INFORME DE AUDITORIA

NOMBRE DEL PROCESO, ÁREA O TEMA A AUDITAR: Auditoría Integral de Gestión al Proceso de Infraestructura Tecnológica Componente Centro de Datos y Operaciones de Red.

INFORME PRELIMINAR: (23/04/2021) **INFORME DEFINITIVO**: (19/05/2021)

1. INTRODUCCIÓN

El Centro de Datos y la gestión de Operaciones de Red, son factores fundamentales para la mitigación de riesgos tecnológicos. El centro de datos centraliza las operaciones y el equipo de TI de la Entidad, los cuales son elementos claves que deben ser gestionados con estándares internacionales y gubernamentales que permitan el control y monitoreo de todos los procesos dependientes de TI para proveer servicios escalables, flexibles y de alto desempeño que posibiliten cumplir con la estrategia y los objetivos del negocio.

La información utilizada para la auditoría fue aportada por el área de Gestión Tecnológica, así como la recolectada a través de las entrevistas y mesas de trabajo con las diferentes áreas de la Entidad, soportando los hallazgos, las observaciones y las recomendaciones generadas en el presente informe.

2. OBJETIVO DE LA AUDITORÍA

Evaluar la efectividad de los controles existentes, la gestión de riesgos, controles, la pertinencia y oportunidad de los procedimientos establecidos en los Manuales, las Circulares Normativas aplicables al componente de Centro de Datos y Operación de Red, la gestión del proceso y el diseño y operatividad de indicadores que soportan las actividades clave del proceso de operaciones tecnológicas.

Los objetivos específicos definidos para la evaluación de este componente son los siguientes:

1. Revisión de los protocolos y privilegios de control de acceso al centro de cómputo.

2. Revisión y evaluación del modelo de servicios y operación de las aplicaciones que están en producción.
3. Revisión y evaluación del cumplimiento de los ANS (Acuerdos de Niveles de Servicios).
4. Evaluación de los controles ambientales implementados en el centro de cómputo.
5. Revisión y evaluación de la administración del desempeño y capacidad de los recursos de TI.
6. Revisión de la administración de incidentes y problemas.
7. Revisión de los planes de mantenimiento al sistema de extinción automático de incendios, aire acondicionado, techo, piso falso y detección de humedad.
8. Revisión y evaluación de la administración de las operaciones del centro de cómputo: ejecución de procesos automáticos en batch o en lotes.
9. Revisión de almacenamiento y copias de respaldo.
10. Revisión del cumplimiento de migración de IPV4 a IPV6 y fases de implementación.
11. Revisión y evaluación de los planes de contingencia y continuidad del negocio (Centro de cómputo alterno).
12. Evaluación de los perímetros de seguridad definidos para los centros de procesamiento.
13. Revisión de los controles de acceso físico.
14. Verificación del registro y evaluación de los accesos al centro de cómputo.
15. Validación que los controles del entorno físico correspondan a los riesgos identificados.
16. Revisión de los controles para la ejecución de arqueos de medios magnéticos y evidencias respectivas.
17. Revisión y evaluación de la custodia de respaldo externa de backup.
18. Revisión y verificación de pruebas de restauración de backup (copias de respaldo).
19. Revisión y verificación que las copias de seguridad de sistemas, aplicaciones, datos, Excel u otras herramientas y documentación se estén realizando de conformidad con una planificación definida, así como probar y mantener legibles las copias de seguridad y la definición de los requerimientos para el almacenamiento de las copias, dentro y fuera de la propia ubicación, que satisfagan los requerimientos del negocio.
20. Evaluación a los controles de restauración de copias de respaldo (backup).
21. Evaluación de la entrega de respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. (Recuperar el servicio normal;

registrar y completar las peticiones de usuario; registrar, investigar, diagnosticar, escalar y resolver incidentes de 1er, 2do y 3er nivel de atención.)

22. Evaluación de la adecuada administración de las licencias de software de forma que se mantenga el número óptimo de licencias para soportar los requerimientos de la entidad y el número de licencias en propiedad sea suficiente para cubrir el software instalado y en uso.
23. Revisión y verificación de la renovación de contratos de mantenimiento y soporte del licenciamiento.
24. Evaluación a través de software instalado en los equipos de la entidad para determinar a ciencia cierta el desempeño de la infraestructura existente y licenciamiento efectivamente instalado.
25. Verificación del licenciamiento de software y Antivirus.
26. Evaluación del cableado – redes eléctricas y de datos de la entidad de conformidad a las normas y estándares internacionales del mercado y sus tecnologías actuales.
27. Revisión y verificación del mantenimiento periódico de la Red de Datos y Corriente Eléctrica Regulada. (certificación de la red.), UPS, Aire Acondicionado.
28. Evaluación del análisis de Impacto al Negocio (BIA) para las aplicaciones CORE críticas de la entidad.
29. Evaluación de las estrategias de recuperación definidas e implementadas.
30. Revisión de los resultados de la última prueba realizada al plan de continuidad.
31. Evaluación de la aplicación de las estrategias de recuperación para la situación actual de pandemia (COVID-19).
32. Evaluación de estrategias de respaldo y contingencia de la plataforma tecnológica que soporta las aplicaciones objeto de la auditoría.
33. Evaluación de la implantación y mantenimiento de un plan que permita a la entidad y al área de Tecnologías, responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios tecnológicos requeridos, y mantener la disponibilidad de la información a un nivel aceptable.
34. Evaluación de estrategias de respaldo y contingencia de la plataforma tecnológica que soporta las aplicaciones.
35. Revisión y evaluación del Plan de Recuperación de Desastres (DRP) y las medidas para mitigar el impacto.

3. ALCANCE

Se realizó Auditoría Interna de Gestión al componente del Centro de Datos y Operaciones de Red, evaluando la aplicabilidad de los procesos y procedimientos establecidos en los manuales y las circulares internas, políticas y normatividad legal vigente, donde se evaluó el periodo comprendido entre el 1 de enero de 2020 al 31 de diciembre de 2020.

Esta auditoría se llevó acabo en cumplimiento a las normas y técnicas de auditoría generalmente aceptadas, con fundamento en normas internacionales de auditoría basadas en riesgos, la auditoría se realizó del 28 de febrero al 16 de abril de 2021.

4. DESARROLLO DE LA AUDITORÍA

4.1. EVALUACIÓN DE AUDITORÍAS ANTERIORES

4.1.1. Auditorías Anteriores, Revisadas las acciones previstas en el Plan de Mejoramiento suscrito producto de la Auditoría realizada en el año 2017 al proceso de Infraestructura Tecnológica se observó que cinco (5) de ellas se relacionan con el componente de Centro de datos y operaciones de Red, como se muestra en el siguiente cuadro:

HALLAZGO	DESCRIPCION DE HALLAZGO	ACCION DE MEJORA	ACTIVIDADES / DESCRIPCIÓN	ACTIVIDADES / UNIDAD DE MEDIDA
5.1.1 Ausencia de DRP	CISA no ha formalizado en el marco de un DRP visible para la entidad a través del sistema de gestión los controles hoy existentes que permiten garantizar la recuperación de la información en caso de desastre. No existe un plan corporativo de continuidad de negocio que revele para el DRP los procesos críticos y los habilitadores y servicios tecnológicos que deben prevalecer en presencia de un desastre mayor.	Contratar los servicios tecnológicos necesarios para contar con una infraestructura de cómputo puertas afuera de CISA que permita garantizar la duplicación asíncrona o sincrónica de la información y la duplicación de los servidores y estructuras de datos de los sistemas críticos para la entidad y los terceros.	Infraestructura de cómputo alterna contratada	Contrato de Servicios

HALLAZGO	DESCRIPCION DE HALLAZGO	ACCION DE MEJORA	ACTIVIDADES / DESCRIPCIÓN	ACTIVIDADES / UNIDAD DE MEDIDA
			Plan de Recuperación de Desastres - DRP construido y socializado a la entidad y los terceros	Documento DRP, Construido, aprobado y divulgado
5.1.2 Inconsistencia en la externalización de copias de respaldo	Conocimiento parcial del procedimiento de externalización por parte de algunos miembros de la Jefatura de Operaciones Tecnológicas.	Entrenamiento y socialización del proceso de externalización a la totalidad de los integrantes de la Jefatura de Operaciones tecnológicas, así como del debido diligenciamiento de los formatos que obligue el procedimiento y los propios del proveedor del servicio de custodia externa.	Capacitación interna al grupo de operaciones tecnológicas en el manejo de externalización	Capacitación
			Soporte de externalización por 6 meses	Formato y envíos al proveedor
5.1.3 Falta de Evidencia para la restauración de copias de respaldo	Documentación parcial en la evidencia de restauración de los datos desde el motor de base de datos	Resocialización del procedimiento por parte de los responsables de las pruebas de restauración de las copias de respaldo.	Capacitación interna al grupo de operaciones tecnológicas en la construcción de las evidencias que respaldan la acción de restauración.	Capacitación
5.1.4 Controles ambientales del Centro de Cómputo	La inversión en el Centro de Cómputo está sujeta a la decisión de la entidad de realizar los cambios locativos que serán propuestos por la Coordinación Administrativa a la entidad. Lo anterior dado que el sistema de extinción y el techo falso se	Una vez se conozca la decisión de la entidad frente a las obras locativas, se procederá a realizar los procesos de compra de bienes y/o servicios para la instalación de los	Controles adquiridos/rentados e instalados	Implementación de Control (1. techo ignifugo, 2. Sistema de extinción de incendios)

HALLAZGO	DESCRIPCION DE HALLAZGO	ACCION DE MEJORA	ACTIVIDADES / DESCRIPCIÓN	ACTIVIDADES / UNIDAD DE MEDIDA
	construyen sobre medida y su traslado obligaría sobrecostos.	controles ausentes en el Centro de Cómputo.		
	El arqueo de medios no está descrito en el procedimiento de externalización de medios ni ha hecho parte del alcance contratado con el custodio externo.	Incluir la actividad en la circular 093 y en el alcance del contrato con el custodio externo para que se le permita a CISA ejecutar arqueo periódico en instalaciones del proveedor y almacenar dichas evidencias.	Actualización de CN093 incluyendo el procedimiento de arqueo físico de medios	Procedimiento
			Incluir actividad de arqueo físico dentro del alcance del contrato del custodio externo de medios	Minuta de contrato
6.2 Falta de trazabilidad en el control de acceso al centro de cómputo	Se consideró al momento de la auditoría que no era posible realizar la lectura de la información contenida en el control biométrico ya que en la inmediatez de la presentación de la evidencia no fue fácil realizar la extracción de la información desde el dispositivo y su posterior lectura.	Instalar software de lectura del archivo de permisos del sistema biométrico	Instalar software de lectura del archivo de permisos del sistema biométrico	Software ZKAccess3.5 Security System instalado

De acuerdo a lo anterior se verificó la implementación y efectividad de las acciones suscritas en el plan de mejoramiento para soportar el cierre de las mismas, el equipo auditor realiza los siguientes procedimientos:

Hallazgo 5.1.1 Ausencia de DRP (Plan de Recuperación de Desastre): Se verificó la implementación de la política descrita en el numeral 5.16 - Control DRP, contenida

en la circular normativa 093 y la cual tiene alcance con la implementación del BCP (Continuidad del Negocio) y DRP (Plan de Recuperación de Desastre).

Apoyados en la métrica de cumplimiento, se verificó que se estableció un contrato N° 030-2019 con COLUMBUS Networks Colombia Ltda, para la prestación de los servicios infraestructura virtual e implementar un esquema de recuperación de desastres – DRP; por lo tanto el equipo auditor considera el cierre del hallazgo.

Hallazgo 5.1.2 Inconsistencia en la externalización de copias de respaldo: No se identificó evidencia que soporte la capacitación dada al grupo de operaciones tecnológicas relacionada con los procedimientos de custodia externa.

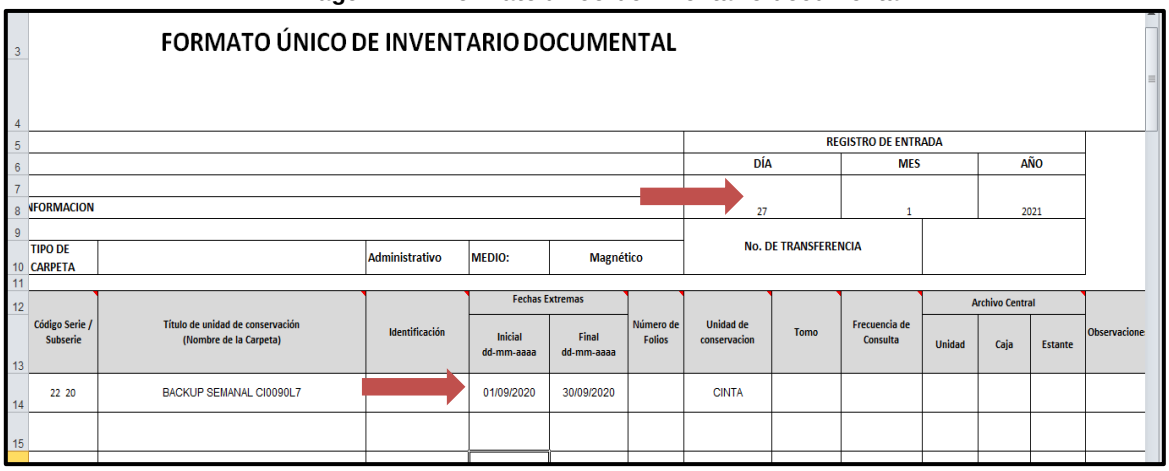
Se evidenció que en el año 2018 la auditoría interna revisó el cumplimiento de las remisiones de las copias al externo, cumpliendo con el diligenciamiento del formato en el momento de dicha revisión.

Aunque la unidad de medida del hallazgo fue la capacitación, se verificó el cumplimiento del procedimiento, calidad de uso de formatos y las evidencias aportadas a la auditoría interna en el 09-2018.

En el desarrollo de la auditoría se realiza un análisis de las evidencias entregadas en los archivos relacionados en *"Evidencias 3\13.Procedimiento para la gestión de copias de respaldo de la información*", para lo cual se verificó el diligenciamiento y uso del formato "*Formato único de inventario documental – fuid.xls*" y la aplicación del "*Instructivo para la generación de backups.pdf*", donde se describe que los envíos de copias externas se realizan mensual y semanal; lo que permitió identificar que el hallazgo no se cierra y en la verificación de efectividad se demostró que:

La fecha registrada en el campo "*Registro de Entrada*" del "*Formato Único de Inventario Documenta*l" no tiene una relación cronológica con las fechas registradas en el campo "*Fechas Extremas"* que corresponden al periodo inicial y final del backup efectuado. Esto se evidencia en cinco (5) de los nueve (9) periodos solicitados, donde se incluyen formatos de los años 2020 y 2021. En la imagen 1 se observa que la fecha final de la copia es el 30-09-2020 y la fecha de entrada es el 27-01-2021, siendo aproximadamente cuatro meses después de realizado el backup, el cual debería corresponder a un lapso de periodo cercano a la fecha final registrada.

Imagen 1. Formato único de inventario documental



FORMATO ÚNICO DE INVENTARIO DOCUMENTAL

								REGISTRO DE ENTRADA							
								DÍA	MES	AÑO					
NFORMACION								27	1	2021					
TIPO DE CARPETA		Administrativo	MEDIO:	Magnético				No. DE TRANSFERENCIA							
Código Serie / Subserie	Título de unidad de conservación (Nombre de la Carpeta)	Identificación	Fechas Extremas		Número de Folios	Unidad de conservacion	Tomo	Frecuencia de Consulta	Archivo Central			Observaciones			
			Inicial dd-mm-aaaa	Final dd-mm-aaaa					Unidad	Caja	Estante				
22 20	BACKUP SEMANAL CI0090L7		01/09/2020	30/09/2020		CINTA									

Fuente: Información de la Dirección de Tecnología del 15 de Febrero de 2021

Basados en lo anterior se concluye que el hallazgo no se cierra, por lo tanto, es importante plantear una nueva acción que permita corregir la debilidad identificada y de lugar al cierre del hallazgo.

Hallazgo 5.1.3 Falta de Evidencia para la restauración de copias de respaldo: Realizada la verificación al plan de mejoramiento correspondiente, se dio cumplimiento al 100% de las acciones de capacitación prevista en el plan. El equipo auditor validó las evidencias entregadas por CISA; observando:

- Un formato firmado por los miembros del área de tecnología, aceptando la capacitación recibida en relación con el procedimiento de restauración de información.

- La presentación de la capacitación recibida para el proceso de Gestión documental como soporte del contenido recibido.

Se concluye que la acción de capacitación interna al grupo de operaciones tecnológicas se cumplió y las evidencias respaldan la acción, razón por la cual se cierra el hallazgo.

Hallazgo 5.1.4 Controles ambientales del Centro de Cómputo: Para la verificación de la "implementación de control (1. Techo ignifugo, 2. Sistema de extinción de incendios)", se solicitó el avance de la reubicación el centro de cómputo, identificando que, aunque cuentan con un proyecto aprobado para la construcción

de un nuevo centro de cómputo que cuente con adecuados controles físicos y ambientales; pero no hay soportes para el cierre de este hallazgo. Ver desarrollo en el numeral 4.4.

Para la recomendación de actualizar el documento de la circular normativa 093, incluyendo el procedimiento de arqueo físico de medios, se verificó el mismo y se observó que se incluyó el Anexo No.15 Instructivo para realizar arqueo de medios electrónicos el 05 de abril de 2019.

En la revisión del cumplimiento de la recomendación "Incluir actividad de arqueo físico dentro del alcance del contrato del custodio externo de medios", se soporta con la inclusión de la cláusula en el contrato del Custodio de Medios (Arprotec), el Numeral 19 de la Cláusula Cuarta – Obligaciones específicas del contratista. Ver ruta \\serverfile\Presidencia\AUDITORIA_INTERNA\2017\Auditoria de Tecnología\PLAN DE MEJORAMIENTO\HALLAZGO 5.1.4 y según lo analizado por auditoria se cierra el hallazgo.

Hallazgo 6.2 Falta de trazabilidad en el control de acceso al centro de cómputo: Se verificó la instalación del sistema biométrico - ZKAccess3.5 Security System y se evidenció el informe de registro de acceso al centro de cómputo. Se soporta con la evidencia identificada en la ruta compartida por CISA \\serverfile\Presidencia\AUDITORIA_INTERNA\2017\AuditoriadeTecnología\ PLAN DE MEJORAMIENTO\ OBSERVACION 6.2.

Se concluye que el hallazgo se cierra al dar cumplimiento del registro de acceso al centro de cómputo generado desde el sistema ZKAccess3.5 Security System.

4.2. EVALUACIÓN DE RIESGOS

4.2.1. Metodología de Riesgos: Central de Inversiones S.A tiene definido en la Circular Normativa N° 107 "*Política de Administración de Riesgos en Central de Inversiones S.A*" Versión 22 del 18 de diciembre de 2020, los lineamientos relacionados con la gestión de los riesgos que se aplican en los procesos de la organización, dentro de los cuales se encuentra los del proceso de Infraestructura Tecnología de la entidad. La metodología está alineada con los aspectos definidos en la guía de riesgos de la Función Pública y el estándar internacional ISO 31000 sobre Administración de Riesgos.

4.2.2. Valoración y Tratamiento de los Riesgos: La información de riesgos aportada por el proceso auditado, refleja que la Dirección de Tecnología y Sistemas de Información viene aplicando la metodología definida en la Circular Normativa N°107 "*Política de Administración de Riesgos en Central de Inversiones S.A*" Versión 22 del 18 de diciembre de 2020 y que se ha realizado el monitoreo periódico correspondiente. En el mapa relacionado a continuación se describen los dos riesgos identificados del proceso, clasificados como riesgo de corrupción y riesgo operativo:

Imagen 2. Matriz de Riesgos – Infraestructura tecnológica

CISA
CENTRAL DE INVERSIONES S.A.

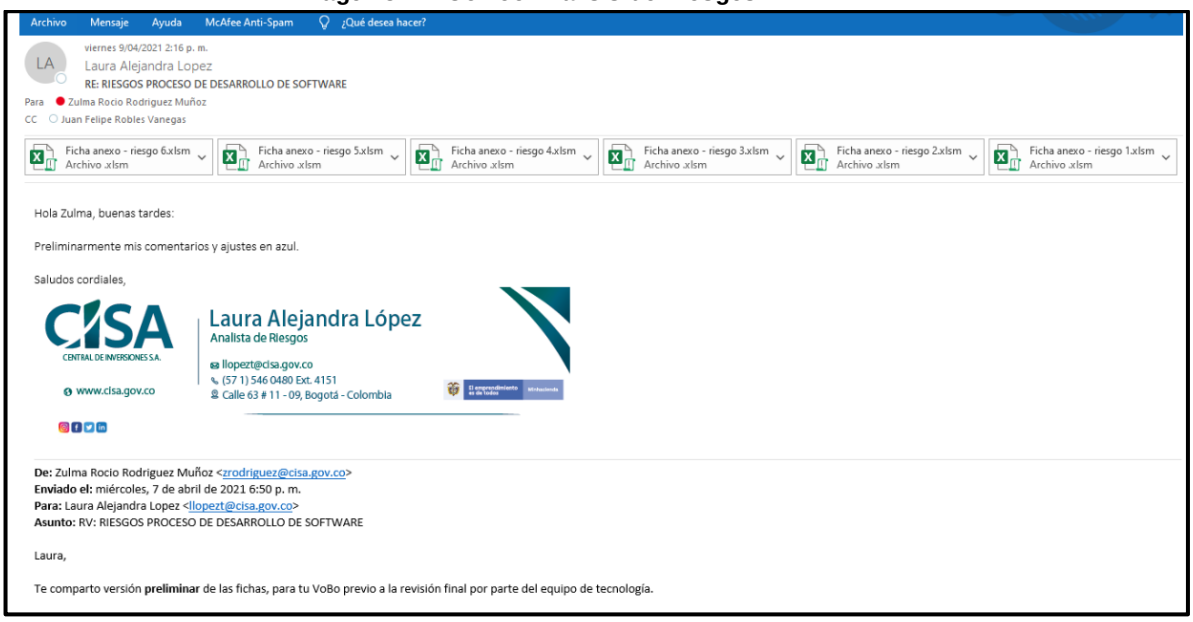
Matriz de riesgos - Infraestructura tecnológica

Procesos	Clase	Nombre	Descripción	Agentes generadores
* Infraestructura Tecnológica	Riesgo de Corrupción	RC-IT-01 Recibir y/o pagar bienes o servicios sin el cumplimiento de los requisitos establecidos contractualmente para beneficio propio o de terceros	Materialización del riesgo: Se entenderá como materializado el riesgo cuando en la instancia correspondiente se establezca la culpabilidad sin lugar a dudas. Certificar el cumplimiento del objeto contractual sin que se de cumplimiento a las obligaciones y condiciones establecidas buscando beneficio propio o para un tercero.	* Comportamiento humano
* Infraestructura Tecnológica	Riesgo Operativo	RO-IT-01 Indisponibilidad de los servicios tecnológicos que provee la Dirección de Tecnología a la entidad y a terceros	Materialización objetiva: Esta materialización de riesgo solo se evaluará de forma interna ya que los servicios de terceros estan en nube, implicando que los riesgos están en el proveedor de servicio y contemplados en los contratos. Con respecto a los servicios internos se entenderá materializado el riesgo cuando en el cuatrimestre evaluado el indicador asociado a la disponibilidad de servicios del SIG, haya estado por debajo del limite inferior en dos (2) de los tres (3) periodos evaluados. Fallas en los servicios tecnologicos que provee la Dirección de TI a todas las areas de negocio de la entidad y que afecten la normal operación de los servicios y accesos a los sistemas de información propios y de terceros que tiene CISA. Adicionalmente, Inconvenientes en la conectividad de terceros a los servicios tecnologicos que provee la entidad a las areas y terceros que requieren acceder para realizar su gestión (VPN, telefonia, servicios de red MPLS, portal web).	* Circunstancias políticas * Aspectos tecnológicos

Fuente: Información de la Dirección de Tecnología del 15 de enero de 2021

Se evidencia que en el mapa de riesgos no se está reflejando un análisis detallado respecto a los elementos definidos en la caracterización de los procesos de Operaciones Tecnológicas asociadas a las actividades de gestión de capacidad y desempeño, atención de mesa de ayuda, gestión de copias de respaldo de la información, entre otros. Es de anotar que la Dirección de Tecnología informa que se encuentra en el proceso de identificación de los riegos del proceso de gestión tecnológica con apoyo con la Analista de Riesgos asignada, mostrando como avance la declaración de riesgos, análisis, valoración del riesgo y controles para el subproceso de construcción de software en sus diferentes etapas; evidenciado en el correo electrónico generado por el Director de Tecnología el 15 de abril del 2021, entre los que se encuentran las comunicaciones de la analista de riesgos y el área de tecnología como se observa en la siguiente imagen.

Imagen 3. Correo Análisis de Riesgos

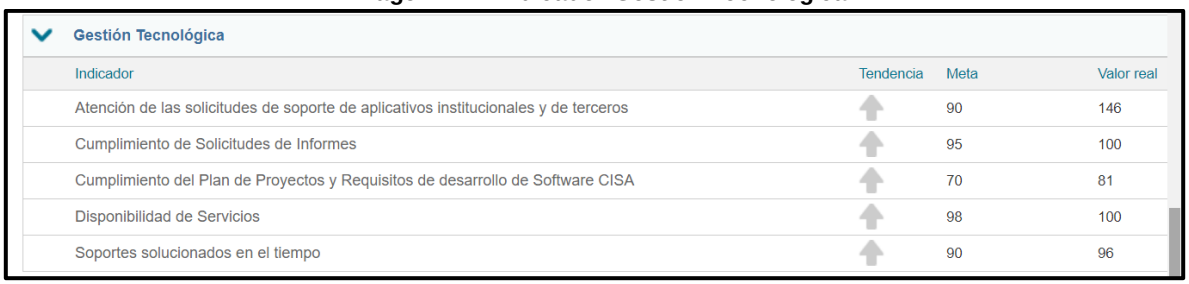


Fuente: Información de la Dirección de Tecnología del 15 de enero de 2021

4.3. EVALUACIÓN DE INDICADORES

De los cinco indicadores definidos para el proceso de Gestión Tecnológica, dos tienen relación con la Operación que soporta la infraestructura tecnológica de la entidad y se encuentran configurados en la herramienta ISOLUCION como se muestra en la siguiente imagen:

Imagen 4. Indicador Gestión Tecnológica



Gestión Tecnológica

Indicador	Tendencia	Meta	Valor real
Atención de las solicitudes de soporte de aplicativos institucionales y de terceros	↑	90	146
Cumplimiento de Solicitudes de Informes	↑	95	100
Cumplimiento del Plan de Proyectos y Requisitos de desarrollo de Software CISA	↑	70	81
Disponibilidad de Servicios	↑	98	100
Soportes solucionados en el tiempo	↑	90	96

Fuente: Herramienta Isolucion – 14 de abril de 2021

a. Indicador: Disponibilidad del Servicio

Se consulta el resultado del indicador "Disponibilidad del servicio"; en un periodo de un año, del 14 de abril de 2020 hasta el 14 de abril del 2021, observando que la

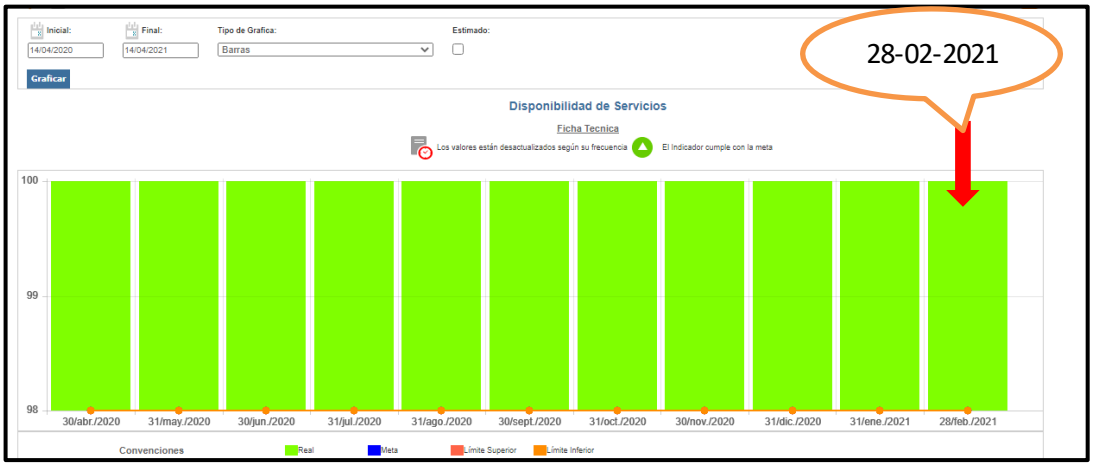
periodicidad estipulada es mensual; y analizando este principio debería estar actualizado a marzo 31 de 2021. Ver imagen 5. Los valores están desactualizados y reflejan hasta el 28 de febrero de 2021, lo que puede generar dificultad en la identificación de situaciones que requieran la implementación de planes de acción para subsanar las fallas que se puedan presentar.

El cálculo de este indicador se obtiene con la siguiente fórmula:

((HOM x CSO) - (HNDM x CSND)) / (HOM x CSO) * 100

HOM (Horas Ofrecidas al Mes Lunes a Viernes de 7am - 7 pm)
CSO (Cantidad de Servicios Ofrecidos)
HNDM (Horas no Disponibles al mes)
CSND (Cantidad de Servicios No Disponibles al mes)

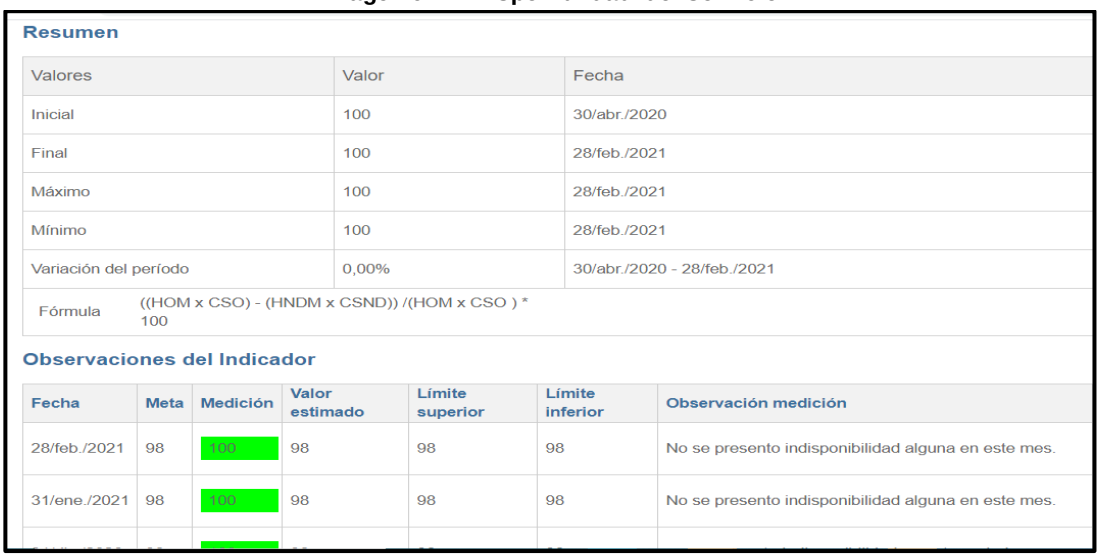
Imagen 5. Disponibilidad del servicio



Fuente – Herramienta Isolucion – 14 de abril de 2021

El objetivo de este indicador es "Determinar el nivel de disponibilidad de los servicios Tecnológicos ofrecidos por CISA, tanto para usuarios como para partes Interesadas". Al analizar la fórmula, esta mezcla los tiempos no disponibles de los servicios con el total de servicios, es decir, sobrestimando la cantidad de horas no disponibles, por lo cual se requiere ajustar el diseño de la formulación del indicador.

Imagen 6. Disponibilidad del servicio



Resumen

Valores	Valor	Fecha
Inicial	100	30/abr./2020
Final	100	28/feb./2021
Máximo	100	28/feb./2021
Mínimo	100	28/feb./2021
Variación del período	0,00%	30/abr./2020 - 28/feb./2021
Fórmula	((HOM x CSO) - (HNDM x CSND)) /(HOM x CSO) * 100	

Observaciones del Indicador

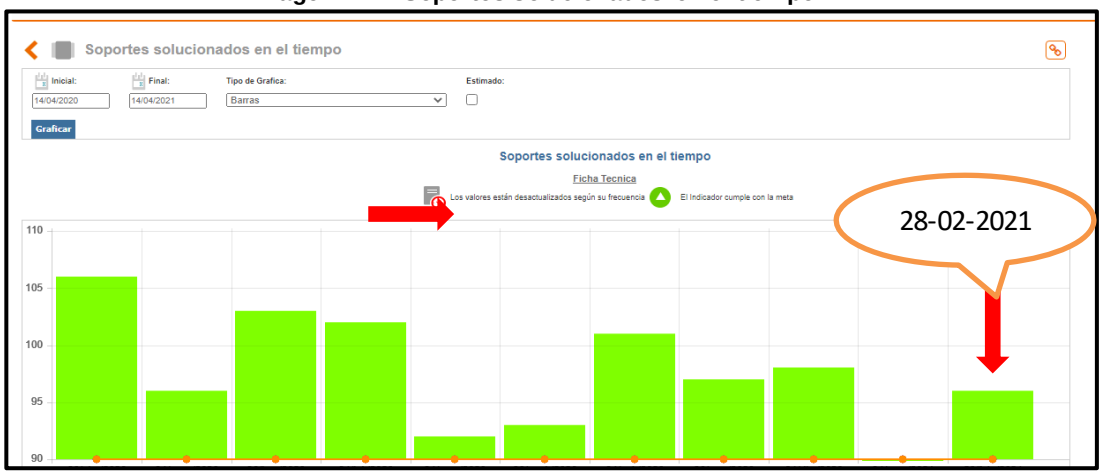
Fecha	Meta	Medición	Valor estimado	Límite superior	Límite inferior	Observación medición
28/feb./2021	98	100	98	98	98	No se presento indisponibilidad alguna en este mes.
31/ene./2021	98	100	98	98	98	No se presento indisponibilidad alguna en este mes.

Fuente: Herramienta Isolucion – 14 de abril de 2021

b. Indicador: Soporte solucionados en el tiempo

El indicador "Soporte solucionados en el tiempo"; está desactualizado según su frecuencia mensual, descrita en la ficha técnica.

Imagen 7. Soportes solucionados en el tiempo



Fuente: – Herramienta Isolucion – 14 de abril de 2021

El objetivo de este indicador es "determinar el nivel de atención oportuna de los soportes técnicos o incidentes tecnológicos que generan cada uno de los procesos". Observando que, para la vigencia de abril de 2020 a abril de 2021, el área de Gestión tecnológica realizó la medición y reporte al 28 de febrero de 2021, evidenciando que

cumplió la meta del 90%; los casos fueron solucionados en un tiempo menor o igual a 8 horas en el rango de 8 am-5pm.

El cálculo se obtiene con la siguiente formula:

(No. de soportes atendidos en el tiempo (Zeus) / No. de soportes reportados) * 100

En el cálculo del indicador "Soporte solucionados en el tiempo"; basado en la fórmula: (No. de soportes atendidos en el tiempo (Zeus) / No. de soportes reportados) * 100, identificamos que éste incluye los casos que fueron solucionados en el mes anterior y el usuario no los ha cerrado. Aspecto que puede generar inconsistencias en el cálculo del indicador y/o inadecuada medición en el monitoreo y gestión de los servicios de soporte de TI.

4.4. CENTRO DE CÓMPUTO

4.4.1 Control de acceso físico y ambientales al centro de cómputo

Con base en el documento Circular Normativa 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, numeral 5.2. se realizó por parte del equipo auditor prueba de recorrido a las instalaciones de la Dirección General en Bogotá el 1 de marzo de 2021 y se identificó la implementación de los controles de acceso físico y ambiental. Se solicitaron los siguientes soportes documentales para evaluar la eficacia de los controles existentes:

- El listado de usuarios autorizado con acceso al centro de cómputo.
- Listado del personal que ingresó al centro de cómputo durante los meses de noviembre, diciembre de 2020 y enero de 2021 en los formatos de ingreso al CPD.
- Registro del sistema biométrico del año 2020 con los ingresos al centro de cómputo para compararlos con el registro manual en el formato del área de tecnología.

En la inspección del centro de cómputo (tercer piso) y los centros de cableado localizados en el primer y segundo piso, se verificó que existen controles ambientales de humedad, techo, piso falso a prueba de fuego, planta generadora, UPS y aires acondicionados, etc.; sin embargo, existen debilidades en los controles ambientales del centro de cómputo debido a la ausencia de un techo ignifugo, sistema de supresión de incendios y cableado sin etiquetas.

CISA cuenta con un diseño para la construcción de un nuevo centro de cómputo, además, se indica por parte de la Dirección de Tecnología que se inició con la contratación de la interventoría para la adecuación del Centro de Cómputo, no obstante, a la fecha de la auditoria no se contaba con dicha contratación.

4.4.2 Mantenimiento de equipos tecnológicos

Para la revisión del cumplimiento de los mantenimientos de los equipos de control ambientales y eléctricos del centro de cómputo y planta telefónica, el equipo de auditoria se basó en el documento Circular Normativa 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, numeral 5.2.4. Basados en lo anterior y para verificar si los mantenimientos se encuentran debidamente planeados durante el año 2020 y que exista un monitoreo periódico, se evaluaron los siguientes documentos relacionados con el anexo 2 Plan de mantenimiento versión 4 del 30 de diciembre de 2020 de la CN 093 versión 62:

- Los formatos de "mantenimiento preventivo equipos de aire acondicionado" generados por el proveedor.
- El documento "Plan mantenimiento 2020.xls" describe los mantenimientos de software y Hardware planeados para el 2020.
- Se validó la existencia de un procedimiento de control que verifique la calidad del servicio y que incluya el mantenimiento de los otros componentes de seguridad ambiental del centro de datos.

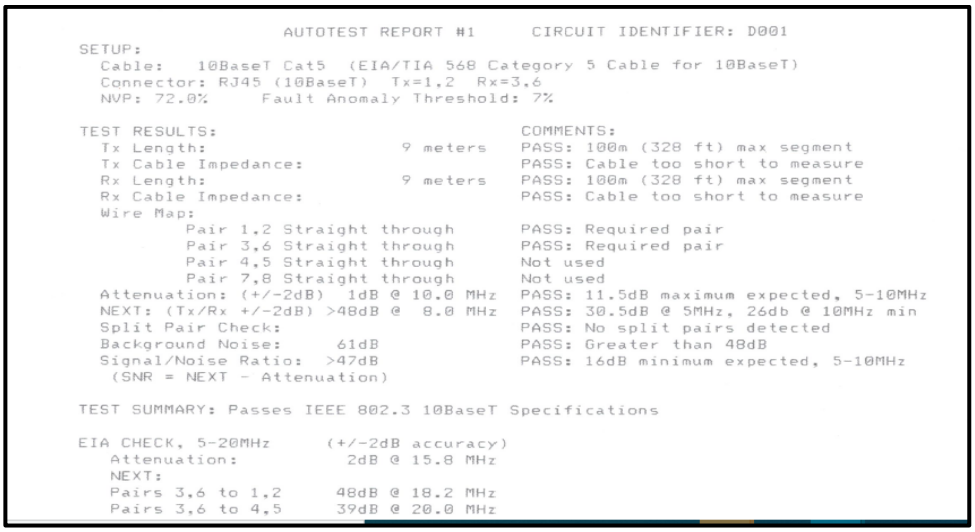
Se evidencia en lo soportes de mantenimiento de agosto, mayo y diciembre de 2020, la revisión del techo, del piso, de los dos aires acondicionados, temperatura y humedad del centro de cómputo de la sede principal y revelan que se encuentran en correcto funcionamiento.

Cuentan con evidencia de los mantenimientos del sistema UPS (Servicio de respaldo eléctrico y supresor de picos) realizados en las sedes de Medellín, Barranquilla y Cali realizados el 16/01/2021 y Bogotá el día 26/12/2020; cumpliendo con las actividades de mantenimiento y en las redes de datos se realiza internamente por los mismos especialistas del área de tecnología y su funcionamiento se encuentra sin eventos adversos identificados.

Para la revisión de los mantenimientos del cableado que soporta los servicios tecnológicos, se revisó el documento de revisión del cableado estructurado del nodo

de Barranquilla, confirmando que es una prueba técnica que revela el correcto funcionamiento del cableado. Como se evidencia en la imagen siguiente:

Imagen 8. Test de la red de datos de Barranquilla



```
                    AUTOTEST REPORT #1      CIRCUIT IDENTIFIER: D001
SETUP:
  Cable:   10BaseT Cat5  (EIA/TIA 568 Category 5 Cable for 10BaseT)
  Connector: RJ45 (10BaseT)  Tx=1,2  Rx=3,6
  NVP: 72.0%      Fault Anomaly Threshold: 7%

TEST RESULTS:                                COMMENTS:
  Tx Length:                    9 meters     PASS: 100m (328 ft) max segment
  Tx Cable Impedance:                        PASS: Cable too short to measure
  Rx Length:                    9 meters     PASS: 100m (328 ft) max segment
  Rx Cable Impedance:                        PASS: Cable too short to measure
  Wire Map:
          Pair 1,2 Straight through          PASS: Required pair
          Pair 3,6 Straight through          PASS: Required pair
          Pair 4,5 Straight through          Not used
          Pair 7,8 Straight through          Not used
  Attenuation: (+/-2dB)  1dB @ 10.0 MHz      PASS: 11.5dB maximum expected, 5-10MHz
  NEXT: (Tx/Rx +/-2dB) >48dB @  8.0 MHz      PASS: 30.5dB @ 5MHz, 26db @ 10MHz min
  Split Pair Check:                          PASS: No split pairs detected
  Background Noise:      61dB                PASS: Greater than 48dB
  Signal/Noise Ratio:  >47dB                 PASS: 16dB minimum expected, 5-10MHz
   (SNR = NEXT - Attenuation)

TEST SUMMARY: Passes IEEE 802.3 10BaseT Specifications

EIA CHECK, 5-20MHz      (+/-2dB accuracy)
   Attenuation:           2dB @ 15.8 MHz
   NEXT:
   Pairs 3,6 to 1,2      48dB @ 18.2 MHz
   Pairs 3,6 to 4,5      39dB @ 20.0 MHz
```

Fuente: – Información de la Dirección de Tecnología del 24 de Febrero de 2021

Para la revisión de los mantenimientos del cableado que soporta los servicios de comunicaciones, se identificó que las ciudades se comunican por canales de voz, entre Medellín, Cali y Barranquilla por medio de una red IP a través del MPLS y canales redundantes para garantizar el servicio en caso de presentarse situaciones de contingencia.

En la planta telefónica de la Dirección general y en Cali, se realiza mantenimiento predictivo que incluye: Back up en CPU, copia de seguridad, limpieza de equipo, medición de voltaje, pruebas de carga satisfactoria, verificación aplicaciones y tarificación.

Imagen 9. Plan de mantenimiento

CISA Central de Inversiones S.A.

PLAN DE MANTENIMIENTO PREVENTIVO

PERIODO : 2020 ; F.P. : FECHA PROGRAMADA, F.R.: FECHA REALIZADA

EQUIPOS	DESCRIPCIÓN	CANTIDAD	FECHA	MES 1	2	3	4	5	6	7	8	9	10	11	12	OBSERVACIONES
Alcatel Planta Telefonica. (DIRECCION GENERAL)	Mantenimiento de Hardware	1													F.P	Realizar mantenimiento predictivo, Back up en CPU, copia de seguridad, Limpieza de equipo, medicion de voltaje, pruebas de carga, verificacion aplicaciones, tarificacion.
	Mantenimiento de Software														F.P	

Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

Se solicitó soporte del mantenimiento de la planta de Alcatel realizado el 1 de diciembre del 2020, evidenciando que se realizó el respectivo mantenimiento.

Imagen 10. Mantenimiento Alcatel

Código: F.04.008
Edición: 3

LLAMADA DE SERVICIO
REMISIÓN FACTURABLE
BO No. 61566

FECHA 1 12 20 PROYECTO MANTENIMIENTO X

CLIENTE: Central de Inversiones S. NIT:
E-MAIL: TELÉFONO: 3715900 EXT 4570
RESPONSABLE: Cindy de la hoz
DIRECCIÓN: Kra 54 # 68-196 Piso 2 DE 201 CIUDAD: Barranquilla
PRODUCTO: OXE

TIPO DE SERVICIO: COBRO ☐ CONTRATO X GARANTIA ☐

INGENIERO 1 Juan Jairo Cera INGENIERO 2 INGENIERO 3

ACTIVIDAD A REALIZAR: Mantenimiento Preventivo NÚMERO DE LLAMADA: Rm 061814

LABOR REALIZADA — MANTENIMIENTO PREVENTIVO X — CORRECTIVO ☐ — INSTALACIÓN ☐

Se Realiza Backup del Equipo de Voz de 9 Posiciones
Se Realiza limpieza en general del Equipo OXE
Se Verifica Condiciones Ambientales del Cuarto de Equipo
Se Valida Valores Eléctricos

Fuente: Información de la Dirección de Tecnología del, - 24 de Febrero de 2021

Se concluye que cuentan y cumplen con mantenimientos planeados durante el año 2020, lo que revela la efectividad del control establecido.

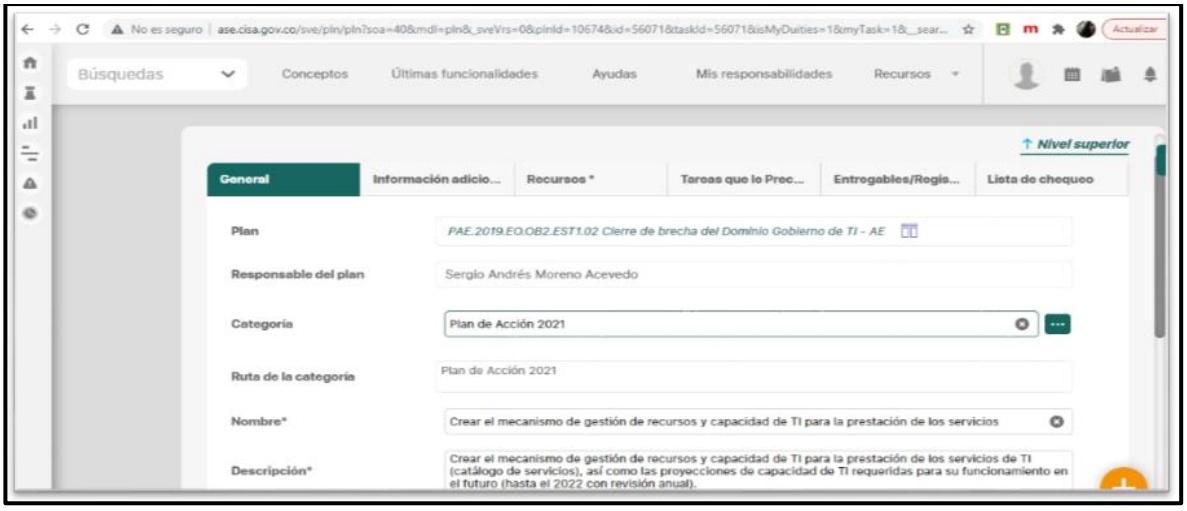
4.5 GESTIÓN DE LA CAPACIDAD Y DESEMPEÑO

Con base en el documento Circular Normativa 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, numeral 5.14 se pudo establecer que el área de Gestión Tecnológica "*debe monitorear el uso de recursos, así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro, con el fin de asegurar el funcionamiento de las aplicaciones o servicios tecnológicos. "*

Dado lo anterior el equipo de auditoría solicitó el modelo de operación de las aplicaciones sobre la infraestructura tecnológica y el plan de capacidad y desempeño de recursos tecnológicos, CISA hizo entrega del documento "Arquitectura Centro De Computo_10022021.pdf", como respuesta a la solicitud. Producto del análisis realizado a la información entregada, se identificó que la Entidad tiene un modelo definido de servicios y operación de las aplicaciones que están en producción, con una arquitectura establecida del centro de cómputo para los elementos que conforman la infraestructura virtual y física.

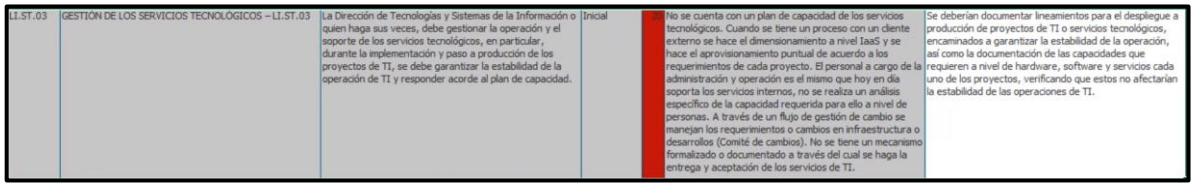
Actualmente el área de Gestión Tecnológica no cuenta con un Plan de Capacidad y de Gestión de Desempeño de TI; sin embargo, en reunión con el equipo de auditoría, el Director de Tecnología, suministró información relacionada con el plan de acción 2021 definido para dar cierre a la brecha identificada en el dominio Gobierno de TI, al no contar con un plan de capacidad de los servicios tecnológicos como se evidencia en las siguientes imágenes 11 y 12.

Imagen 11. Mantenimiento Alcatel



Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

Imagen 12. Documentar lineamientos



LI.ST.03	GESTIÓN DE LOS SERVICIOS TECNOLÓGICOS – LI.ST.03	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe gestionar la operación y el soporte de los servicios tecnológicos, en particular, durante la implementación y paso a producción de los proyectos de TI, se debe garantizar la estabilidad de la operación de TI y responder acorde al plan de capacidad.	Inicial		No se cuenta con un plan de capacidad de los servicios tecnológicos. Cuando se tiene un proceso con un cliente externo se hace el dimensionamiento a nivel IaaS y se hace el aprovisionamiento puntual de acuerdo a los requerimientos de cada proyecto. El personal a cargo de la administración y operación es el mismo que hoy en día soporta los servicios internos, no se realiza un análisis específico de la capacidad requerida para ello a nivel de personas. A través de un flujo de gestión de cambio se manejan los requerimientos o cambios en infraestructura o desarrollos (Comité de cambios). No se tiene un mecanismo formalizado o documentado a través del cual se haga la entrega y aceptación de los servicios de TI.	Se deberían documentar lineamientos para el despliegue a producción de proyectos de TI o servicios tecnológicos, encaminados a garantizar la estabilidad de la operación, así como la documentación de las capacidades que requieren a nivel de hardware, software y servicios cada uno de los proyectos, verificando que estos no afectarían la estabilidad de las operaciones de TI.

Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

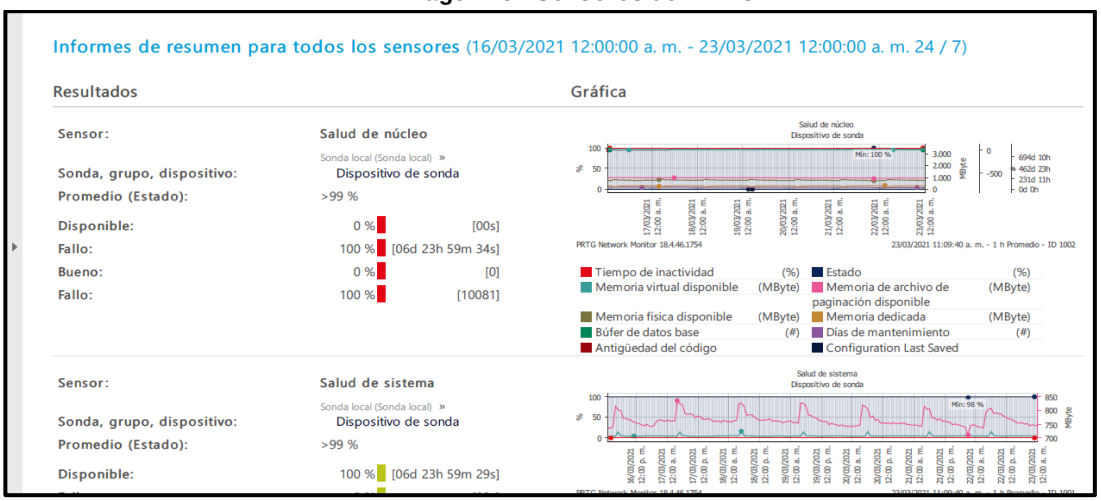
Ante la ausencia de un Plan de Capacidad, cuando se solicita un nuevo proyecto corporativo, siguen el flujo de Zeus, denominado como “Gestión de Cambios”, aquí se evalúa si tienen la capacidad para poder atender los procesos misionales, caso contrario se evalúa la opción de adquisición.

Para evaluar la gestión del desempeño y la capacidad de los recursos tecnológicos, se realizaron reuniones con el área de tecnología y en revisión de los soportes del monitoreo y control entregados, se identificó que:

- El Proceso TI cuenta con la herramienta de control PRTG que permite verificar la disponibilidad de los componentes, umbrales de uso, la internet provista por terceros y estado actual de los componentes, entre otros.

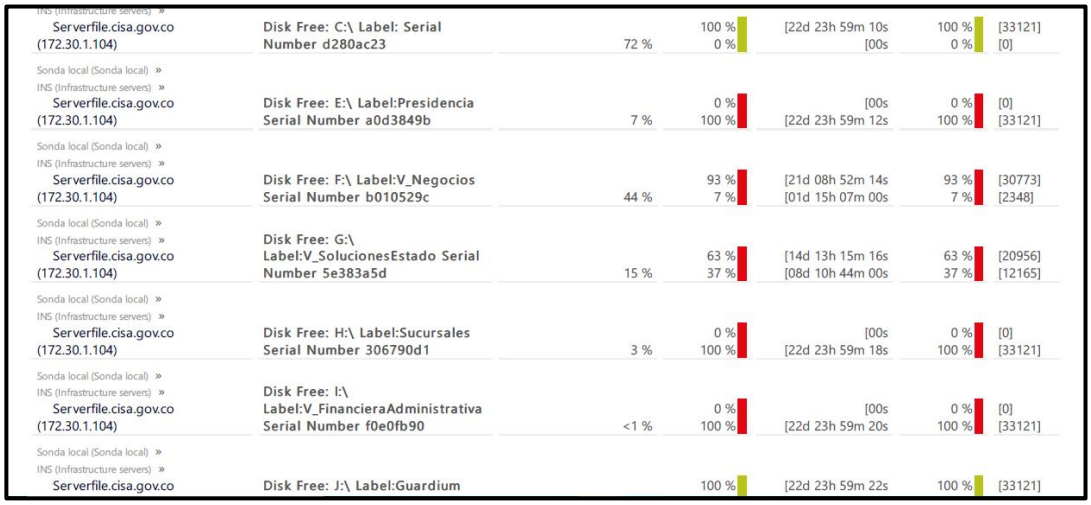
- Para el monitoreo de la Operación de TI, han definido en la herramienta (PRTG), 500 sensores para medir el desempeño y la capacidad de los sistemas tecnológicos de CISA. Esto tiene una categoría por colores como, rojas de alta criticidad y existe una falla, amarilla alerta una situación de posible falla y verdes se opera en normalidad. En el evento que se genere una alerta roja se genera de manera automática un correo electrónico al ingeniero de procesos de infraestructura para su atención.

Imagen 13. Sensores del PRTG



Fuente: Información de la Dirección de Tecnología del 24 de marzo de 2021

Imagen 14. Sensores del PRTG



Fuente: Información de la Dirección de Tecnología del 24 de marzo de 2021

De lo anterior no se evidencia trazabilidad de las acciones preventivas que se toman ante las alertas arrojadas en los sensores configurados con alertas amarillas, esto puede generar demoras en la atención y respuesta a incidentes e interrupciones del servicio originadas por falta de capacidad o degradaciones del desempeño.

Así mismo, se efectúo una revisión de los archivos de Excel "Capacidad_Almacenamiento.xlsx" y "Almacenes_de_Datos_VMWare.xls" los cuales permiten identificar el registro de la capacidad de los discos o datastore y el espacio disponible en los servidores y unidades virtualizadas, lo que permite al área

de Operaciones Tecnológicas establecer el espacio que tienen sobre las unidades de disco y tomar acciones preventivas requeridas en capacidad. El archivo de Excel "Almacenes_de_Datos_VMWare.xls" contiene el registro de la capacidad en disco de 54 servidores virtualizados, entre los que se encuentran los siguientes: VFileserver, Vm_Demeter, Vm_Eros, Vm_Hela, Vm_HeraServer, Vm_LuxriotServer, Vm_Pluto, Vm_Prometeo, Vm_ServerFile, Vm_Tartaro, VmTartaro2016, VM_TestSQL,Vm_Vidar, VmApolo, VmAramis, VmArtemisa, VmBogServer, VmCellServer, VmCeo, VmCromos, VmDataRoom, VmDevelopServer, VmDevopServer. La información analizada de la capacidad en espacio de los discos de VMWare y DataStore revela que cubren la capacidad de los servicios que soportan el negocio, de acuerdo a lo reflejado en las imágenes 15 y 16.

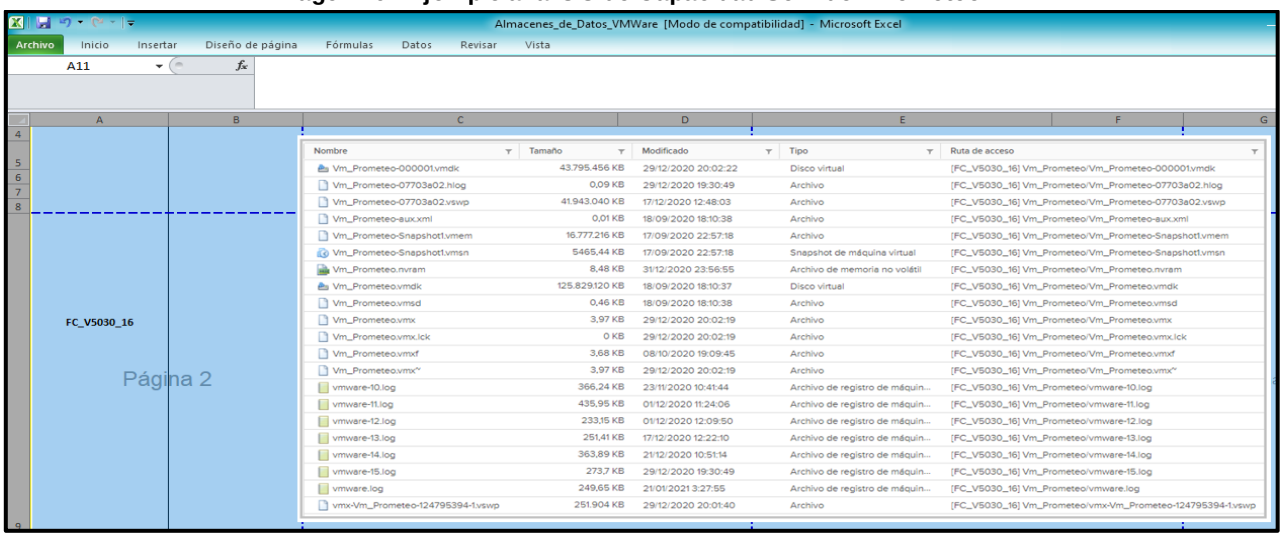
Imagen 15. Capacidad de Discos o Datastore

Nombre	Condición	Capacidad	Libre
srvesxi04_local	Normal	271 GB	266,81 GB
srvesxi03_local	Normal	271 GB	270,05 GB
srvesxi02_local	Normal	271 GB	270,05 GB
srvesxi01_local	Normal	271 GB	270,05 GB
ISOs	Normal	299,75 GB	110,48 GB
FC_V5030_16	Normal	1,71 TB	285,05 GB
FC_V5030_15	Normal	2 TB	860,59 GB
FC_V5030_14	Normal	2 TB	749,23 GB
FC_V5030_13	Normal	2 TB	458,2 GB
FC_V5030_12	Normal	2 TB	449,88 GB
FC_V5030_11	Normal	2 TB	1.014,26 GB
FC_V5030_10	Normal	1,86 TB	275,33 GB
FC_V5030_09	Normal	2 TB	996,82 GB
FC_V5030_08	Normal	2 TB	821,96 GB
FC_V5030_07	Normal	2 TB	529,56 GB
FC_V5030_06	Normal	2 TB	641,99 GB
FC_V5030_05	Normal	2 TB	318,26 GB
FC_V5030_04	Normal	2 TB	597,93 GB
FC_V5030_03	Normal	2 TB	841,04 GB
FC_V5030_02	Normal	2 TB	540,01 GB
FC_V5030_01	Normal	2 TB	582,89 GB
EVAP_DS4	Normal	1.023,75 GB	650,42 GB
EVAP_DS3	Normal	1.023,75 GB	265,2 GB
EVAP_DS2	Normal	1.023,75 GB	315,72 GB
EVAP_DS1	Normal	1.023,75 GB	706,61 GB
EVAD_DATASTORE02	Normal	499,75 GB	295,8 GB
EVAD_DATASTORE01	Normal	499,75 GB	379,58 GB

Capacidad_Datastore

Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

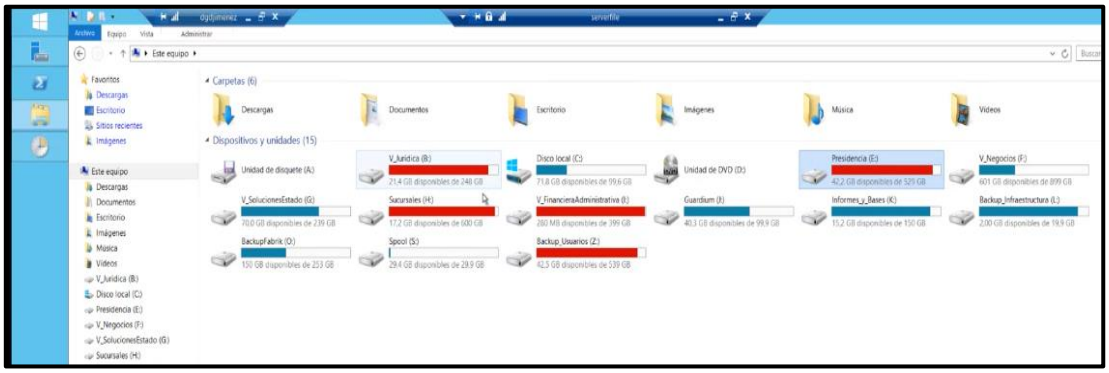
Imagen 16. Ejemplo análisis de Capacidad Servidor Prometeo



Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

Adicionalmente se efectuó revisión a la capacidad del servidor "serverfile" y se observó que algunos discos asignados para el almacenamiento de la información de los procesos: V_Juridica, V_FinancieraAdministrativa, Sucursales, Backup_Usuarios y Presidencia se encuentran muy cercanos a su máxima capacidad lo que podría afectar almacenamiento de información al usuario final en un corto tiempo, de llegar a ocuparse el máximo de capacidad, ver imagen 17.

Imagen 17. Capacidad en Disco disponible



Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

4.6 MESA DE AYUDA Y GESTIÓN DE INCIDENTES

Con base en el documento Circular Normativa 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, Anexo 11 denominado "Instructivos para gestionar los procedimientos de gestión tecnológica",

en este se relacionan los instructivos “para la atención de soporte de aplicativos Institucionales” y “para la atención y soporte tecnológico”. Se efectuaron reuniones con el Jefe de Operaciones se validó el procedimiento de soporte de atención a usuarios, con el fin de corroborar la gestión y monitoreo que realiza el área de Gestión Tecnológica en la entrega de respuesta oportuna y efectiva a los requerimientos de usuarios y la resolución de incidentes.

Se cuenta con una mesa de ayuda de microinformática, proveída por Microhard, mediante el contrato No. 029-2014 y adicionalmente brindan soporte técnico a los usuarios, dando cumplimiento al numeral 3.5 de la cláusula tercera del contrato, donde indica que “Por cada 80 equipos de cómputo de escritorio y/o portátiles, el contratista deberá poner a disposición de CISA y sin costo, un (1) técnico exclusivo en un horario de ocho (8) horas por cinco (5) días a la semana, en la sucursal o sede de CISA que disponga el supervisor del contrato”.

Los incidentes presentados en los aplicativos institucionales desarrollados internamente por CISA, son reportados a través de los líderes “ULA” a través del flujo en ZEUS “Soportes Aplicativos Institucionales” y los requerimientos de servicio técnico, pueden ser registrados por cualquier usuario a través del flujo ZEUS “Atención y Soporte Tecnológico” o comunicándose telefónicamente con la mesa de ayuda.

El monitoreo de atención y soporte tecnológico se realiza a través de tableros de control configurados por el área de Gestión Tecnológica para identificar el análisis del comportamiento de los requerimientos de soporte por parte de usuarios finales, en los cuales se pueden visualizar la totalidad de requerimientos anual, estado de requerimientos, cantidad y duración en promedio de atención por usuario, promedio de tiempos muertos.

Imagen 18. Tablero de control totalidad requerimientos año 2020

Fuente: Dirección de Tecnología del 24 de febrero de 2021

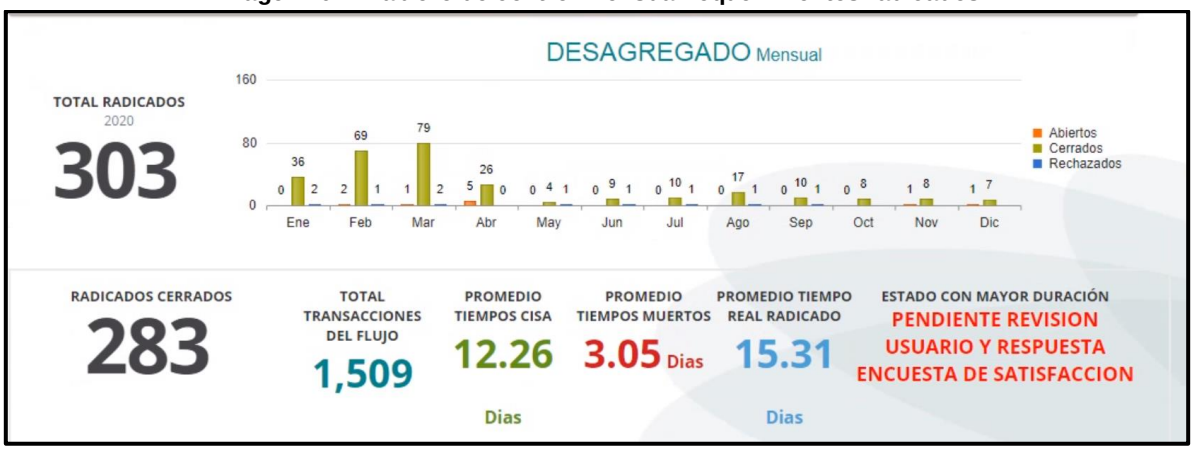
Imagen 19. Tablero de control promedio de estado de requerimientos año 2020

Estado	Cantidad	Promedio Duración	
RADICADO	306	0.67	Más Detalles
PENDIENTE VALIDAR SOLICITUD	300	0.79	Más Detalles
SOPORTE DE APLICATIVOS INSTITUCIONALES	4	0.27	Más Detalles
PROCEDIMIENTO DE ATENCION INCIDENTES SEGURIDAD DE LA INFORMACION	2	1.73	Más Detalles
PENDIENTE CLASIFICACION DE LA SOLICITUD	287	0.22	Más Detalles
PENDIENTE REALIZAR SOPORTE CONFORME A LA SOLICITUD	316	5.28	Más Detalles
PENDIENTE SOLICITAR IMPLEMENTACION DEL CAMBIO	1	1.05	Más Detalles

Usuario	Promedio Duración	
PAOLA ANDREA BAYONA JARABA	196.29	Más Detalles
CARLOS ALBERTO SANDOVAL VARGAS	157.09	Más Detalles
MARIA DE LOS ANGELES ESCANDON POLANIA	127.45	Más Detalles
JULIO CESAR VARON CORAL	114.08	Más Detalles
YULI ANDREA OLAYA CABEZAS	48.83	Más Detalles
LAURA TATIANA QUINTERO RAMIREZ	47.07	Más Detalles
PATRICIA ALEJANDRA FANDIÑO SILVA	39.93	Más Detalles
SOCIEDAD DE ACTIVOS ESPECIALES SAE	32.81	Más Detalles
JOSE GREGORIO BARRIOS FONTALVO	31.85	Más Detalles

Fuente: Información de la Dirección de Tecnología del 24 de febrero de 2021

Imagen 20. Tablero de control mensual requerimientos radicados



Fuente: Información de la Dirección de Tecnología del 24 de febrero de 2021

Como soporte de las actividades realizadas por el área de tecnología, al equipo de Auditoría le fue suministrado el archivo "BSC y Subproceso Operar procesos ágiles y óptimos.doc", en el cual se refleja el modelo de operación que planea implementar la Dirección de Tecnología para de gestión de problemas e incidentes y mesa de servicio, no obstante, a la fecha no cuentan con un procedimiento e indicadores para la gestión y medición de incidentes y problemas, que permita el aseguramiento de la atención y resolución de eventos que se puedan presentar en la infraestructura y servicios de TI.

Se sugiere fortalecer el diseño de controles para el aseguramiento en la administración, gestión y monitoreo de la mesa de ayuda e incidentes en los servicios de Tecnología.

4.7 GESTIÓN DE ACUERDOS DE NIVELES DE SERVICIO – ANS

De acuerdo a la circular normativa 093 versión 63, se observa que en el numeral 5.11 describen las "políticas de gestión de acuerdos de servicios" y el anexo 6 "Instructivo para la Gestión de Nivel de Servicios" donde se menciona la metodología para la definición y gestión de los acuerdos de niveles de servicio para mantener y mejorar la calidad de los servicios de TI a través de un constante ciclo de establecimiento, seguimiento y reporte de cumplimiento de acuerdos, en cuanto a los alcances del servicio de TI.

Respecto a lo anterior se analizó el "*Instructivo atención soporte aplicativos institucionales.docx*" el cual contiene los Acuerdos de Niveles de Servicios Internos, donde se relaciona la atención para incidentes presentados sobre los aplicativos en ambiente productivo; se establece el horario, la disponibilidad, los tipos de incidencias y nivel de soporte al mismo. Sin embargo, no incluyen todos los servicios provistos por el área de tecnología tales como: Telefonía, Internet, Correo, Impresoras, Red, Hardware, etc.

Se seleccionaron los proveedores críticos acorde con lo informado por el área de Gestión Tecnológica y se solicitaron los contratos de COLUMBUS Networks Colombia Ltda, IFX Networks Colombia S.A.S y MICROHARD S.A.S. identificando que:

- En el contrato de COLUMBUS Networks Colombia Ltda, se tienen establecidos Acuerdos de Niveles de Servicios mediante el Anexo 1 del contrato número 030-2019 para la prestación de los servicios infraestructura virtual e implementar un esquema de recuperación de desastres – DRP, se definen acuerdos medidos por Disponibilidad del servicio e Indisponibilidad, no obstante en el contrato no se establece una periodicidad de entrega de reportes a la Entidad con las variables de medición, que permitan reflejar la gestión de los servicios contratados, esto dificulta monitorear oportunamente la calidad y cumplimiento de los servicios de TI. Para los requerimientos de cambios, se definen los siguientes tiempos:

Imagen 21. Tiempo para requerimientos de cambios

Cambio Estándar	8 horas hábiles
Cambio No Estándar	Se seguirá el procedimiento de control de cambios.

Fuente: Información de la Dirección de Tecnología del- 24 de Febrero de 2021

Cuando la solicitud es generada por un incidente, reportado vía telefónica seguirán los siguientes tiempos de respuestas. Ver la imagen 22.

Imagen 22. Tiempo de atención

Prioridad del Incidente	Tiempo Máximo de Respuesta	Actualizaciones	Escalamiento 2do Nivel	Escalamiento 3er Nivel
Critico	Inmediata(*)	Contacto permanente si es necesario	Inmediata	Inmediato
Alto	30 min	Cada 30 minutos hasta ser resuelto el Incidente o Service Request	Inmediata	1 Hora
Medio	2 horas	Cada 4 horas hasta ser resuelto el Incidente o Service Request	4 horas	12 Horas
Bajo	8 horas hábiles	Solicitud de pruebas de Servicio y aprobación de cierre de ticket al finalizar actividad	24 horas	36 horas

Fuente: - Información de la Dirección de Tecnología del 24 de Febrero de 2021

- En el contrato de IFX Networks Colombia S.A.S, se tienen establecidos Acuerdos de Niveles de Servicios, entre la Dirección General, sucursales y proveedores mediante el **Anexo 1** del contrato número 007-2020, del proveedor de telecomunicaciones, observando que:

  a. Cuando exista una falla, seguirán los siguientes tiempos de respuestas:

Imagen 23. Tiempos de Respuestas o ANS IFX

CARACTERIZACIÓN DE LA FALLA			TIEMPO MÁXIMO DE ATENCIÓN
PRIORIDAD	EFECTO	DESCRIPCIÓN	
1	Desconexión total	Se entiende que la comunicación entre los 2 puntos de un enlace se ha interrumpido totalmente	2 Horas
2	Operación Degradad	Servicio restringido; servicio por ruta alterna de inferior velocidad; lentitud en el servicio debido a errores en los enlaces, a retransmisiones ó perdidas de paquetes; presencia de fallas presentadas esporádicamente y que pueden causar interrupción en el servicio por periodos de tiempo cortos. El tiempo de duración de las fallas de operación degradada formará parte de la indisponibilidad, siempre y cuando sea medible y mayor a 10 segundos. Latencia por canal.	4Horas
3	Falla moderada	Se entiende como la que no afecta ni degrada la prestación del servicio.	6 Horas

Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

  b. Se deberá presentar por parte del proveedor en el reporte mensual el cálculo del indicador "disponibilidad de cada canal" establecido en el contrato, de igual forma CISA verificará estos resultados ingresando al software de gestión del proveedor y comparará dicha información ejecutando la misma

fórmula con base a los resultados vistos en el software. Se evidenció el informe de gestión del proveedor.

- En el contrato con MICROHARD S.A.S. número 029-2014 donde el proveedor se compromete a entregar a título de arrendamiento equipos de cómputo a CISA y en el cual se establecen los siguientes acuerdos de niveles de servicio:

  a. En caso de presentarse incidentes técnicos en los equipos serán atendidos y solucionados según lo descrito en la siguiente tabla:

Criterio	Tiempo de solución
Incidente Alto	4 horas contadas a partir del reporte
Incidente Medio	24 horas contadas a partir del reporte
Incidente Bajo	44 horas contadas a partir del reporte

  b. Para los nuevos requerimientos deberán ser y solucionados de la siguiente manera:

Criterio	Tiempo de solución
Equipos de escritorio	24 horas contadas a partir del reporte
Equipos portátiles	24 horas contadas a partir del reporte
Tabletas	48 horas contadas a partir del reporte

  Sin embargo, no se identificó seguimiento e informes de gestión de este proveedor por parte de la jefatura de operaciones tecnológicas que permita la verificación del cumplimiento del nivel de calidad y eficiencia de los servicios contratados.

De acuerdo a lo definido en la Circular Normativa N° 044 *"Manual de Contratación"* versión 17 del 30 de diciembre de 2020 y el Memorando Circular N°024 *"Procedimiento de Contratación para las Operaciones Conexas a la Operación mediante Órdenes de Servicio y Contratos"* versión 12 del 30 de diciembre de 2020, los lineamientos relacionados con la contratación y gestión de los proveedores de servicios, y en especial las actividades del supervisor de los contratos; en cumplimiento de esta normatividad, la Dirección de Tecnología realiza sus actividades de evaluación de proveedores soportado en el flujo de Zeus de reevaluación de proveedores, ver siguientes imágenes:

Imagen 24. Radicado Reevaluar Proveedor

Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

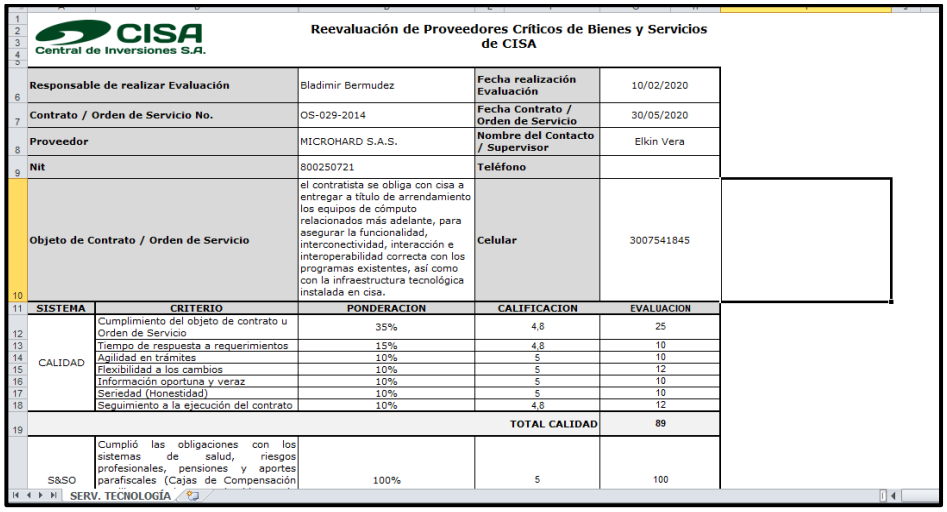
Imagen 25. Radicado Reevaluar Proveedor

Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

Así mismo se revisó el formato de evaluación de los proveedores de los servicios de tecnología para el año 2020 de COLUMBUS NETWORKS DE COLOMBIA LTDA y MICROHARD S.A.S, observando que se han realizado las respectivas evaluaciones y al analizar el formato (imágenes 26 y 27) se observa que no se cuentan con escalas o rangos de los criterios de medición de las variables definidas para calificar el proveedor, al indagar con el jefe de operaciones tecnológicas indicó que da la puntuación de acuerdo al comportamiento y conocimiento que tiene del servicio.

Es importante contar con la definición de acuerdos de niveles de servicio para todos los proveedores de tecnología de información, con el fin de contar con elementos más formales y objetivos de soporte a los procesos de gestión y evaluación.

Imagen 26. Evaluación Proveedor MICROHARD S.A.S



CISA Central de Inversiones S.A.

Reevaluación de Proveedores Críticos de Bienes y Servicios de CISA

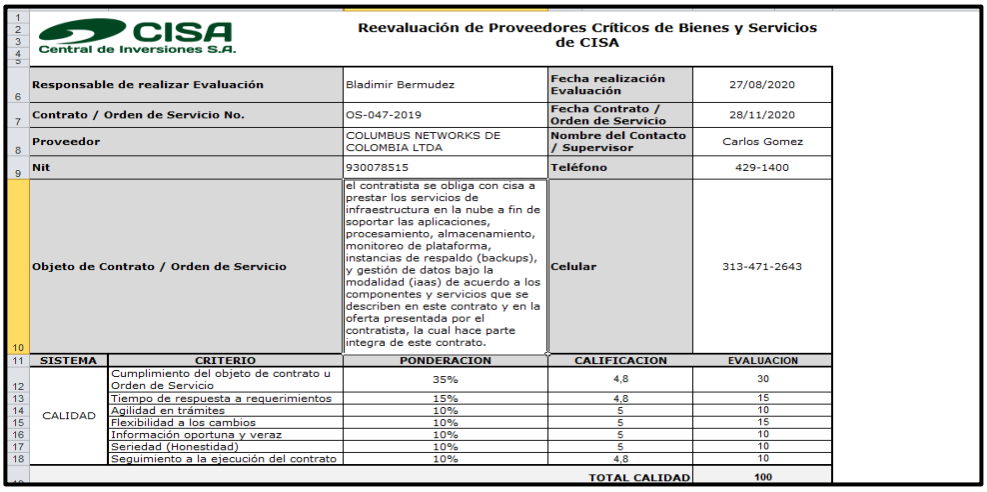
Responsable de realizar Evaluación	Bladimir Bermudez	**Fecha realización Evaluación**	10/02/2020
Contrato / Orden de Servicio No.	OS-029-2014	**Fecha Contrato / Orden de Servicio**	30/05/2020
Proveedor	MICROHARD S.A.S.	**Nombre del Contacto / Supervisor**	Elkin Vera
Nit	800250721	**Teléfono**	
Objeto de Contrato / Orden de Servicio	el contratista se obliga con cisa a entregar a titulo de arrendamiento los equipos de cómputo relacionados más adelante, para asegurar la funcionalidad, interconectividad, interacción e interoperabilidad correcta con los programas existentes, así como con la infraestructura tecnológica instalada en cisa.	**Celular**	3007541845

SISTEMA	CRITERIO	PONDERACION	CALIFICACION	EVALUACION
CALIDAD	Cumplimiento del objeto de contrato u Orden de Servicio	35%	4,8	25
	Tiempo de respuesta a requerimientos	15%	4,8	10
	Agilidad en trámites	10%	5	10
	Flexibilidad a los cambios	10%	5	12
	Información oportuna y veraz	10%	5	10
	Seriedad (Honestidad)	10%	5	10
	Seguimiento a la ejecución del contrato	10%	4,8	12
			TOTAL CALIDAD	**89**
S&SO	Cumplió las obligaciones con los sistemas de salud, riesgos profesionales, pensiones y aportes parafiscales (Cajas de Compensación	100%	5	100

SERV. TECNOLOGÍA

Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

Imagen 27. Evaluación Proveedor COLUMBUS



CISA Central de Inversiones S.A.

Reevaluación de Proveedores Críticos de Bienes y Servicios de CISA

Responsable de realizar Evaluación	Bladimir Bermudez	**Fecha realización Evaluación**	27/08/2020
Contrato / Orden de Servicio No.	OS-047-2019	**Fecha Contrato / Orden de Servicio**	28/11/2020
Proveedor	COLUMBUS NETWORKS DE COLOMBIA LTDA	**Nombre del Contacto / Supervisor**	Carlos Gomez
Nit	930078515	**Teléfono**	429-1400
Objeto de Contrato / Orden de Servicio	el contratista se obliga con cisa a prestar los servicios de infraestructura en la nube a fin de soportar las aplicaciones, procesamiento, almacenamiento, monitoreo de plataforma, instancias de respaldo (backups), y gestión de datos bajo la modalidad (iaas) de acuerdo a los componentes y servicios que se describen en este contrato y en la oferta presentada por el contratista, la cual hace parte integra de este contrato.	**Celular**	313-471-2643

SISTEMA	CRITERIO	PONDERACION	CALIFICACION	EVALUACION
CALIDAD	Cumplimiento del objeto de contrato u Orden de Servicio	35%	4,8	30
	Tiempo de respuesta a requerimientos	15%	4,8	15
	Agilidad en trámites	10%	5	10
	Flexibilidad a los cambios	10%	5	15
	Información oportuna y veraz	10%	5	10
	Seriedad (Honestidad)	10%	5	10
	Seguimiento a la ejecución del contrato	10%	4,8	10
			TOTAL CALIDAD	**100**

Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

4.8 PROCESOS AUTOMÁTICOS EN BATCH O LOTES – JOBS

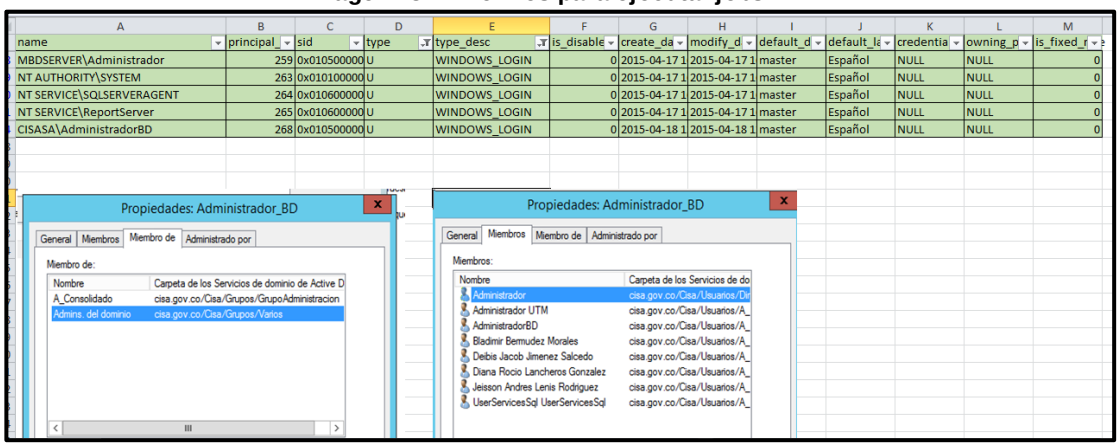
De acuerdo con el marco de referencia de Cobit (Objetivos de control para la información y tecnologías relacionadas) dominio “Entregar y Dar Soporte – Administración de Operaciones” se debe tener un procedimiento y/o instructivo que refleje las actividades críticas en tecnología, que son ejecutadas mediante procesos automáticos (Batch o lotes) o tareas programadas (Jobs), por lo tanto, se revisó la existencia de control sobre estos procesos, identificando que parte del

procesamiento sobre los sistemas de información se efectúan mediante tareas programadas (*System Jobs*), los cuales son monitoreados y configurados a través de la pantalla de control del manejador de base de datos.

Respecto a la información solicitada sobre la gestión de Jobs fue suministrada una lista y documentación de las tareas automáticas y se validó junto con el Jefe de Operaciones Tecnológicas la configuración de estas, no obstante, no se identifica un procedimiento formalizado para describir los controles y actividades que se deben seguir en caso de diseñar, ejecutar, eliminar y monitorear un Job.

Para hacer una evaluación de los usuarios que tienen permisos para ejecutar los Jobs o modificarlos, se solicitó el listado y privilegios de estos, observando, que todos corresponden a los roles establecidos por el Director de Tecnología:

Imagen 28. Perfiles para ejecutar jobs



Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

4.9 MIGRACIÓN DE IPV4 a IPV6

Para la migración de protocolos de IPV4 a IPV6, en el año 2020 se aprobó el presupuesto, no obstante el Director de Tecnología informó que no se ha implementado por los eventos nacionales de salud del año 2020. La fase de diagnóstico fue completada; para lo cual existe un entregable por Innovate Operational Infraestructure SAS (Consultor contratado) y se observa que para el análisis se tomó cada artefacto de TI y fue comparado con la ficha técnica del fabricante para el diagnóstico de viabilidad. Cuentan con la configuración, pruebas que se deben tener en cuenta por parte de la entidad cuando se efectué la fase de implementación y se revelan las siguientes excepciones en el informe del consultor:

- Los Servidores de versiones Windows Server 2003 – Requiere ajustes tecnológicos.
- Algunas impresoras deben ser actualizadas.
- Se requiere coordinar con el proveedor de servicios para la migración a dual stack.
- Estandarizar el uso de FQDN "Fully Qualified Domain Name "donde se puedan tener IPs estáticas, esto permitirá a los sistemas la comunicación optima por resolución de los DNS por IPv4 e IPV6.

De acuerdo al documento "Plan de Diagnostico IPv6v1.pdf" entre las recomendaciones de la consultoría se encuentra: "Revisar el siguiente modelo de transición desde el punto de vista del recurso humano y recurso técnico, a seguir para todo el ciclo de transición hacia IPv6.". El Director de Tecnología informó que se realizó lo sugerido en el "Plan Implementación de IPv6 - Proyecto IPv6 CISA" y en "Plan de Diagnostico IPv6 v1", logrando identificar que el 95% de los artefactos tecnológicos soportan el IPV6; sin embargo, a marzo de 2021 no se ha implementado el proyecto de migración a IPV6.

4.10 PROCEDIMIENTOS DE COPIAS DE RESPALDO DE LA INFORMACIÓN

Para la revisión del cumplimiento de políticas de generación y restauración de backups, el equipo de auditoria se basó en el documento Circular Normativa 093– Política y Procedimiento de Gestión Tecnológica versión 62 del 30 de diciembre de 2020, numeral 5.3 y 5.10; se realizaron reuniones y evaluación de documentos para el entendimiento e identificación de controles en los procedimientos de copias de respaldo de la información.

CISA cuenta con un sistema de replicación al centro de datos alterno localizado en Tocancipá – Cundinamarca, con las siguientes estrategias:

- FullServer – Todo lo que se hace en Producción, Fileserver, Prometeo y Webserver.
- Replica de SQL – Se replica la data de las bases de datos SQL.

Cuentan con un instructivo para la generación y restauración de Backup y el uso de Dataprotector como herramienta para configurar los backups. Se observa que:

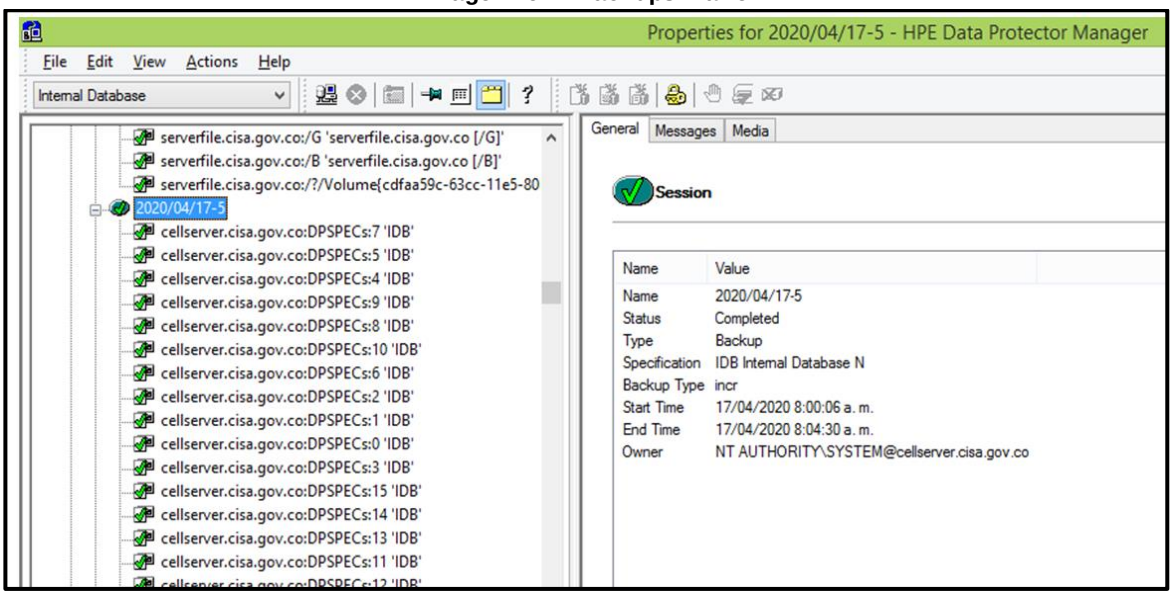
- Diariamente se realiza una copia incremental del fileserver que tiene la carga transaccional más grande.

- Semanal se realiza backup full
- Administra el inventario de cintas

Además se revisó la tabla de retención documental, observando que no se identifican los requerimientos de los dueños de información para salvaguardar la información acorde con la clasificación, criticidad y periodicidad para la generación de copias de respaldo.

Para el análisis de las backups realizados diarios y mensual, se solicitaron 35 ejecutados diariamente en las siguientes fechas del 2020: enero 3, enero 16, febrero 13, febrero 25, marzo 4, marzo 12, marzo 26, abril 7, abril 17, abril 28, mayo 5, mayo 11, mayo 29, junio 10, junio 25, julio 8, julio 22, agosto 13, agosto 27, septiembre 1, septiembre 18, septiembre 28, octubre 8, octubre 21, noviembre 6, noviembre 24, diciembre 2, diciembre 15, diciembre 30. 2021: enero 5, enero 20, enero 29, febrero 8, febrero 16 y febrero 26.

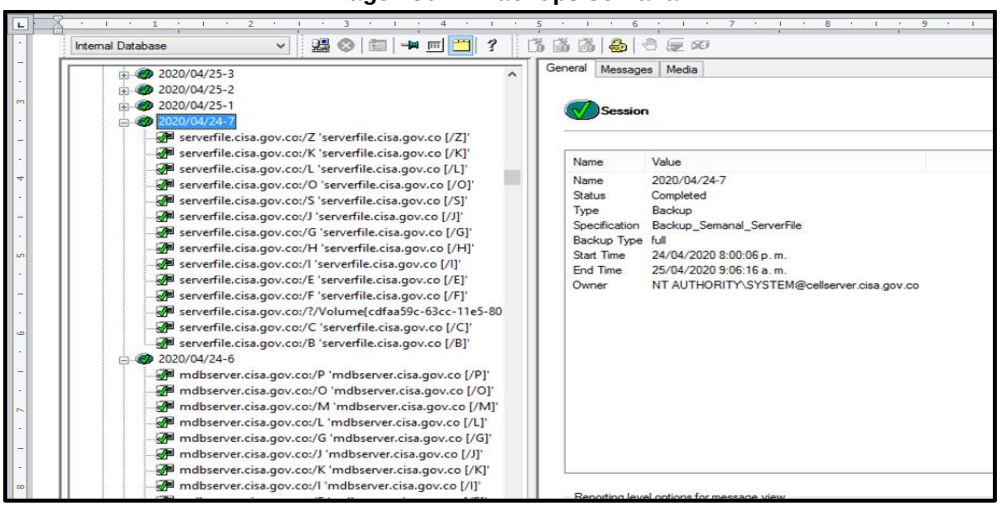
Imagen 29. Backups Diario



Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

Al analizar los 35 logs generados al ejecutarse las copias de respaldo con periodicidad diaria; se evidencia que todos fueron completados satisfactoriamente. Posteriormente, se evaluaron cinco (5) logs de los backups realizados semanalmente: de las siguientes semanas: 24 de abril, 19 de junio, 22 de agosto, 28 de noviembre y 22 de enero de 2021; evidenciando que el resultado fue satisfactorio para las copias seleccionadas. Como se evidencia en la siguiente imagen.

Imagen 30. Backups semanal



Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

Adicionalmente, se revisó el inventario de medios magnéticos entregado, observando que se cuenta con 3719 cintas de copias de respaldo con información desde septiembre de 2005 en el custodio externo hasta el 30 de septiembre de 2020.

Se analizó el informe del plan de pruebas de restauración, con un periodo evaluado desde febrero a diciembre de 2020; basado en la información del archivo "InformeGeneralPlandeRestauracion.xls", identificando que se cumple con este plan y que en la herramienta Novasec se registran las pruebas de integridad y calidad ejecutadas por parte del Operador que las ejecuta y posteriormente son revisadas por la Oficial de Seguridad.

4.11 CONTROL DE LICENCIAMIENTO DE SOFTWARE

Con base en el documento Circular Normativa 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, numeral 5.8.1 se identificó que la entidad cuenta con una política de Gestión de Activos de Información en su aparte 5.8.1. "Responsabilidad por los activos de información" de la "circular normativa 093 versión 62", se refiere al uso de software donde se menciona que *este "debe ser legalmente adquirido o licenciado mediante distribuidores autorizados a empresas o compañías que lo provean, también se menciona que en caso de necesitarse software diferente al autorizado o de uso libre, se debe tener autorización de la Oficial de Seguridad de la Información*". Sin embargo, no se identificó un procedimiento formal que rijan las actividades de monitoreo de software instalado en los equipos.

En el documento suministrado por la Jefatura de Operaciones Tecnológicas denominado *"Matriz_Software.xlsx"* se identifica el software aplicativo, de ofimática y utilitarios que utiliza la entidad y cual es autorizado por la Oficial de Seguridad por ser de uso gratuito.

Como control de instalación de software para los usuarios finales se cuenta con la restricción de acceso desde el directorio activo, esto para que solo le permita instalar software al usuario que tenga asignado perfil de administrador.

También se cuenta con la herramienta Spiceworks que permite efectuar una validación del software de los equipos conectados a la red; en el reporte entregado del 15 de febrero de 2021 denominado "*report-applications_by_computer_2021_02_15.xls*" se identifica que el análisis se efectuó sobre 106 equipos de la entidad, situación que se ha presentado debido a la implementación del esquema de trabajo en casa por la pandemia, lo que ha conllevado a que no todos los equipos se encuentran conectados como parte de la red LAN, además que existen usuarios que se soportan en sus equipos personales para el trabajo de oficina, presentado desde el 2020 por la pandemia, estos tampoco serían objeto de verificación de la herramienta Spiceworks. Estas situaciones hacen que no se efectué una monitoreo completo y efectivo sobre el software instalado en los equipos, además de que se generan brechas de seguridad informática sobre la red de la Entidad al no identificar y contener conexiones de "end-points" vulnerables no corporativos (computadores portátiles, teléfonos inteligentes, tabletas, entre otros), que pueden tener sistemas desactualizados, no contar con soluciones antivirus e incluso podrían estar infectados con malware.

Respecto a lo anterior la Dirección de Tecnología mencionó que se encuentra en el proceso de adquisición de nuevos equipos para asignarlos al personal que no cuenta con este recurso corporativo y con la implementación del proyecto de la red extendida para dar cobertura a todas las conexiones válidas de la red de CISA.

4.12 PLAN DE CONTINUIDAD DEL NEGOCIO (BCP – DRP)

La Entidad cuenta con el Manual de Continuidad del Negocio versión 6 – MN022 del 23 de diciembre de 2020, el cual fue estructurado en el año 2019 y basado en la norma ISO22301 gestión de continuidad del negocio, en revisión de este documento y en entrevista con la Oficial de Continuidad se estableció que el plan de continuidad de la Entidad cuenta con los elementos y estrategias requeridos para soportar la

operación en los eventos y escenarios allí identificados, a continuación se presentan los más relevantes para este tipo de planes:

4.12.1 Política de continuidad del negocio

En el Manual de Continuidad del Negocio versión 6 – MN022 del 23 de diciembre de 2020, entregado al equipo de auditoría, - numeral 4 se declara como política "*garantizar la generación de valor en la gestión de activos para las entidades del Estado, en las diferentes zonas de CISA, cuando se produce un evento de interrupción".*

4.12.2 Análisis del impacto al Negocio – BIA

La Entidad efectuó un análisis de impacto al negocio a los procesos críticos soportado en el MN022 Anexo 1 V3 "Análisis de Impacto al Negocio – BIA", estableciendo seis (6) procesos críticos:

- Proceso de servicio integral al ciudadano
- Proceso de gestión de activos (cartera)
- Proceso de gestión de activos (inmuebles)
- Proceso gestión jurídica del negocio
- Procesos de gestión tecnológica
- Proceso financiero y Contable

Así mismo en el BIA, CISA establece las prioridades y tiempo de recuperación de dichos procesos, definiendo que el RTO (Tiempo objetivo de recuperación) en los periodos más críticos es de 24 horas, tiempo prudencial dada la naturaleza del negocio para priorizar las estrategias a seguir en caso de activarse la contingencia.

4.12.3 Identificación y selección de estrategias BCP y DRP

Con base en el documento Circular Normativa 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, numeral 5.16 y en el MN022 V6 numeral 7, se revisó que CISA estableció unas estrategias de recuperación ante interrupciones como se observa a continuación:

Imagen 31. Estrategias de recuperación de TI

A continuación, se presentan las estrategias de recuperación definidas como mecanismo de respuesta, frente a la materialización de cualquier evento de interrupción que pueda conllevar a la indisponibilidad de la operación de CISA:

Indisponibilidad de la infraestructura física	Indisponibilidad de los colaboradores	Indisponibilidad de proveedores y/o terceros	Indisponibilidad de la Tecnología
• Trabajo en casa • Acuerdo con Proveedores • Respaldo entre Zonas	• Personal alterno formalmente definido del mismo proceso • Personal alterno formalmente definido de otro proceso • Capacitación/ Entrenamiento y Gestión del conocimiento	• Acuerdos de nivel de servicio en aspectos de Continuidad de Negocio • Desarrollo de pruebas de continuidad conjuntas con los proveedores críticos	• Estrategia de Recuperación ante Desastres (DRP) – DraaS • Operación de Actividades Manuales

Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

CISA apoyado en el análisis del BIA ha definido las estrategias de recuperación para suplir el riesgo tecnológico denominado "Interrupción de la operación de los procesos críticos", el cual tiene impacto moderado y la probabilidad de ocurrencia es "rara vez", reflejando que los procesos de CISA están conformados para no ser impactados gravemente y que con los antecedentes y la infraestructura actual la operación es estable.

Respecto al DRP, la entidad cuenta con un servicio contratado con COLUMBUS Networks Colombia Ltda. para la recuperación de desastres con disponibilidad 7x24x365, lo que permite contar con respaldo para aplicar los planes de continuidad cuando se genere algún incidente que interrumpa las operaciones basadas en tecnología de la información. El Servicio contratado de DRP, se encuentra configurado con las características descritas por el área de tecnología, basadas en la Circular Normativa 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, numeral 5.16 y en el MN022 Anexo 9 V4, numeral 3.4 "Estrategia de Recuperación de Ante Desastres – DRP" para la seguridad y operatividad, contando así con un firewall y un VPN applying, el control de la navegación a internet recae sobre el cliente.

De acuerdo con lo analizado, el DRP está compuesto por cinco máquinas, contratado con el proveedor COLUMBUS, servicio que incluye el espacio para las máquinas en la nube, herramienta de replicación, configuración y administración de los servicios

que están replicados con el servidor de base de datos, fileserver, servidor de aplicaciones Prometeo, servidor Webserver y un servicio secundario que controla los perfiles de acceso a la información en contingencias. Es un sistema configurado de forma Activo-Pasivo para el trabajo de réplica y se conecta con un mecanismo de transporte de datos estándar (MPLS).

Cada usuario tendría una VPN para tener a acceso a los servicios en el esquema de operación en contingencia para que puedan ingresar a los sistemas críticos establecidos por la Compañía, como son los procesos misionales, la página web y fileserver.

Los planes de continuidad del negocio (BCP) definen acciones y tareas propias de los procesos de CISA para actuar durante y después de alguna situación de contingencia, esto se encuentra documentado en los anexos del MN022 V6, con guías de acción para Presidente - MN022 Anexo 46 V3, Vicepresidente Jurídico- MN022 Anexo 48 V4, Director de Tecnología y Sistemas de Información - MN022 Anexo 51 V3, entre otros, identificando el personal clave en cada una de estos procesos, revelando que tienen un diseño organizado donde se incluyen los interesados y define las acciones a seguir por los mismos.

4.12.4 Plan de pruebas del BCP y DRP

Con base en el documento Circular Normativa 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, numeral 5.16 y en el anexo 56 denominado “Programa de ejercicios y/o pruebas del Manual de Continuidad del negocio” del manual de continuidad del negocio (manual 22), donde se establecen las actividades que se deben realizar para mantener actualizados planes BCP y DRP y las pruebas que se debían ejecutar en el año 2020.

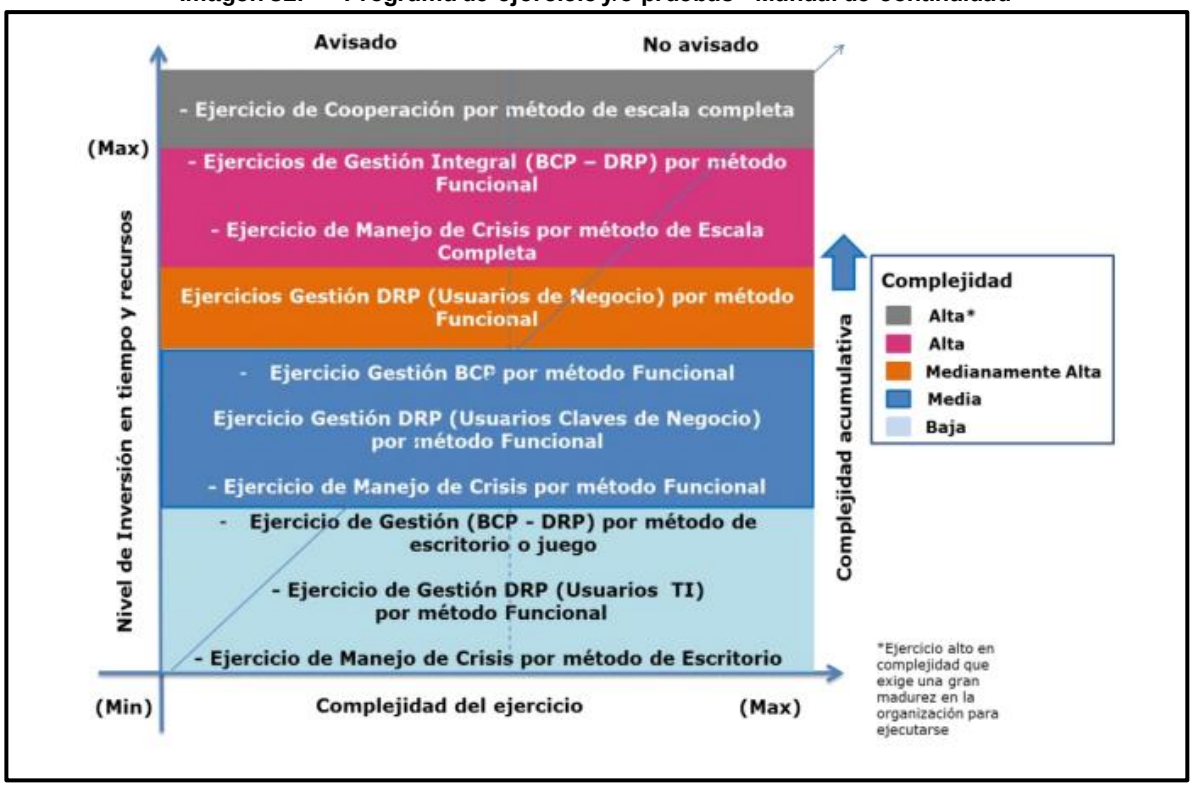
Se solicitó el soporte del Ejercicio de Escritorio – Planes de Continuidad BCP´s, planeado para el año 2020, en el cual se consideraban escenarios de indisponibilidad de servicios de tecnología; sin embargo, se identificó que las actividades de pruebas planeadas no fueron realizadas en su totalidad para llegar a simular una situación de contingencia real y activar el DRP, debido a la crisis sanitaria presentada.

El escenario actual de Pandemia no ha requerido activar el DRP pero si se ha requerido el esquema de trabajo en casa que inicialmente se contemplaba como una

estrategia de continuidad, esta nueva forma de trabajo se debe considerar en los ejercicios de pruebas a estos planes.

De acuerdo a la metodología estándar ISO /FDIS 22398, la analista de procesos y continuidad del negocio ejecutó el método de escritorio o juego de pruebas con complejidad baja.

Imagen 32. "Programa de ejercicio y/o pruebas" Manual de continuidad



Fuente: Información de la Dirección de Tecnología del 24 de Febrero de 2021

La ausencia de pruebas de continuidad y recuperación de desastres puede ocasionar interrupciones en los procesos y operación de negocio ante la debida preparación y alistamiento de información, componentes tecnológicos y recursos necesarios para actuar ante un evento de anormalidad en las operaciones de los procesos o infraestructura tecnológica.

4.12.5 Incidente Sucursal Zona Andina

Como proceso adicional a lo establecido en el alcance de la auditoría y dada las circunstancias presentadas durante el período de desarrollo de esta, el 28 de abril de 2021 se presentó un acto vandálico atacando la infraestructura física y robo de equipos de cómputo en la sede Andina de CISA en la ciudad de Medellín.

Con el fin de establecer los protocolos activados por la Entidad para reaccionar a dichos eventos, el equipo auditor efectuó una reunión con el Director de Tecnología, la Oficial de Seguridad y la Analista de Procesos y Continuidad quienes estuvieron a cargo de realizar los respectivos análisis y valoraciones de los eventos presentados en la oficina, se activó el comité de crisis y se declaró el evento como un incidente.
Se identificó que la Entidad actuó acorde con lo establecido en el procedimiento de gestión de incidentes, referenciado en el Manual de Continuidad del negocio (022), anexo 10 denominado "Plan de Manejo del Incidente – Oficial de Continuidad", para lo cual se llevaron a cabo las siguientes actividades:

- Inspeccionar el lugar para identificar daños físicos.
- Contactar el proveedor de MICROHARD S.A.S., responsable de entregar a título de arrendamiento equipos de cómputo para efectos de reemplazar los equipos hurtados y dañados.
- Verificar la conectividad a la red.
- Verificar conexiones remotas.
- Bloquear rack de comunicaciones para evitar conexiones físicas no autorizadas en la sede.

No fue necesario activar el DRP ya que no se presentaron eventos que superaran el RTO (Tiempo objetivo de recuperación) de 24 horas, período establecido de recuperación para los procesos críticos. Actualmente se están realizando entrevistas a los usuarios afectados, con el fin de establecer el nivel de riesgo por la pérdida de información tanto física como digital y/o acceso no autorizado a información confidencial.
Se sugiere dar continuidad y priorización a la culminación del análisis del incidente con el propósito de cumplir los lineamientos establecidos para gestionar dicho evento, implementando oportunamente las acciones correctivas, lecciones aprendidas y actualizaciones que deban ser incorporadas en el Manual de Continuidad, asegurando las respectivas capacitaciones a todos los interesados.

5. HALLAZGOS

5.1. Centro de acceso físico y ambiental del Centro de Cómputo

Evaluada en el plan de mejoramiento la "implementación de control (1. Techo ignifugo, 2. Sistema de extinción de incendios)" y basados en la Circular Normativa N° 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, numeral 5.2., se observó que no se ha implementado, no obstante, se ha definido un proyecto para la construcción de un nuevo centro de

cómputo y se observa que al 30 de abril del 2021 no se ha iniciado su construcción, persistiendo aún los riesgos identificados en la auditoría del 2017 relacionados con la implementación de controles ambientales del Centro de Cómputo.

Las debilidades en la instalación física del centro de cómputo como:

a. Puerta de madera al ingreso inicial del centro de Datos
b. Localización en el último piso (3er) de la sede principal.
c. El cableado de fibras redundantes en el primer piso está próximo a una ventana que da al exterior de las oficinas, con flujo peatonal sin control.
d. Algunos cables cuentan con marquillas de identificación para facilitar su mantenimiento y adecuado.
e. Las llaves para el ingreso al centro de cómputo no cuentan con una marcación, lo que dificulta en un momento de emergencia identificar la llave de apertura.

Estas debilidades pueden generar afectación en los servicios de tecnología, incidentes de seguridad en los recursos técnicos, humanos y/o afectaciones en las operaciones que soporta los procesos de negocio de la Entidad.

5.2. Gestión de la Capacidad y Desempeño

Evaluada la gestión y monitoreo de los recursos tecnológicos con base en la Circular Normativa N° 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, numeral 5.14, se evidenció que no se cuenta con un plan formal que contenga el análisis de capacidad en la infraestructura tecnológica de CISA, que incluya los procesos, tecnologías y personas necesarias para el correcto funcionamiento de los servicios de TI de la entidad a mediano y largo plazo en cuanto a desempeño, disponibilidad y optimización de la utilización de recursos que soportan la plataforma tecnológica. Actualmente el área de Gestión Tecnológica se encuentra construyendo este plan.

5.3. Gestión de Acuerdos de Niveles de Servicio – ANS

Evaluado los acuerdos de niveles de servicios relacionados en el anexo 6 “Instructivo para la Gestión de Nivel de Servicios” y de conformidad con la Circular Normativa N°093 versión 63, numeral 5.11 “*Políticas de Gestión de Acuerdos de Servicios*”, se evidenció que:

a. Si bien se cuenta con acuerdos de niveles de servicio para el soporte de aplicativos institucionales, no se identifican este tipo de acuerdos para los demás servicios que presta tecnología a los diferentes procesos de negocio.

b. En el contrato de COLUMBUS Networks Colombia Ltda, se tienen establecidos Acuerdos de Niveles de Servicios mediante el Anexo 1 del contrato N° 030-2019 para la prestación de los servicios infraestructura virtual e implementar un esquema de recuperación de desastres – DRP, se definen acuerdos medidos por Disponibilidad del servicio e Indisponibilidad, no obstante en el contrato no se establece una periodicidad de entrega de reportes a la Entidad con las variables de medición, que permitan reflejar la gestión de los servicios contratados, esto dificulta monitorear oportunamente la calidad y cumplimiento de los servicios de TI.

c. Para el contrato del proveedor MICROHARD S.A.S. no se identificó seguimiento e informes de gestión de este proveedor por parte de la Jefatura de Operaciones Tecnológicas que permita la verificación del cumplimiento del nivel de calidad y eficiencia de los servicios contratados.

d. En el formato de "Reevaluación de proveedores Críticos de Bienes y Servicios de CISA" no se cuentan con escalas o rangos definidos por cada uno de los criterios para la medición de variables de calificación para el proveedor, al indagar con el jefe de operaciones tecnológicas indicó que da la puntuación de acuerdo al comportamiento del servicio.

5.4. Procedimientos de copias de respaldo de la información

Evaluado el cumplimiento de políticas de generación y restauración de backups, el equipo de auditoria se basó en el documento Circular Normativa N° 093– Política y Procedimiento de Gestión Tecnológica versión 62 del 30 de diciembre de 2020, numeral 5.3 y 5.10, evidenciando que:

a. Evaluada la frecuencia del envío de la cinta a custodia externa de las copias de respaldo, se observó que la fecha registrada en el campo "Registro de Entrada" del "Formato Único de Inventario Documental" no tiene una relación cronológica con las fechas registradas en el campo "Fechas Extremas" que corresponden al periodo inicial y final del backup efectuado. Esto se evidencia en cinco (5) de los nueve (9) periodos solicitados, donde se incluyen formatos de los años 2020 y

2021 donde la fecha de envío de la cinta corresponde hasta cuatro (4) meses después de realizado el backup, el cual debería corresponder a un lapso de periodo cercano a la fecha final registrada. Es de aclarar que en reunión con la Dirección de Tecnología se mencionó que por situación de pandemia se presentaron estos casos.

b. Otra situación que se presenta es que son enviadas al custodio externo al completar las 15 Terabytes que tiene cada cinta de almacenamiento.

c. En cuanto al diligenciamiento del formato se observa que no tienen la firma del responsable de entrega, ni del receptor.

5.5. Control de licenciamiento del software

Evaluado el cumplimiento del uso de software relacionado con la política de Gestión de Activos de Información en su aparte 5.8.1. "Responsabilidad por los activos de información" de la "circular normativa 093 versión 62", del 30 de diciembre de 2020, se evidenció que:

a. Una vez verificados los controles del control de instalación de software, no se identificó un procedimiento formal que rijan las actividades de monitoreo de software instalado en los equipos.

b. Si bien se cuenta con la herramienta Spiceworks que permite efectuar una validación del software de los equipos conectados a la red; se está presentando que en las revisiones no se efectué un monitoreo completo y efectivo sobre el software instalado en los equipos por el esquema de trabajo en casa en donde no todos los equipos se encuentran conectados como parte de la red LAN, además que existen usuarios que se soportan en sus equipos personales para el trabajo de oficina, generando brechas de seguridad informática sobre la red de la Entidad al no identificar y contener conexiones de "end-points" vulnerables no corporativos (computadores portátiles, teléfonos inteligentes, tabletas, entre otros), que pueden tener sistemas desactualizados, no contar con soluciones antivirus e incluso podrían estar infectados con malware.

5.6. Plan de continuidad del negocio

Evaluado el plan de pruebas del BCP y DRP relacionado con el anexo 56, denominado "Programa de ejercicios y/o pruebas del Manual de Continuidad del negocio" del manual de continuidad del negocio (manual 22) y con base en el documento Circular Normativa 093 Política y Procedimiento de Gestión Tecnológica – versión 62 del 30 de diciembre de 2020, numeral 5.16, se solicitó el soporte del Ejercicio de Escritorio – Planes de Continuidad BCP´s, planeado para el año 2020, en el cual se consideraban escenarios de indisponibilidad de servicios de tecnología, se identificó que este no activó el DRP con un entorno real, debido a la crisis sanitaria presentada.

La ausencia de pruebas de continuidad y recuperación de desastres puede ocasionar interrupciones en los procesos y operación de negocio ante la debida preparación y alistamiento de información, componentes tecnológicos y recursos necesarios para actuar ante un evento de anormalidad en las operaciones de los procesos o infraestructura tecnológica.

6. OBSERVACIONES

6.1. Gestión de riesgos de tecnología

Evaluado el mapa de riesgos, se observó que no se está reflejando un análisis detallado respecto a los elementos definidos en la caracterización de los procesos de Operaciones Tecnológicas asociadas a las actividades de gestión de capacidad y desempeño, atención de mesa de ayuda, gestión de copias de respaldo de la información, entre otros. Aunque la Dirección de Tecnología ha avanzado en la declaración de riesgos, análisis, valoración del riesgo y controles para el subproceso de construcción de software en sus diferentes etapas, es importante tener en cuenta la identificación y alcance de los servicios que se incluirán en su portafolio el subproceso de Operaciones Tecnológicas.

6.2. Evaluación de indicadores

- Evaluado los indicadores "Soporte solucionados en el tiempo" y "Disponibilidad del servicio"; se observó que los valores aún no han sido actualizados al 14 de abril para la medición del mes de marzo de 2021 en la herramienta Isolucion, se sugiere reportar el estado de los indicadores en el sistema ISOLUCIÓN en los

primeros diez días de cada mes, con el fin de dar cumplimiento a lo establecido por la entidad respecto a la gestión de indicadores.

- Analizando el indicador de "Disponibilidad del Servicio" se observó que la formulación mezcla los tiempos de los servicios, ejemplo: Para el indicador de "Disponibilidad del servicio"; este cálculo (HNDM x CSND)) estaría inexacto, porque si tuve 2 horas sin correo y 3 horas sin una aplicación, siguiendo la formula diría 2 y 3 son 5 horas x 2 servicios y CISA no estuvo 10 horas por fuera, por esto, no se deben mezclar porque puede generar la sobreestimación en el cálculo del indicador presentando niveles de disponibilidad no reales, por lo tanto se sugiere revisar y ajustar el diseño de la fórmula del indicador "Disponibilidad del servicio" de tal forma que se mida realmente el tiempo que se presente como no disponibilidad y también se debe considerar la definición de los límites inferiores y superiores para contar con un umbral claramente definido.

- En el cálculo del indicador "Soporte solucionados en el tiempo", basado en la fórmula: (No. de soportes atendidos en el tiempo (Zeus) / No. de soportes reportados) * 100, identificamos que éste incluye los casos que fueron solucionados en el mes anterior y el usuario no los ha cerrado. Aspecto que puede generar inconsistencias en el cálculo del indicador y/o inadecuada medición en el monitoreo y gestión de los servicios de soporte de TI, así que se sugiere considerar en el cálculo del indicador que la variable *No. de soportes atendidos en el tiempo (Zeus)* solo debe incluir los casos que se hayan gestionado en el periodo evaluado.

6.3. Gestión de la Capacidad y Desempeño

No se identifica trazabilidad de las acciones preventivas que se toman ante las alertas arrojadas en los sensores configurados con alertas amarillas, esto puede generar demoras en la atención y respuesta a incidentes e interrupciones del servicio originadas por falta de capacidad o degradaciones del desempeño, por lo tanto sugerimos considerar en el procedimiento de gestión de monitoreo capacidad la documentación de los análisis y acciones que se toman producto de las mediciones de alertas preventivas, con el fin de establecer el adecuado cumplimiento y gestión de los sensores en la herramienta PTRG.

6.4. Mesa de Ayuda y Gestión de Incidentes

No se identificó un procedimiento formalmente establecido para la gestión de incidentes y problemas que permita el aseguramiento en la atención y resolución de eventos que afecten la funcionalidad y operación en la infraestructura y servicios de TI.
El área de Operación de Tecnología cuenta con personal técnico para atender las situaciones presentadas; sin embargo, no está estructurado como un servicio de la mesa de ayuda para la atención y resolución de incidentes y problemas que sean registrados, analizados, diagnosticados y escalados para su resolución de acuerdo con la clasificación de niveles de atención (1er, 2do y 3er nivel).
No se tienen definidos indicadores que permitan medir la gestión de incidentes y problemas.

6.5. Procesos automáticos en Bath o lotes – Jobs

No se identifica un procedimiento formalizado para describir los controles y actividades que se deben seguir en caso de diseñar, ejecutar, eliminar y monitorear un Job, generando la posibilidad de una eventual falla en las operaciones por posible error humano en la modificación de las instrucciones configuradas en una tarea programada.

6.6. Migración de IPV 4 a IPV 6

Para la migración de protocolos de IPV4 a IPV6, en el año 2020 se aprobó el presupuesto, pero no se pudo ejecutar el proyecto por la situación de pandemia de acuerdo a lo mencionado por el Director de Tecnología; sin embargo, la fase de diagnóstico fue completada para lo cual existe un entregable por el Consultor contratado, donde se establece que el 95% de los artefactos tecnológicos soportan el IPV6 pero a marzo de 2021 no se ha implementado este proyecto.

7. RECOMENDACIONES[1]

7.1. Centro de acceso físico y ambiental del Centro de Cómputo

Una vez construido y puesto en marcha el nuevo centro de cómputo se sugiere actualizar y complementar la política establecida para la administración y gestión del centro de cómputo, considerando aspectos como:

a. Procedimientos para otorgar, revocar y limitar el acceso a la instalación. Considerando todo el personal autorizado que acceda a dicho lugar, como funcionarios, clientes, proveedores, visitantes o cualquier tercera persona.

b. Capacitar al personal del área de Gestión Tecnológica en el uso de extintores con simulacros de incendio y rescate para asegurar el conocimiento y las acciones que se deben tomar en caso de incendio o incidentes en el centro de cómputo.

c. Definir responsabilidades sobre el monitoreo, procedimientos de reporte y de resolución de incidentes de seguridad física.

d. Separar las llaves de acceso al centro de cómputo y etiquetarlas para facilitar su utilización.

e. Aseguramiento de la implementación de controles ambientales y físicos como:

- Sistemas de prevención, detección y extinción de incendios. (Sistema de ingeniería que permite la extinción del fuego incipiente durante los primeros minutos de su generación, de manera automática a fin de salvaguardar personas, bienes e inmuebles).
- Vigencia de Extintores.
- Sistema de ventilación / Aire Acondicionado.
- Control de temperatura y humedad.
- Marquillas de cableado.

f. Evaluar los riesgos a los que se podrá ver expuesto el nuevo centro de cómputo, que permita prever la administración y gestión de riesgos.

[1] Se incluye este texto como última recomendación en el informe definitivo

g. Realizar un análisis de factores de riesgos para centro de cableado en los pisos 1 y 2 restringiendo el flujo peatonal.

h. Obtener las certificaciones pertinentes respecto al cableado de datos y eléctrico.

7.2. Gestión de la Capacidad y Desempeño

El área de Gestión Tecnológica actualmente se encuentra diseñando el plan de capacidad y desempeño de TI y adelantando el proyecto de migración de documentación histórica digital para conservar esta información en un repositorio dedicado a esta función que se denomina *historico.cisa.gov.co.,* es importante considerar que estos deben estar alineados con el plan estratégico de Tecnología de Información.

Es importante documentar el análisis de capacidad tecnológica de los activos críticos con el fin de proyectar la atención de los requerimientos y necesidades futuras como: recursos tecnológicos, cargas de trabajo, almacenamiento y contingencias, con el fin de garantizar la disponibilidad de manera continua en la infraestructura tecnológica que soporta el negocio.
El análisis de la Gestión de la Capacidad debe estar soportado en modelos y simulaciones de diferentes escenarios de capacidad, monitoreo del uso y rendimiento de la infraestructura de TI y la gestión de la demanda.
Es importante diseñar indicadores que faciliten la medición de la gestión de capacidad, tales como:

- El uso de recursos.
- Desviaciones de la capacidad real sobre la planificada.
- Análisis de tendencias en el uso de la capacidad.
- Análisis de la capacidad y monitorización del rendimiento.
- Impacto en la calidad del servicio, disponibilidad y otros procesos TI.
- Porcentaje de picos donde excede la meta de utilización.
- Análisis de alertas preventivas y correctivas

El procedimiento de gestión de monitoreo capacidad debe permitir identificar los análisis y acciones que se toman producto de las mediciones de alertas preventivas y correctivas, con el fin de establecer el adecuado cumplimiento y gestión del plan.

Un plan de capacidad facilita la asignación presupuestal para inversiones en recursos tecnológicos y la atención oportuna de requerimientos tecnológicos necesarios para soportar los procesos de negocio.

7.3. Mesa de Ayuda y Gestión de Incidentes

Se sugiere fortalecer la estructura actual de la mesa de ayuda, considerando el modelo de operación que se encuentra diseñando la Dirección de Tecnología, cuyo enfoque está alineado con un esquema ITMS (Administración de servicios de Tecnología de Información), que permita evaluar el impacto de TI en los diferentes procesos de negocio.

El portafolio de los servicios ofrecidos por tecnología, deben ser administrados gestionados y monitoreados mediante un proceso consolidado de mesa de servicio que asegure la administración de activos, problemas e incidentes.
Este modelo debe estar soportado con una herramienta tecnológica robusta que permita la configuración, clasificación y medición de los servicios que deben ser administrados.

La implementación del modelo ITSM debe contar con la definición roles, responsabilidades y Acuerdos de Niveles de Servicio, del equipo de funcionarios que deberá atender los incidentes, requerimientos de usuarios y solicitudes de información de los usuarios de tecnología.

La documentación de un procedimiento de gestión de incidentes fortalece el flujo de las actividades e implementación de controles para el escalamiento de los niveles de atención de acuerdo con la criticidad o complejidad del evento.

El diseño y medición de indicadores contribuye a la mejora continua del proceso, es importante establecer en el modelo de operación indicadores que permitan el monitoreo de la resolución, cierre y análisis de tendencias de incidentes. Por ejemplo: Cantidad de incidentes repetidos, Cantidad de escalados, Tiempo de resolución del incidente, Esfuerzo de resolución del incidente, entre otros.

7.4. Gestión de Acuerdos de Niveles de Servicio – ANS

- Documentar y formalizar los acuerdos de niveles de servicio (ANS) para cada uno de los servicios prestados por el proceso de Gestión tecnológica en los procesos de negocio.

- Definir de manera contractual con el proveedor COLUMBUS Networks Colombia Ltda, la entrega periódica de los informes de gestión del servicio prestado y para el proveedor MICROHARD S.A.S. la formalización de informes de gestión de los acuerdos de niveles de servicio establecidos, con el fin de mantener un monitoreo objetivo basado en indicadores y fortalecer la adecuada gestión de proveedores de tecnología.

- Junto con el área de Mejoramiento continuo definir escalas o rangos definidos por cada uno de los criterios para la medición de variables de calificación cuando es necesario reevaluar un proveedor crítico, de tal manera que no se llegue a incurrir en la subjetividad de una calificación.

7.5. Procesos automáticos en Bath o lotes – Jobs

Con el propósito de mejorar la administración de las operaciones en la ejecución de procesos automáticos en batch o en lotes, se sugiere definir un procedimiento que incluya, entre otras actividades o controles:

- Que se identifique la periodicidad para la ejecución de las interfaces y/o *Jobs*
- Un cronograma de ejecución que involucre los responsables de la ejecución, hora de inicio, hora de finalización, insumo (pueden ser datos de entrada o salidas de otros procesos), salida, estado de finalización y número de reprocesos.
- Existan totales de control y/o listados de excepción que permitan identificar el número de registros cargados o no cargados y si aplica, el valor de la suma de los registros.
- Existan procedimientos de depuración y análisis de los listados de excepción.

7.6. Migración de IPV4 a IPV6

Se recomienda dar continuidad a la fase de implementación de la migración a IPV6, con el fin de cumplir lo dispuesto por el MINTIC. Se sugiere incluir los cambios en la

infraestructura tecnológica que se hayan efectuado desde la fecha de la elaboración del plan de la fase implementación, de tal forma que se pueda medir el impacto y posibles nuevas consideraciones a tener en cuenta.

7.7. Procedimientos de copias de respaldo de la información

- Dar cumplimiento al envío de copias externas al custodio en periodo que define el actual procedimiento o considerar un análisis de riesgo donde se pueda efectuar una variación al periodo que se envía al sitio externo que permita el ajuste del procedimiento. Así como establecer una firma digital o física que garantice quien entrega y receptor de las cintas enviadas a custodia.

- Capacitar a los interesados sobre el uso del "formato único de inventario documental – fuid" y los cambios a realizar en el "Procedimiento generación y restauración de backups".

7.8. Control de licenciamiento de software

- Establecer un procedimiento formal que asegure la implementación de actividades de control para el monitoreo del software autorizado que debe estar instalado en los equipos de la entidad, que contemple la periodicidad de la ejecución de la herramienta, soporte del análisis efectuado respecto a la línea base de software, protocolo de desinstalación (si es necesario), con el fin de dar cumplimiento de la ley 603 de derechos de autor.

- Dar continuidad al proceso de adquisición de nuevos equipos para asignarlos al personal que no cuenta con este recurso corporativo y con la implementación del proyecto de la red extendida para dar cobertura a todas las conexiones válidas de la red de CISA y reforzar con la implementación de controles de protección de punto final que permitan generar alertas y tratar las amenazas identificadas en las conexiones remotas de equipos no corporativos, cuando no se cumplan las políticas del servidor, de antivirus y antispyware.

- Se sugiere complementar las prácticas de monitoreo periódico para verificar que todas las defensas están activas y actualizadas en todos los sistemas administrados.

7.9. Plan de continuidad del negocio

Efectuar una revisión al plan establecido en los ejercicios de escritorios – planes de continuidad BCP´s diseñados en el año 2020, ajustándolo al nuevo normal que ha conllevado la pandemia, de tal forma que se identifiquen la totalidad de escenarios, infraestructura, medidas de control, análisis de riesgos como ciberataques, pérdida de funcionarios ante un evento desafortunado de muerte, que puede afectar el conocimiento o prestación de servicio definido actualmente para declarar un plan de continuidad de negocio o activar un DRP.

Es importante considerar que en la medida que se avance en las pruebas de continuidad se deben establecer planes de acción que les permitan cerrar las brechas presentadas en los ejercicios, de tal forma que a mediano plazo puedan escalar el nivel de madurez de complejidad del ejercicio hasta llegar al nivel Alto y Alto* para asegurar que la Entidad está preparada para reaccionar en una eventualidad por método de gestión integral o de cooperación por método de escala completa.

8. CONCLUSIÓN DE AUDITORÍA

Los procesos de soporte de la infraestructura de tecnología de la información de CISA se realizan con un enfoque hacia la operación y resolución de situaciones que puedan afectar la operación de tal forma que han mantenido el funcionamiento de dicha infraestructura, no obstante, es importante que se evolucione a un nivel de madurez orientado a un modelo de prestación de servicios de tecnología basado en buenas prácticas de gestión de TI, herramientas de apoyo y definición de esquemas de monitoreo continuo.

La entidad realiza la gestión integral de continuidad de negocio en la operación de los procesos críticos, el cual se alinea con el DRP – plan de recuperación de desastres y se describen los procesos y procedimientos que indican las actividades que deben seguir los funcionarios que realizan la recuperación tecnológica en un centro de datos alterno.

9. MESA DE TRABAJO

En atención al “Procedimiento para Auditorías Internas de Gestión”, una vez remitido el informe preliminar por el Auditor Interno, se realizó mesa de trabajo el día 14 de

mayo de 2021, entre el Director de T.I, el Jefe de Operaciones, Equipo Auditor Bellicorp SAS y Equipo de Auditoría Interna de CISA, con el fin de consolidar el informe definitivo, los ajustes y observaciones allí presentados quedan soportados en el acta de mesa de trabajo que hace parte de los papeles de trabajo de la auditoría interna y estarán disponibles para su consulta en caso de ser requeridos.

Aprobado por:	Elaborado por:	Fecha aprobación
Elkin Orlando Ángel Muñoz Auditor Interno	**Bellicorp SAS** **Auditor Externo** Equipo Auditor	(19/05/2021)