FECHA DE EMISIÓN DEL INFORME	**Día:**	30	**Mes:**	09	**Año:**	2021

Unidad Auditada:	AUDITORIA DATA CENTER (CENTRO DE COMPUTO), CUARTOS DE COMUNICACIÓN Y BACKUPS
Dependencia(s):	OFICINA ASESORA DE PLANEACIÓN Y SISTEMAS
Líder de la Unidad Auditada (Nombre y Cargo)	JAVIER ENRIQUE ARIZA RODRIGUEZ – JEFE OFICINA ASESORA DE PLANEACIÓN Y SISTEMAS (E)
Objetivo de la Auditoría:	Evaluar el diseño del Data Center, controles, sistemas, procedimientos, equipos tecnológicos empleados, recurso humano encargado de la gestión, su eficiencia, redundancia y seguridad.
Alcance de la Auditoría:	Evaluar el diseño del Data Center, su administración, nivel de seguridad, mantenimiento, planes de contingencia, gestión sobre los Backups de Información y otros aspectos que surjan durante el curso de la actividad, para lo corrido de la actual vigencia.
Criterios de la Auditoría:	ANSI/TIA-942: estándar para un Data Center. UPTIME INSTITUTE: Clasificaciones en niveles (TIER). ISO/IEC 27001, COBIT V. 5. Matriz de Evaluación de Riesgos Institucionales Supersolidaria. Políticas, procedimientos y riesgos que se hayan definido en la entidad relacionados con la gestión del aplicativo.

Reunión de Apertura			**Ejecución de la Auditoría**							**Reunión de Cierre**		
Día	**Mes**	**Año**	**Desde**	**Día**	**Mes**	**Año**	**Hasta**	**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
06	08	2021		13	09	2021		23	09	2021	30	09	2021

Jefe oficina de Control Interno	**Auditor**
Mabel Astrid Neira Yepes	Jorge Armando Marimón Acosta Contratista

I. DECLARACION

La auditoría se realiza con base en el análisis de diferentes muestras aleatorias seleccionadas por el auditor y se fundamenta en el siguiente soporte documental: expedientes fuente, procesos y procedimientos del sistema de gestión, reportes de los sistemas de información, cruces y validaciones, página web y normas internas y externas.

En aplicación al Decreto 648 de 2017 Artículo 2.2.21.4.8, la Oficina de Control Interno incorpora los siguientes instrumentos para la Actividad de la Auditoría Interna:

i. Código de Ética del Auditor Interno que tiene como bases fundamentales, la integridad, objetividad, confidencialidad, conflictos de interés y competencia de este.

ii. Estatuto de auditoría, en el cual se establecen y comunican las directrices fundamentales que definen el marco dentro del cual se desarrollan las actividades de la Oficina de Control Interno, según los lineamientos de las normas internacionales de auditoría.

II. COMPROMISO DEL AUDITADO

Carta de representación en la que se establezca la veracidad, calidad y oportunidad de la entrega de la información presentada a las Oficinas de Control Interno.

III. NOTA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

Este documento contiene información de interés exclusivo del auditor y el auditado para surtir los trámites establecidos en la Guía de Auditoria. En ese sentido, hasta tanto no se constituya como informe final y sea publicado en la página Web de la Superintendencia de la Economía Solidaria, no podrá ser distribuido ni utilizado por terceros, ni se podrá hacer referencia a él en ningún otro asunto, sin el consentimiento previo y por escrito del Jefe de Control Interno.

IV. METODOLOGÍA

Para el desarrollo de la auditoría efectuada al Data center (centro de cómputo), cuartos de comunicación y Backups, y teniendo en cuenta el objetivo y alcance mencionados anteriormente, los cuales fueron presentados a la Oficina Asesora de Planeación y Sistemas a través del memorando 20211300016703 del 6 de agosto de 2021, se desarrollaron las siguientes actividades:

a) Entendimiento del proceso: Se revisó el mapa de procesos de la entidad para identificar los procesos y los riesgos que están relacionados con la gestión del Data center (centro de cómputo), cuartos de comunicación y Backups, así como también se verificó la documentación asociada a su gestión en el Sistema de Gestión de Calidad “Isolución”; de igual manera, se solicitó a la Oficina Asesora de Planeación y Sistemas coordinar una visita presencial a las instalaciones de la entidad, para conocer el Data Center, su diseño, controles y demás aspectos relacionados a su gestión, actividad que fue realizada el día lunes 13 de septiembre de 2021.

b) Diseño del plan de auditoría: Se estableció la programación del plan de trabajo para el desarrollo de la auditoría, de modo que permitiera lograr el objetivo propuesto.

c) Reunión de apertura: la apertura de la auditoría se realizó a través del memorando 20211300016703 del 6 de agosto de 2021, donde se describió la metodología a utilizar para esta actividad.

d) Obtención y análisis de la información: Fue solicitada la información suficiente, relacionada con el universo de la unidad auditada para efectos de seleccionar una muestra.

e) Ejecución de pruebas: Se realizó la verificación sobre el cumplimiento de los requisitos normativos internos y externos, en relación al diseño y gestión del Data Center y Backups, controles, sistemas, procedimientos, equipos tecnológicos empleados, recurso humano encargado de la gestión, su eficiencia, redundancia y seguridad.

f) Definición de observaciones y recomendaciones: Surgieron producto de la comparación entre el estado correcto del requisito (criterio) y el estado actual, socializando cada uno de ellos con el líder del proceso y personal a cargo de la gestión.

RIESGOS EVALUADOS (Riesgos evaluados en el proceso de auditoría)

El proceso GSTI - Gestión de Servicios de Tecnologías de Información, incluido en el mapa de procesos de la entidad, y oficializado en el sistema de gestión de calidad (Isolución), cuenta con los siguientes riesgos de gestión identificados en el Mapa de Riesgos Institucional, los cuales están directamente relacionados con la unidad auditada:

1. GSTI-1 Interrupción en la operación de la plataforma tecnológica.
2. GSTI-2 Inaccesibilidad a los servicios de TI.
3. GSTI-3 Pérdida de información de la entidad.

La identificación de los riesgos trae consigo sus respectivas actividades de control ejecutadas por los líderes del proceso, las cuales van desde seguimientos y monitoreos trimestrales realizados por la Oficina Asesora de Planeación y Sistemas, de acuerdo a la metodología definida por la entidad, hasta las posteriores verificaciones efectuadas durante las auditorías y seguimientos que realiza la Oficina de Control Interno.

DESARROLLO DEL EJERCICIO DE AUDITORÍA (Resultados de los Aspectos Evaluados)

1. Descripción del proceso

Un Data Center, Cuarto de Comunicaciones o Centro de Procesamiento de Datos, corresponde a una infraestructura física o virtual utilizada para alojar sistemas informáticos, que puedan procesar, servir o almacenar datos. Los Data Center proporcionan servicios de almacenamiento de datos, respaldo o Backup, recuperación de datos y gestión de la información.

El propósito principal de un Data Center es alojar los servidores necesarios para soportar los servicios ofrecidos a los clientes. El personal capacitado para gestionar su administración se encarga de que todos los servidores estén actualizados y de asegurar que tengan un perfecto funcionamiento, tanto software (Sistemas operativos, actualizaciones críticas, aplicaciones, copias de seguridad, parches), como hardware (memorias, discos duros, CPU´s, etc.).

Estos servidores se colocan en grandes armarios denominados Racks. Normalmente el proveedor del alojamiento proporciona el ancho de banda, la seguridad, refrigeración e instalaciones, para mantener los servidores en perfectas condiciones de uso y que puedan brindar un rendimiento óptimo.

Clasificación de un Data Center

De acuerdo con la American National Standars Institute (ANSI), los Data Center poseen una norma de mejores prácticas llamada ANSI/TIA 942, la cual tiene como objetivo el certificar la disponibilidad de los componentes que tienen estos inmuebles. El tamaño, el tiempo de respuesta y los niveles de redundancia, son algunos ejemplos de los aspectos que se consideran en dicha certificación.

Todas las partes expuestas deben desarrollarse paralelamente para obtener los resultados óptimos que se esperan de un Data Center profesional, cuya calidad se mide por la disponibilidad efectiva de todos los sistemas a lo largo del año, mediante los certificados que otorga el Uptime Institute y que se clasifican en 4 niveles llamados Tier que van desde el 99,741% al 99,995% de disponibilidad.

En la actualidad se han definido cuatro tipos de Tier, que son:

Tier 1 = Componentes sin capacidad redundante (ejemplo 1 sola UPS o 1 solo proveedor de datos). La tasa de disponibilidad máxima del Data center es 99.671% del tiempo.

Tier 2 = Tier 1 + Dispositivos con componentes redundantes. La tasa de disponibilidad máxima del Data center es 99.749% del tiempo.

Tier 3 = Tier 1 + Tier 2 + Equipos de alimentación eléctrica dual y varios enlaces de salida. La tasa de disponibilidad máxima del Data center es 99.982% del tiempo.

Tier 4 = Tier 1 + Tier 2 + Tier 3 + todos los componentes son completamente tolerante a fallos incluyendo enlaces de datos, almacenamiento, aire acondicionado, energía eléctrica, etc. La tasa de disponibilidad máxima del Data center es 99.995% del tiempo.

2. Detalle de las validaciones realizadas

De acuerdo a la Norma EIA / TIA 942, establecida para la gestión de un Data Center, se deben tener en cuenta cuatro subsistemas, que son:

- Telecomunicaciones
- Arquitectura
- Sistema eléctrico
- Sistema mecánico

Teniendo en cuenta estos aspectos a verificar, se desarrolló un cuestionario para el diligenciamiento por parte de los encargados de la gestión del Data Center y de los Backup de

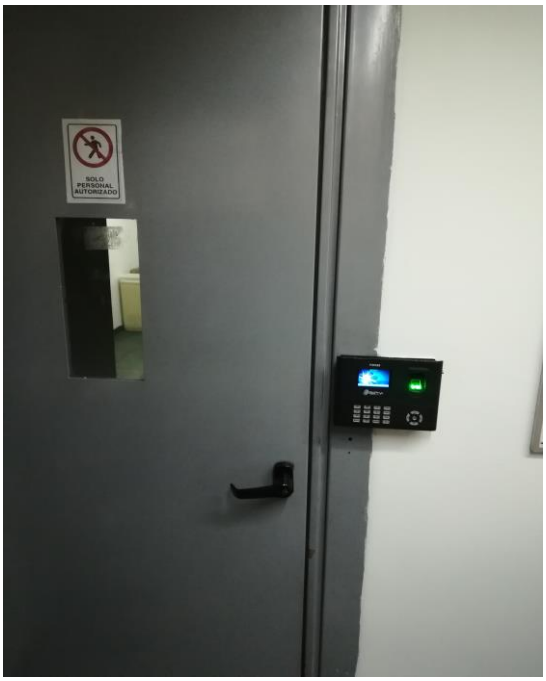
información, al cual se le realizó comprobación, de acuerdo a las respuestas indicadas, en la visita en sitio al centro de datos, llevada a cabo el día lunes 13 de septiembre de 2021 en compañía de un funcionario de la Oficina Asesora de Planeación y Sistemas, encargado de la administración del lugar, encontrándose situaciones como las descritas a continuación:

- Fue posible determinar que el centro de cómputo de la entidad se encuentra ubicado en la clasificación TIER 2 – Componentes Redundantes, teniendo en cuenta que cuenta con aspectos como los señalados a continuación:

- ✓ Redundancia en la parte eléctrica (2 circuitos)
- ✓ Routers & switches tienen fuentes de alimentación redundantes.
- ✓ Hiperconvergencia en los servidores.
- ✓ Cableado, Racks y Gabinetes conforme a la norma TIA 942.
- ✓ Piso Falso.
- ✓ Polo a tierra.
- ✓ Unidades de enfriamiento
- ✓ El mantenimiento en la línea de distribución eléctrica o en otros componentes de la infraestructura pueden causar una interrupción del procesamiento.
- ✓ Módulos UPS
- ✓ El mantenimiento de la alimentación y otras partes de la infraestructura requieren de una interrupción del procesamiento.

Se adjuntan algunas evidencias de los aspectos evaluados en la inspección física:

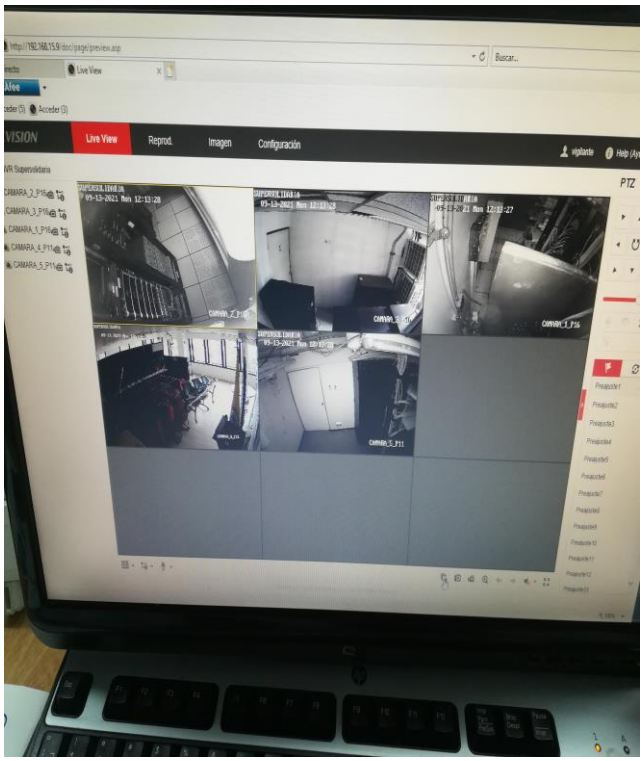
Seguridad del Data Center

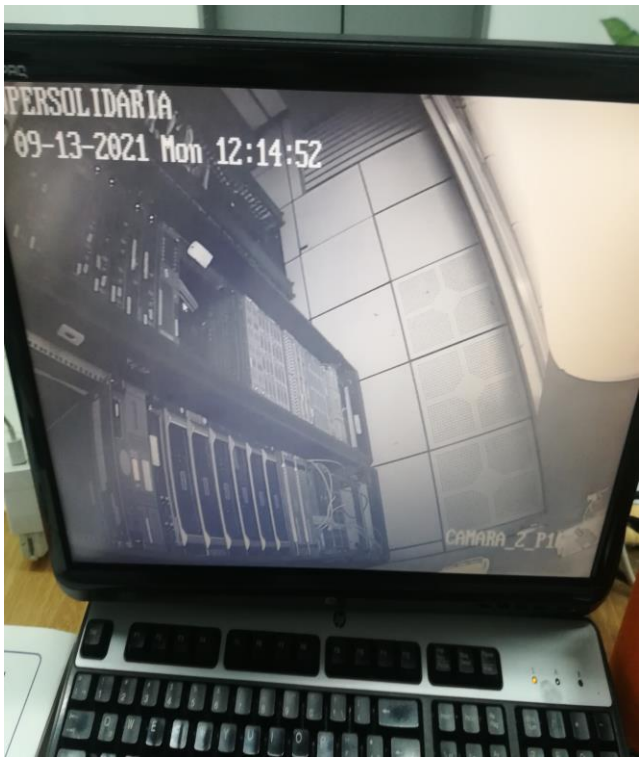


- Como se alcanza a apreciar en las imágenes, se tienen implementados controles para el acceso de la oficina que antecede al centro de cómputo, a través de una cerradura de seguridad en la puerta principal del sitio. Posteriormente, se dispone de una puerta de seguridad con un sistema de control biométrico. Tanto las llaves para el acceso a la oficina como las credenciales del sistema biométrico para acceder al Data Center, son administradas únicamente por tres (3) profesionales de la Oficina Asesora de Planeación y Sistemas, responsables de la gestión del lugar.

- Como debilidad se alcanzó a observar que el Data Center no dispone de una salida de emergencia, es decir, la misma puerta de entrada al sitio es la misma puerta para salir, lo cual genera un riesgo de seguridad y no es acorde a la normativa para la gestión de un centro de cómputo, razón por la cual se registra esta situación dentro de la sección de observaciones del presente informe, con el fin que se implementen acciones para subsanarla.

Vigilancia del Data Center





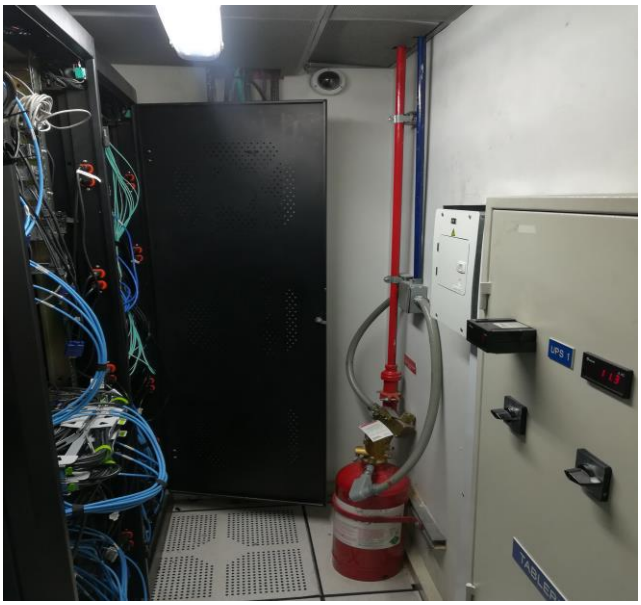
- Se evidenció que existe vigilancia para el Data Center las 24 horas, lo cual se encuentra controlado y supervisado a través del personal de vigilancia, encargado del monitoreo de las cámaras de seguridad del Data Center y del cuarto de comunicaciones, ubicados en el piso 16 y 11, respectivamente.

Refrigeración del Data Center

- Se evidenció que el Data Center cuenta con un sistema de refrigeración central, adicionalmente se dispone de dos mini Split, como medio de ventilación alterno para el sitio, a los cuales se les hace mantenimiento cada seis meses.
Así mismo, el lugar cuenta con controles digitales de temperatura, con el fin de monitorear el cumplimiento de la normatividad, que indica que el rango ideal de temperatura para los servidores debe fluctuar entre los 18 y los 23 grados, lo cual se puede evidenciar a partir de las imágenes relacionadas a continuación:

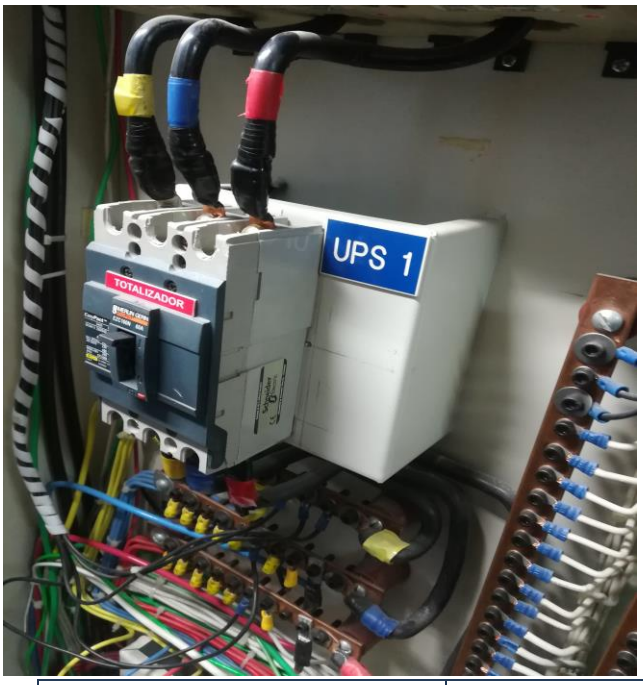
- Se evidenció durante la visita al centro de cómputo que es un lugar que está seguro de inundaciones, sabotaje, que no da hacia el exterior y que cuenta con controles para evitar el robo u otra situación que ponga en peligro los equipos presentes y la información. No se observó la presencia de materiales que puedan ser inflamables.

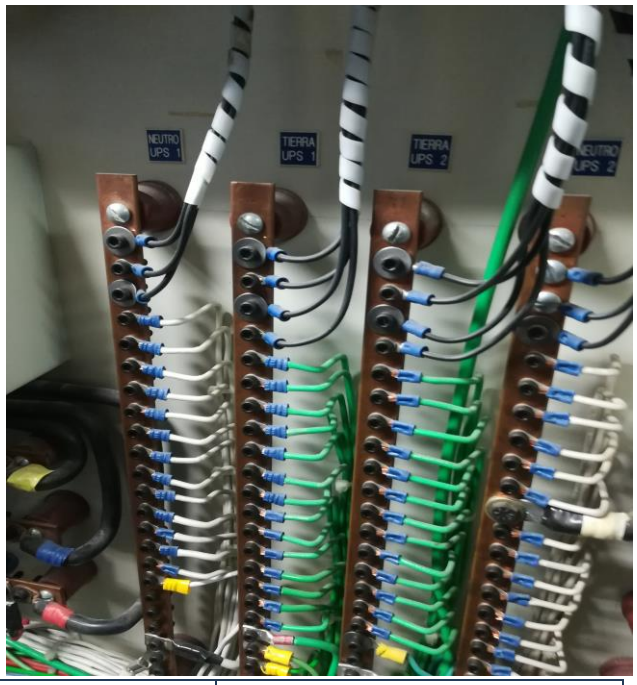
El lugar cuenta con alarma y sistema automático contra incendios a base de gas, extintores manuales contra fuego y sistema de iluminación de emergencia, como se puede apreciar:



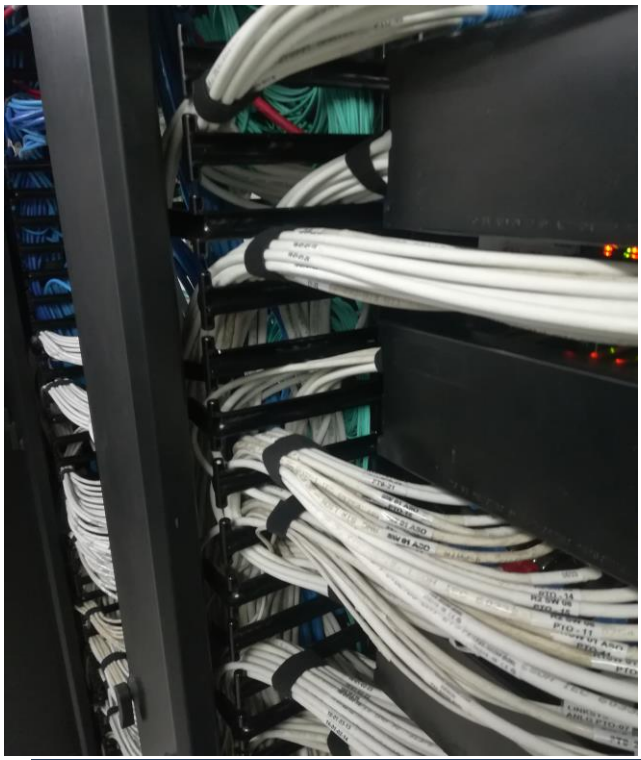
Instalación Eléctrica en el Data Center

Se observo que el cableado eléctrico se encuentra instalado de una manera adecuada, a través de tableros de control con puesta a tierra para protección de los equipos de cualquier descarga eléctrica, y con conexión al sistema de UPS para proveer de energía auxiliar en caso de un apagón, lo cual se puede ver a continuación:





El cableado estructurado se encuentra correctamente dispuesto dentro de paneles y canales eléctricos, como se alcanza a evidenciar a continuación:



Señalización en el Data Center

Se evidenció la ubicación de señalización relacionada con la prohibición de consumir alimentos y bebidas al interior del Data Center, con el fin de evitar cualquier daño sobre los dispositivos presentes. Así mismo, señales relacionadas con el ingreso al lugar, con la forma de accionar el sistema contra incendios y con la monitorización por cámaras que se lleva a cabo sobre la actividad del centro de cómputo.

Política y Procedimientos para la Gestión de Backup

- No existe oficializada una Política de Seguridad de la Información, lo cual fue advertido por esta Oficina en un informe anterior de auditoría, para lo cual la Oficina Asesora de Planeación y Sistemas suscribió una acción de mejora, relacionada con presentar para su aprobación ante el Comité Institucional de Gestión y Desempeño, las Políticas de Seguridad de la Información y demás políticas y procedimientos contemplados en el Sistema de Gestión de Seguridad de la Información (SGSI) y en el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, lo cual será objeto de seguimiento por parte de la Oficina de Control Interno.

- La entidad cuenta con el procedimiento PR-GSTI-001 GESTIONAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS SERVICIOS TI, a través del cual se definen los lineamientos para la realización de copias de seguridad, su restauración y la disposición final de las mismas. Sin embargo, no se dispone de una política de Backup de la información, lo cual fue advertido por esta Oficina en un informe anterior de auditoría, para lo cual la Oficina Asesora de Planeación y Sistemas suscribió una acción de mejora, relacionada con la aprobación de la Política de Backup de la Superintendencia de la Economía Solidaria por medio del Comité de Gestión y Desempeño, a lo cual se le realizará seguimiento por parte de la Oficina de Control Interno.

Características de la herramienta de Gestión de Backup

Para la gestión de Backup se cuenta con la solución Availability Suite Ent. Plus, la cual ofrece disponibilidad para todas las cargas de trabajo (virtuales, físicas y cloud) desde una única consola de administración. Se trata de un paquete de valor agregado que incluye Veeam Backup & Replication, además de las características de monitorización, análisis y generación de informes de Veeam ONE. Ayuda a cumplir con los objetivos de nivel de servicio y disponibilidad del centro de datos.

Veeam Availability Suite es una solución de primera línea que ofrece funcionalidades de protección de datos, permitiendo realizar copias de seguridad y restauración de las mismas.

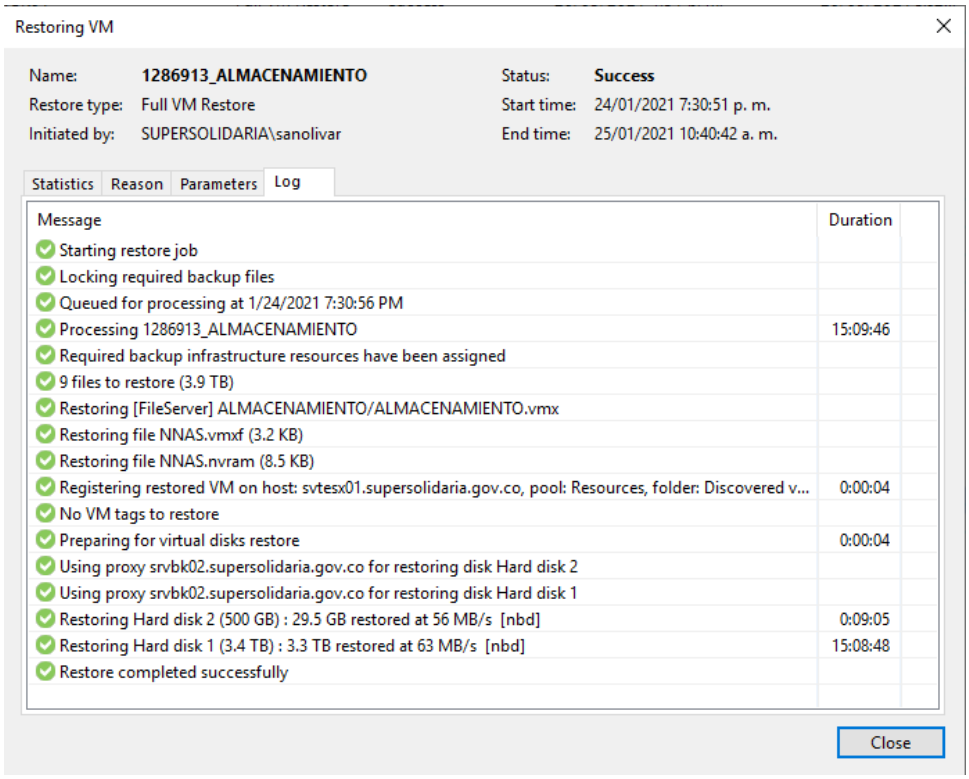
Licenciamiento del software para la Gestión del Data Center

Respecto al licenciamiento de Veeam Availability Suite Enterprise Plus, se evidenció documento donde se soporta que se cuenta con una licencia a perpetuidad para 8 usuarios, la cual fue adquirida con la empresa Veeam Software Corporation durante la vigencia 2018, la cual ha venido siendo renovada y se encuentra vigente hasta el 25 de diciembre del año 2022. Igualmente se comprobó el licenciamiento del software para la administración de la virtualización VMWARE, adquirido con la empresa NEXSYS DE COLOMBIA SA.

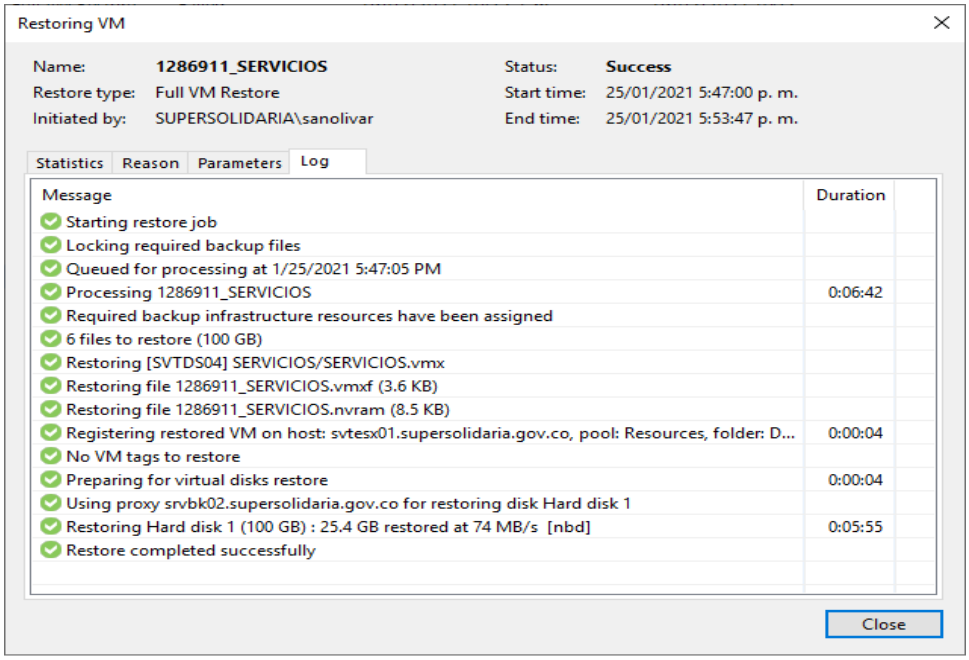
Restauración de Backup

Se requirió a la Oficina Asesora de Planeación y Sistemas, remitir evidencias de restauración de Backups efectuados durante la vigencia en curso, donde se pudo apreciar la realización exitosa de la actividad sobre algunos de los servidores de la entidad, como se puede ver a continuación:

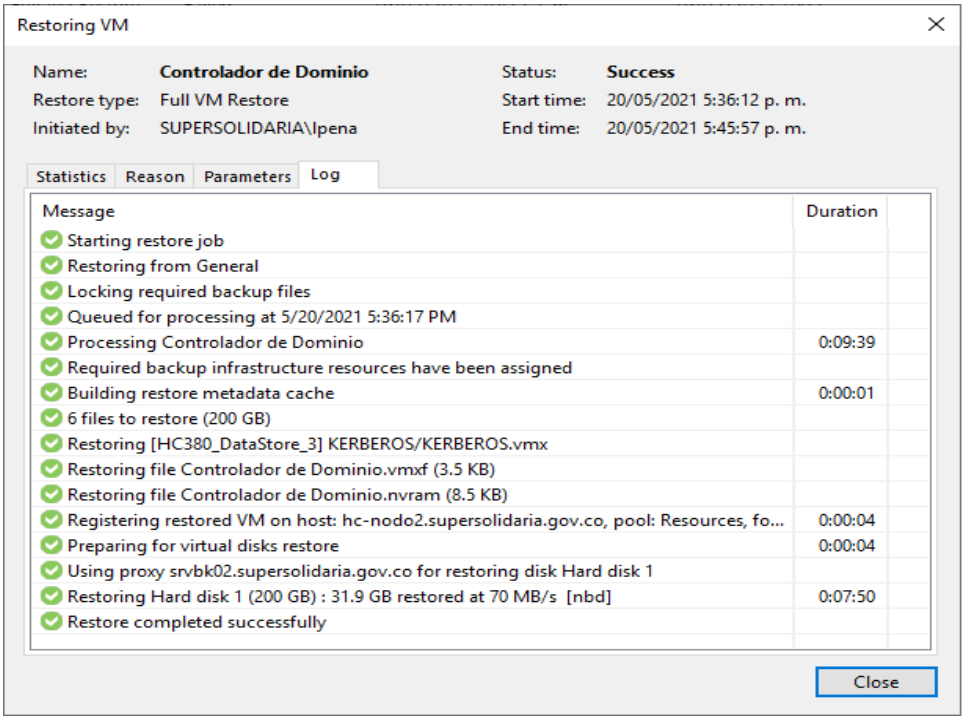
1. 1286913_ALMACENAMIENTO



2. 1286911_SERVICIOS



3. CONTROLADOR DE DOMINIO



Procedimientos y formatos establecidos para la realización y restauración de Backup y para la Gestión del Data Center

- FT-GSTI-001 Entrega de cintas de Backup.
- FT-GSTI-002 Restauración de información.
- FT-GSTI-003 Ingreso al centro de cómputo.
- PR-GSTI-001 Gestionar la confidencialidad, integridad y disponibilidad de los servicios TI (en proceso de actualización).
- IN-GSTI-002 Mantenimiento a la Infraestructura Tecnológica.

Controles establecidos para las copias de seguridad

Para poder ingresar al servidor de los Backups y gestionar la herramienta Veeam Backup, son necesarias las credenciales de acceso, las cuales son administradas únicamente por los tres profesionales de la Oficina Asesora de Planeación y Sistemas, encargados de la gestión del centro de cómputo.

Trimestralmente se realiza una prueba de restauración de Backups, con el fin de comprobar la validez y la integridad de la información que ha sido respaldada a través de los medios dispuestos, como son las cintas magnéticas, dispositivos de Hardware como Store Once (dispositivos de Backup con protección de datos) y Store Easy (almacenamiento simplificado de archivos y

aplicaciones). Esta tarea se encuentra registrada dentro del procedimiento PR-GSTI-001 Gestionar la confidencialidad, integridad y disponibilidad de los servicios TI.

Para la custodia de las copias de seguridad, se guardan las mismas en un lugar distinto al mismo edificio de la entidad, correspondiente a la sede alterna, ubicada en el Edificio Patria, localizado en la Carrera 10 N° 15 - 20 de la ciudad de Bogotá.

Para el efectuar el traslado a la sede alterna de la entidad se debe diligenciar el formato FT-GSTI-001 Entrega de cintas de Backup, formalizado a través del Sistema de Gestión de Calidad de la entidad (Isolución), el cual debe contener información relevante para la trazabilidad del proceso, como es la Fecha de la entrega de la cinta, el nombre de la cinta de Backup, la información que está contenida en esta, quien recibe la cinta, la ubicación final de la misma y un espacio para registrar cualquier observación adicional.

Rotulación y conservación física de las copias de seguridad

La imagen evidencia las cintas magnéticas donde se realizan las copias de seguridad por medio de la Herramienta de Backup y su correspondiente rotulación, sin embargo, no se encuentra documentado en ninguna parte la forma de rotularlas y su significado, por lo cual se va a resaltar esta situación como una oportunidad de mejora, para que sea incluida dentro del procedimiento de PRGSTI001 Gestionar la confidencialidad, integridad y disponibilidad de los servicios TI, o en el que la Oficina Asesora de Planeación y Sistemas considere más conveniente.

La disposición final para la conservación física de las copias de seguridad, está enmarcada dentro del procedimiento PRGSTI001 Gestionar la confidencialidad, integridad y disponibilidad de los servicios TI, para lo cual las cintas son trasladadas al final de la realización de la copia de seguridad, a un sitio externo (correspondiente al edificio Patria de la entidad), para lo cual se deja registro en el formato FT-GSTI-001 ENTREGA DE CINTAS DE BACKUP.

Normatividad bajo la cual se encuentra diseñado e implementado el Data Center

De acuerdo a lo remitido por la Oficina Asesora de Planeación y Sistemas, se obtuvo la siguiente información:

"La normatividad que se debe cumplir para el diseño e implantación de un Data Center es la ANSI / TIA-942 es un estándar de calidad que especifica los requisitos para centros de datos. La topología presentada en la norma es aplicable a cualquier centro de datos de cualquier tamaño y cubre toda la infraestructura física, incluidos, entre otros requisitos: ubicación del sitio, sistema eléctrico, mecánico, seguridad contra incendios, telecomunicaciones, seguridad y entre otros, y las normas TIA-606 y 607 respectivamente, cuando se construyó el Data Center cumplía con la norma, pero que la norma ANSI / TIA-942 se actualizó cambiando a 942 revisión B (12 julio de 2017), por lo que actualmente se encuentra en proceso de mejora para cumplir en su totalidad con la norma anteriormente mencionada".

Por parte de la Oficina de Control Interno, teniendo en cuenta lo evidenciado en la visita efectuada al Data Center y tal cual como fue registrado anteriormente, se considera que el lugar alcanza el nivel II Componentes Redundantes, de acuerdo al estándar TIA 942 y sus requisitos, sin embargo, se deja registrado dentro de las oportunidades de mejora del presente informe, la recomendación para que la Oficina Asesora de Planeación y Sistemas solicite la certificación del centro de cómputo, a través de las entidades especializadas que se encargan de verificar los centros de datos y entregar las correspondientes certificaciones que confirman el diseño, la construcción y la sostenibilidad del lugar.

Mantenimiento a Switch, servidores, unidades de almacenamiento, unidades de cinta o Backup, UPS, aire acondicionado y planta eléctrica

El mantenimiento preventivo de estos equipos tecnológicos se encuentra definido dentro del procedimiento PRGSTI001 Gestionar la confidencialidad, integridad y disponibilidad de los servicios TI, así mismo en el Instructivo IN-GSTI-002 Mantenimiento a la infraestructura tecnológica, lo cual es realizado por medio de personal especializado, de acuerdo a las obligaciones establecidas en los contratos, adicionalmente el proveedor del servicio debe realizar la disposición final de los residuos que se generen en dicho mantenimiento.

En los contratos que se suscriben y de acuerdo al tipo de equipo, se define la periodicidad de los mantenimientos que se deben realizar, bajo la supervisión de la Oficina Asesora de Planeación y Sistemas.

Protección de la información del Data Center

A través del directorio activo de la entidad se controlan los permisos para que los usuarios ejecuten acciones como la instalación de software no autorizado, así como también a través del aplicativo PC SECURE, el cual se encuentra debidamente licenciado. De igual manera, por medio del antivirus que se tiene licenciado y de la plataforma de seguridad del Firewall, se protege la información contra virus, spyware y demás ataques cibernéticos.

Las contraseñas de acceso a las bases de datos son gestionadas por los administradores de las bases de datos, para lo cual se lleva un control de claves con el apoyo del software free o de libre adquisición denominado TeamPass, que básicamente es una herramienta que facilita la administración de contraseñas.

A través del control de activos de la entidad, se lleva una clasificación de la información relevante que es procesada en el centro de cómputo.

Se pudo identificar que no se cuenta con un soporte de los planos del Data Center y de un inventario de los materiales utilizados para su construcción, por lo cual se registra esta situación como una debilidad dentro de la sección de observaciones del presente informe, teniendo en cuenta el riesgo que en algún momento puede llegar a ocasionar afectaciones sobre la planificación e implementación de mejoras a la infraestructura del lugar y con ello afectar su desempeño y operación.

De la misma manera fue posible conocer que no se han realizado simulacros para verificar la efectividad de los controles que se tienen implementados en el Data Center para la protección de los equipos y la información, por lo cual se registra esta situación dentro de la sección Oportunidades de Mejora del presente informe, con el fin que a través de pruebas se pueda asegurar el correcto funcionamiento y la efectividad de los controles.

Se pudo establecer que la entidad, adicional a los controles físicos y lógicos que tiene para el ingreso al Data Center y para la salvaguarda de la información, cuenta además con pólizas adquiridas con la compañía de seguros La Previsora S.A., las cuales tienen como finalidad la protección de la información procesada en el centro de cómputo, lo cual se presenta de manera resumida a continuación:

- ✓ **Póliza Todo Riesgo Daños Materiales No. 1003587:** En esta póliza se amparan daños provenientes de corriente débil, pérdida de datos o portadores externos de datos incluyendo software, terrorismo, explosión por cualquier causa, daños por agua, incendio inherente, hundimiento, asentamiento, deslizamiento y desplazamiento de terrenos, muros, pisos y techos; caída de rocas, árboles y aludes, de eventos tales como hurto y hurto calificado, huelga, motín, asonada, conmoción civil o popular, actos mal intencionados de terceros, terremoto, temblor, eventos de la naturaleza, y se encuentra contratada actualmente las siguientes clausulas:

  - Gastos adicionales para reproducción o reemplazo de información contenida en documentos, archivos de cualquier tipo, bases de datos, planos, etc.: No obstante, lo que se diga en contrario en las condiciones generales y particulares de la póliza, la Compañía se obliga a indemnizar los gastos y costos en que necesaria y razonablemente incurra el asegurado para reproducir o reponer la información contenida en documentos, bases de datos, archivos de cualquier tipo, planos etc., perdidos o dañados a consecuencia de cualquiera de los eventos amparados por la póliza, hasta el 100% de los gastos demostrados. La cobertura se otorga de acuerdo con el sublímite único combinado.

  - Gastos adicionales por reconstrucción de archivos: No obstante, lo que se diga en contrario en las condiciones generales y particulares de la póliza, la Compañía se obliga a indemnizar los gastos y costos en que necesaria y razonablemente incurra el asegurado para obtener, reemplazar o restaurar la información de archivos, documentos y grabaciones perdidas o dañadas a consecuencia de cualquiera de los eventos amparados por la póliza, hasta el 100% de los gastos demostrados. La cobertura se otorga de acuerdo con el sublímite único combinado.

El sublimite único combinado es $1.000.000.000 evento / $2.000.000.000 vigencia, al que hacen referencia en el texto de las cláusulas.

- ✓ **Póliza Manejo Global Para Entidades Estatales No. 1006181 y Póliza No. de Infidelidad y Riesgos Financieros: No. 1001536:** En esta póliza se amparan daños riesgos por apropiación, infidelidad, abusos de confianza, apropiaciones indebidas, cometidas por empleados, contratistas por mencionar entre otros, se encuentra contratada actualmente las siguientes clausulas:

  - Costos de reconstrucción de archivos: Hasta por un 20% del valor total asegurado y sin aplicación de deducibles. El sublimite de esta cláusula sería $40.000.000 dado que el valor asegurado de esta póliza $200.000.000.
  - Perdidas a través de Sistemas computarizados - Sistemas de Computación / Informática, según cláusula 1 del texto LSW983: La Compañía de Seguros se compromete a indemnizar al asegurado la perdida resultante de que el asegurado haya transferido, pagado o entregado fondos o propiedad, o establecido algún crédito, debitado alguna cuenta, o dado cualquier valor como resultado directo de:
    a) el ingreso fraudulento de datos electrónicos directamente a: (i) el sistema de computadoras del asegurado, o (ii) un sistema de computadoras de oficina de servicios, o (iii) cualquier sistema de transferencia electrónica de fondos, o (iv) un sistema de comunicaciones del cliente;
    o b) la modificación fraudulenta o la destrucción fraudulenta de datos electrónicos almacenados en, o que están siendo procesados dentro de cualquiera de los sistemas indicados en el literal a) anterior o durante una transmisión electrónica al sistema de computadoras del asegurado o a un sistema de computadoras de oficina de servicios;
    o c) el ingreso fraudulento de datos electrónicos a través de un sistema de banca telefónica, directamente al sistema de computadoras del asegurado y que tales actos fraudulentos hayan sido ordenados o cometidos por una persona que intentaba causar que el asegurado sufriera una pérdida, o que tratara de obtener una ganancia financiera para sí misma o para cualquier otra persona.

Por parte de la Oficina de Control Interno, se considera que la adquisición de la anterior póliza es un control oportuno y adicional para la salvaguarda de la información y asegurar su disponibilidad, integridad y confidencialidad, por lo cual se recomienda dar continuidad a la misma.

Plan de Continuidad de Negocio – Plan de Recuperación de Desastres

Se ha logrado evidenciar con anterioridad, a través de la actividad “Auditoría a la Gestión de Servicios de TI (GSTI) - Políticas de seguridad de la información, Riesgos Tecnológicos (Criterios de Evaluación COBIT, ITIL, ISO, MSPI)”, la ausencia de un Plan de Continuidad del Negocio (BCP), así mismo de un Plan de Recuperación de Desastres (DRP), que permitan a la entidad establecer acciones oportunas para actuar y restaurar las operaciones de su plataforma tecnológica, y con ello dar continuidad a sus servicios y operaciones, manteniendo la ejecución de sus funciones misionales. Sin embargo, para ello la Oficina Asesora de Planeación y Sistemas suscribió acciones de mejora para ejecutar en la actual vigencia, relacionadas con el diseño y

presentación del BCP y del DRP ante el Comité de Gestión y Desempeño de la entidad, a lo cual se le realizará seguimiento por parte de la Oficina de Control Interno.

Gestión de Incidentes de Seguridad de la Información

Se logró establecer por parte de la Oficina de Control Interno, a través de un informe de auditoría realizado con anterioridad, que la entidad no ha definido y apropiado procedimientos para la Gestión de Incidentes de Seguridad de la Información, para lo cual la Oficina Asesora de Planeación y Sistemas suscribió como acción de mejora, el presentar para aprobación ante el Comité Institucional de Gestión y Desempeño la Política de Gestión de Incidentes de Seguridad de la Información, lo cual será objeto de seguimiento por parte de esta oficina.

3. Oportunidad de Mejora (Relacionada con la evaluación realizada)

- Luego de realizar la visita in situ al Data Center, se pudo evidenciar que es un lugar un poco pequeño que dificulta el transitar dentro del mismo, evidenciando que, al encontrarse más de una persona al tiempo dentro del mismo, puede llegarse a tropezar y/o desconectar algún dispositivo de comunicación, por lo cual se recomienda revisar dicha situación y tomar las medidas que se requieran de manera oportuna.

- En atención a que no se encuentra inmerso en ningún procedimiento y/o formato dispuesto para la gestión de Backup, la forma de rotular las cintas con las copias de seguridad y su significado, se sugiere que sea incluida esta tarea dentro del procedimiento de PRGSTI001 Gestionar la confidencialidad, integridad y disponibilidad de los servicios TI, o en el documento que la Oficina Asesora de Planeación y Sistemas considere más apropiado. Así mismo, que se incluyan las medidas y acciones que se deban tomar, para el caso de extravío de algún dispositivo de almacenamiento de información.

- Teniendo en cuenta que la Oficina Asesora de Planeación y Sistemas se encuentra en proceso de elaboración y oficialización de la Política de Backup, se recomienda que paralelamente sea revisado, y en caso de ser necesario, sea actualizado el procedimiento PRGSTI001 Gestionar la confidencialidad, integridad y disponibilidad de los servicios TI, así como también los demás documentos y formatos que se requiera y que son afines al proceso, con las respectivas oficializaciones en el Sistema de Gestión de Calidad de la entidad.

- Se recomienda la elaboración de un cronograma para la supervisión del Data Center, con el fin que los responsables de dicha tarea conozcan con claridad los días del mes en que deben tener la disponibilidad para el caso en que sean requeridos por alguna emergencia relacionada a la gestión del sitio.

- Finalmente y con el fin de asegurar que todos los recursos presentes en el Data Center apoyan directamente las necesidades de la entidad, se recomienda solicitar la certificación, en relación con la clasificación Tier para el centro de cómputo, otorgada por el Uptime Institute, donde se refrende la disponibilidad y efectividad de todos sus componentes y se determine oportunamente aquellos aspectos susceptibles de mejoramiento.

4. Seguimiento al plan de mejoramiento (Verificación de la ejecución de acciones de mejora del plan de mejoramiento del proceso)

No se encontró un plan de mejoramiento abierto al cual realizarle el respectivo seguimiento durante la presente actividad auditora.

OBSERVACIONES DE LA AUDITORIA (Principales Situaciones Detectadas)

Observación 1: No se realizan simulacros para evaluar la efectividad de los controles implementados en el Data Center para la protección de los equipos y de la información.

Condición: El estándar ANSI/TIA-942 establece en uno de sus apartes: “Además de las pruebas de componentes, el sistema de generación de espera, sistemas UPS, e interruptores de transferencia automática deben ser probados juntos como un sistema. Como mínimo, los ensayos deberán simular una utilidad falla y restauración de la alimentación normal. Fallo de componentes individuales deben ser probados en sistemas redundantes diseñada para seguir funcionando durante el fallo de un componente. Los sistemas deberían ser probados bajo carga utilizando bancos de carga. Además, una vez que el centro de datos está en funcionamiento, los sistemas deben probarse periódicamente para garantizar que sigan funcionando correctamente”.

Así mismo, en la visita física realizada al Data Center fue solicitada esta información, pudiéndose identificar que no se viene realizando esta actividad de control. Es importante aclarar que un simulacro se realiza para evaluar la planeación, la pertinencia y la efectividad de los controles, por lo tanto, las fallas que se detecten llegan a ser corregidas de manera oportuna como parte del proceso de aprendizaje en el ejercicio.

Criterio: ANSI/TIA-942, ISO/IEC 27001, COBIT V. 5.

Causa: Posiblemente no se ha contado con los recursos requeridos para implementar esta recomendación de los estándares y normas para la administración y gestión de un centro de cómputo. También es posible que de desconociera este lineamiento presente en el estándar ANSI/TIA-942, con lo cual se genera riesgo sobre la seguridad de la información.

Efecto: Su afectación es transversal a los riesgos del proceso GSTI - Gestión de Servicios de Tecnologías de Información, como son: GSTI-1 Interrupción en la operación de la plataforma tecnológica, GSTI-2 Inaccesibilidad a los servicios de TI, GSTI-3 Pérdida de información de la entidad.

Recomendación: Se sugiere la realización de simulacros periódicos para verificar la efectividad de los controles que se tienen implementados en el Data Center, con el fin de comprobar el aseguramiento y protección de los equipos y de la información, permitiendo encontrar deficiencias,

fallos de diseño, problemas que no pueden preverse al hacer la planificación “en papel”, pero que aparecen en la realidad, etc.

Observación 2: No se evidenció un Plan de Continuidad para el Data Center.

Condición: No se allegó evidencia de esta documentación.

Criterio: ISO/IEC 27001, COBIT V. 5.

Causa: No se ha generado la documentación de las acciones y planes a desarrollar e implementar en el momento de interrupción o falla de los procesos críticos, con el fin de mantener o recuperar las operaciones y asegurar la disponibilidad de la información.

Efecto: Su afectación es transversal a los riesgos del proceso GSTI - Gestión de Servicios de Tecnologías de Información, como son: GSTI-1 Interrupción en la operación de la plataforma tecnológica, GSTI-2 Inaccesibilidad a los servicios de TI, GSTI-3 Pérdida de información de la entidad.

Recomendación: Documentar, y de ser necesario, oficializar en el Sistema de Gestión de Calidad (Isolución), un Plan de Continuidad para el centro de cómputo, que esté relacionado con el Plan de Continuidad de la entidad o BCP, el cual posibilite contrarrestar las interrupciones en las actividades del lugar y proteger los procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, asegurando al mismo tiempo una recuperación oportuna de los servicios y la protección de la información.

Observación 3: No existe salida de emergencia del Data Center.

Condición: En la visita in situ realizada al Data Center fue posible evidenciar esta debilidad.

Criterio: ANSI/TIA-942.

Causa: Posiblemente, al tratarse de un edificio en arriendo, se ha generado algún inconveniente para la implementación de este control de seguridad física y del entorno.

Efecto: Posible riesgo sobre la seguridad de los encargados de la gestión del Data Center.

Recomendación: Adoptar las medidas necesarias, las cuales estén enfocadas en la protección de la salud del personal administrador del centro de cómputo y de la gestión de sus componentes.

Observación 4: No se cuenta con los planos y un inventario del material con que fue diseñado el Data Center.

Condición: En la visita in situ realizada al Data Center fue posible evidenciar esta debilidad.

Criterio: ANSI/TIA-942.

Causa: De acuerdo a lo informado por el personal que atendió la visita al centro de cómputo, el lugar se encontraba diseñado desde hace tiempo y no se dispone de esta documentación.

Efecto: Su afectación es transversal a los riesgos del proceso GSTI - Gestión de Servicios de Tecnologías de Información, como son: GSTI-1 Interrupción en la operación de la plataforma tecnológica, GSTI-2 Inaccesibilidad a los servicios de TI.

Recomendación: Se sugiere que se tomen las acciones necesarias para contar con el inventario de los materiales de construcción del Data Center, y con los planos de las instalaciones del mismo, teniendo en cuenta que los proveedores de acceso a internet y demás servicios relacionados a la operación del Data Center, normalmente solicitan esta información para la planificación de cambios sobre la estructura del centro de datos, evitando con ello cualquier tipo de afectación sobre su operación.

Observación 5: No se realiza diariamente la validación al funcionamiento de las UPS del centro de cómputo, teniendo en cuenta las evidencias presentadas a través del formato FT-GSTI-003 Ingreso al centro de cómputo.

Condición: El control establecido para el riesgo GSTI-1 Interrupción en la operación de la plataforma tecnológica, señala: “El administrador de Infraestructura eléctrica revisa y valida el funcionamiento de las UPS todos los días, dejando como evidencia el formato de monitoreo, y cuando se identifique el mal funcionamiento de alguna de ellas se debe reportar al jefe de la Oficina Asesora de Planeación y Sistemas”.

Criterio: Mapa de riesgos del proceso GSTI Gestión de Servicios de Tecnologías de Información.

Causa: Posiblemente y de acuerdo a lo informado por la Oficina Asesora de Planeación y Sistemas, se viene ejecutando la actividad, pero no se viene registrando oportunamente en el formato establecido.

Efecto: GSTI-1 Interrupción en la operación de la plataforma tecnológica, GSTI-2 Inaccesibilidad a los servicios de TI.

Recomendación: Dar cumplimiento estricto a las acciones de control establecidas para el riesgo GSTI-1 Interrupción en la operación de la plataforma tecnológica; en su defecto, realizar la revisión de las acciones suscritas y de llegar a ser necesario, establecer las correcciones a que haya lugar en el mapa de riesgos del proceso, velando por su cumplimiento.

RESUMEN DE OBSERVACIONES

Producto de la evaluación realizada por parte de la Oficina de Control Interno, fueron evidenciadas las siguientes observaciones las cuales requieren de la formulación de acciones de mejora que permitan subsanar la causa que las generó:

No	OBSERVACIONES	REPETITIVO
1	No se realizan simulacros para evaluar la efectividad de los controles implementados en el Data Center para la protección de los equipos y de la información.	No
2	No se evidenció un Plan de Continuidad para el Data Center.	No
3	No existe salida de emergencia del Data Center.	No
4	No se cuenta con los planos y un inventario del material con que fue diseñado el Data Center.	No
5	No se realiza diariamente la validación al funcionamiento de las UPS del centro de cómputo, teniendo en cuenta las evidencias presentadas a través del formato FT-GSTI-003 Ingreso al centro de cómputo.	No

CONCLUSIONES DE LA AUDITORÍA (Pueden incluir, antecedentes y resúmenes)

Luego de finalizada la actividad auditora, por parte de la Oficina de Control Interno se puede concluir que en gran medida el Data Center cumple con los requerimientos de la normatividad que regula su diseño, implementación y gestión, sin embargo, se invita a tener en cuenta las recomendaciones y oportunidades de mejora señaladas en el presente informe, con la finalidad de hacer más eficiente la gestión llevada a cabo a través del mismo y de contribuir en la mejora continua del proceso de aseguramiento de la información, procurando por su disponibilidad, integridad y confidencialidad.

(Original Firmado)
MABEL ASTRID NEIRA YEPES
Jefe Oficina de Control Interno
Elaboró: Jorge Armando Marimón Acosta