades de Gobierno Distrital...”*

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	13 de 15

La SSA informa que: “De manera cuatrimestral, se solicita a la Dirección de Talento Humano la base de datos con novedades de nómina, en la cual se relacionan los funcionarios desvinculados. Dicha información, se cruza con los registros de inventarios con el fin de identificar bienes a cargo de funcionarios desvinculados. En los casos en que se detectan ese tipo de novedades, se avisa al jefe de la dependencia correspondiente por medio de memorando para que se tramiten los traslados y/o reintegros que permitan dejar los bienes a cargo de personal activo.”, no se recibió evidencia que diera cuenta de la aplicación de este control. Adicionalmente, la SSA indica: “Es preciso señalar que, a diferencia de los contratistas, la paz y salvos que se generan para los funcionarios no se encuentra condicionado al pago de su liquidación, como medida preventiva para la devolución de los bienes a cargo”.

En tal sentido, se recomienda a la SSA, evaluar la periodicidad cuatrimestral definida para el control de revisión del inventario vs las novedades de desvinculación de nómina; con el fin de tener mayor oportunidad en la actualización del inventario de equipos acorde con las novedades de retiro de los funcionarios y reasignación de los equipos de cómputo a cargo de dichos funcionarios y dar cumplimiento a las políticas en materia de Seguridad de la Información.

Dado lo anterior, y de acuerdo con la reunión realizada el 4/06/2024 entre la SSA y la OCI, se recomienda solicitar a las dependencias la acción correctiva para que los equipos que aún se encuentran a cargo de funcionarios retirados de la entidad, sean debidamente reasignados.

5. Mantenimiento UPS

Revisado el inventario de las UPS que actualmente se encuentran registradas en el inventario de la entidad (sistema de información SAI/SAE) 12 elementos con descripción “UPS”, y una vez verificada la documentación asociada a los mantenimientos respectivos, se evidenció que el 100%, cuenta con el soporte de mantenimientos preventivos realizados y se realizaron 36 visitas técnicas durante el año 2023.

Se concluye que a las UPS se les ha realizado mantenimiento preventivo de acuerdo con las necesidades y requerimientos de cada elemento, control que se lleva a cabo tres veces al año y, para el año 2024 se inicia el proceso en julio 2024.

6. Seguimiento en la adopción de medidas de control sobre situaciones observadas auditoría vigencia 2021

Se observó que todas las situaciones reportadas como resultado de la auditoría practicada en la vigencia 2021, la mayoría fueron implementadas, por ende, subsanadas, evidenciando lo siguiente:

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	14 de 15

- Los pisos y las paredes del Data Center, se encontraron en buenas condiciones.
- Los equipos al interior del Data Center, se encontraron en uso y en orden.
- No se observaron equipos a la entrada del Data Center, excepto algunos bien dispuestos en estantería que, de acuerdo con lo informado por la OTIC, son equipos para ser utilizados como repuestos o para reponer alguno que se dañe.
- El cuarto de medios que se encontraba en la sede del Archivo de Bogotá, se reubicó en la misma sede en un sitio diferente. En visita realizada el 26 de abril 2024, se observó organización del espacio y de los medios debidamente ubicados en estantería, se cuenta con acceso controlado con puerta con llave que se encuentra a cargo del responsable de la OTIC y se diligenció registro de acceso en formato dispuesto para tal fin (FT-267 Bitácora de acceso a centros de cómputo y cuartos de comunicaciones).

Recomendación No. 3

Con relación a la recomendación dada en la auditoría vigencia 2021 referente a contar con un Plan de Contingencia relacionado con poner en marcha o continuidad del funcionamiento de la entidad frente a cualquier evento de siniestro, se encontró que aún no se cuenta con este plan generando debilidad de control para la entidad, en el sentido que permita dar continuidad a la operación en caso de materialización riesgos geográficos por ubicación cercana de ambos Data Center como ejemplo en los casos de terremoto, amotinamientos, actos terroristas, entre otros.

Se observó la publicación en Daruma del documento denominado “Plan de Contingencia TI – DRP V7 (PL-020)” con fecha de publicación 19/01/2023, el cual contiene: roles y responsabilidades, estado actual de la infraestructura de la SGAMB, Sistemas de Información Críticos que soportan la operación de la Entidad, Fase reducción de riesgos, Monitoreo, estrategia plan de contingencia, plan de continuidad de operaciones, entre otros.

En este documento, se menciona en la página 35 la situación deseada relacionada al plan de continuidad Centro Alterno (Archivo de Bogotá), donde se indica que: *“En un evento donde se requiera activar el centro de cómputo alternativo de la SG, es necesario contar con la infraestructura técnica mínima requerida, para ello es importante disponer de un sistema similar o de características compatibles con la infraestructura actual en el centro de cómputo principal en la manzana Liévano. Por lo tanto, debemos disponer de la **siguiente infraestructura que actualmente no dispone la SG** y cuyo valor promedio de adquisición también lo mencionamos, de acuerdo con el promedio de los estudios de mercado realizados en el año 2022.”* *Negrilla y subrayado por fuera de texto.*

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	15 de 15

De igual forma es conocido, que la entidad no cuenta con un plan de contingencia que permita dar continuidad al negocio en caso de falla total o daño del centro de Cómputo principal, en consecuencia, se reitera nuestra recomendación emitida hace dos años atrás en la vigencia 2021, respecto de la necesidad a evaluar la infraestructura de contingencia con que cuenta actualmente en la entidad, de llevar a cabo un estudio juicioso de costo/beneficio, evaluar las diferentes opciones para la implementación y/o actualización de un Data Center Alterno y puesta en marcha el funcionamiento de un plan de contingencia.

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