Documento firmado digitalmente

GTEC

Para contestar cite:
Radicado ANI No.: **20251020217413**
20251020217413
Fecha: **02-12-2025**

MEMORANDO

Bogotá D.C.

PARA: **ÓSCAR FLOREZ MORENO**
Vicepresidente de Planeación, Riesgos y Entorno

HERNAN DARIO GUTIÉRREZ CASAS
Gerente de Proyectos G2- G.I.T. Tecnologías de la Información y las Telecomunicaciones.

DE: **JUDITH ALEJANDRA VARGAS LÓPEZ**
Jefe de la Oficina de Control Interno

ASUNTO: Informe de Auditoría Interna sobre la Infraestructura Tecnológica de la Agencia Nacional de Infraestructura (ANI).

Respetados Doctores,

La Oficina de Control Interno, realizó la auditoría interna de gestión sobre la Infraestructura Tecnológica de la Agencia Nacional de Infraestructura (ANI), documento que se anexa a la presente comunicación y en el cual se describen las conclusiones y recomendaciones en el capítulo 6, con el fin de que se coordinen las acciones tendientes a la atención del hallazgo y de las recomendaciones realizadas.

De acuerdo con lo previsto en el literal g del art. 4o y los literales h, j y k del artículo 12 de la Ley 87 de 1993, se envía copia de este informe a la dependencia responsable, con el fin de que se formulen los planes de mejoramiento correspondientes, en consideración a la necesaria adopción de medidas preventivas y/o correctivas, para lo cual el término recomendado es de treinta (30) días calendario contados a partir de la radicación del informe de auditoría.

Documento firmado digitalmente

GTEC

Para contestar cite:
Radicado ANI No.: **20251020217413**
20251020217413
Fecha: **02-12-2025**

Cordialmente,

JUDITH ALEJANDRA VARGAS LÓPEZ
Jefe de la Oficina de Control Interno

cc: 1) HERNAN DARIO GUTIERREZ CASAS G GIT GIT de Tecnologias de la Informacion y las Telecomunicaciones BOGOTA D.C.

Proyectó: Andrea del Pilar Lozada Lugo – Contratista Oficina de Control Interno

VoBo: JUDITH ALEJANDRA VARGAS LOPEZ GIT

Nro Rad Padre:

Nro Borrador: 20251020081185

GADF-F-010

Firmado Digitalmente
JUDITH ALEJANDRA VARGAS LOPEZ
YKTH-LOAJ-OF1O-TK49-A176-4724-6173-47

02/12/2025 20:16:57 COT -05

ANI

AUDITORÍA DE GESTIÓN

Informe de Auditoría Interna sobre la Infraestructura Tecnológica de la Agencia Nacional de Infraestructura (ANI).

2025

CONTENIDO

1. OBJETIVO

OBJETIVO GENERAL

Evaluar el estado actual, la gestión y los controles en relación con la infraestructura tecnológica de la Agencia Nacional de Infraestructura (ANI).

OBJETIVOS ESPECÍFICOS:

1. Verificar el estado físico y lógico de los componentes de la infraestructura tecnológica, incluyendo inventario, condiciones operativas y controles de manejo.

2. Revisar la existencia, funcionalidad y efectividad de las herramientas de monitoreo implementadas para supervisar la infraestructura tecnológica.

3. Validar los procedimientos de almacenamiento de información, copias de seguridad y el plan de recuperación ante desastres, asegurando su alineación con estándares de seguridad y continuidad del negocio.

4. Evaluar el diseño y efectividad de los controles de gestión asociados a la Infraestructura Tecnológica.

2. ALCANCE

La auditoría abarcó el periodo comprendido entre el 1 de enero de 2024 y el 31 de octubre de 2025, en cuanto a la revisión de los activos tecnológicos de la ANI, incluyendo servidores, redes, sistemas de almacenamiento, herramientas de monitoreo, políticas de respaldo y recuperación de información.

La evaluación se enfocó en las operaciones realizadas por el equipo de trabajo de infraestructura del GIT de Tecnologías en cuanto al cumplimiento de lineamientos y normas vigentes sobre la materia, la gestión y el monitoreo sobre la infraestructura tecnológica, y el diseño y la ejecución de controles asociados.

3. MARCO NORMATIVO

A continuación, se describe el marco legal e institucional.

- Ley 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la Organización de las Tecnologías de la Información y las Comunicaciones y otras disposiciones.
- Decreto 1078 de 2015: Régimen general de las TIC " Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

- Manual Operativo MIPG- Modelo Integrado de Planeación y Gestión: Establece actividades de control relevantes sobre las infraestructuras tecnológicas.
- Modelo MSPI: El Modelo de Seguridad y Privacidad de la Información.
- Instructivo copias de seguridad de los sistemas de información e infraestructura tecnológica. (GTEC-I-005)
- Guía para la gestión integral del riesgo en entidades públicas v7
- Instructivo metodológico para la administración de riesgos de gestión – fiscales (SEPG-I-015)

4. METODOLOGÍA

La metodología empleada por la Oficina de Control Interno para esta auditoría de gestión se basa en la Guía de Auditoría Interna basada en riesgos para entidades públicas del Departamento Administrativo para la Función Pública y el procedimiento interno a cargo de la Oficina de Control Interno, para la cual se realizaron las siguientes actividades:

Notificación y Solicitud de Información: El día 27-10-2025, a través de memorando interno No.20251020193023 emitido por la Oficina de Control Interno (OCI) se notificó la auditoría interna de la Infraestructura Tecnológica de la Agencia Nacional de Infraestructura (ANI) a la Vicepresidencia de Planeación, Riesgos y Entorno y al Gerente de Proyectos G2 del G.I.T Tecnologías de la Información y las Telecomunicaciones (GIT de TI) y se solicitó la información correspondiente. Posteriormente, el día 30-11-2025, el Gerente de Proyectos del GIT de TI solicitud ampliación de plazo para la entrega de información con el memorando No 20256070195273 a la Oficina de Control interno sobre la cual la OCI dio respuesta con memorando No. 20251020196283 del 31-10-2025 otorgando el plazo de entrega de información e informando el correspondiente ajuste en el plan de auditoria para las fases de Ejecución, Informe y Cierre.

***Ejecutar la Auditoría*:** Durante la ejecución de la auditoría, se revisó la información aportada para la auditoría y se realizaron las correspondientes reuniones presenciales y virtuales con el propósito de recopilar información adicional para complementar los análisis de la auditoria. Adicionalmente, se realizó visita al Data Center y a los cuartos técnicos.

Los resultados de la evaluación se detallan en el presente informe, en el que se generaron hallazgos, conclusiones y recomendaciones.

***Socialización de resultados**:* El día 28-11-2025, a las 7:07 p.m. se socializó mediante correo electrónico los resultados del informe de seguimiento de la auditoría de infraestructura.

5. DESARROLLO DEL INFORME

El presente informe tiene como propósito evaluar el estado actual, la gestión y los controles en relación con la infraestructura tecnológica de la Agencia Nacional de Infraestructura (ANI).

A partir de la revisión realizada a continuación, se detallan los resultados por cada uno de los objetivos específicos planteados. Así mismo, se incluyen conclusiones y recomendaciones orientadas a optimizar los recursos tecnológicos y la infraestructura, garantizando la continuidad operativa y fortaleciendo la capacidad de adaptación frente a nuevas demandas de infraestructura.

5.1 VERIFICAR EL ESTADO FÍSICO Y LÓGICO DE LOS COMPONENTES DE LA INFRAESTRUCTURA TECNOLÓGICA, INCLUYENDO INVENTARIO, CONDICIONES OPERATIVAS Y CONTROLES DE MANEJO.

5.1.1 Revisión componentes de infraestructura.

Se llevó a cabo una inspección de las instalaciones del Data Center y Cuartos técnicos o de comunicaciones, con el acompañamiento del Experto G3. El recorrido realizado para la visita fue en el edificio T3, Piso 2 de la Torre 4, para cuartos técnicos o de comunicación en Piso 6,7 de la misma torre y piso 8 (zonas sur y norte) de la Torre 3, con el objetivo de observar el estado actual de la infraestructura disponible para garantizar su adecuación a los requerimientos operativos y de servicio.

A continuación, se relacionan los centros de datos inspeccionados y los aspectos relevantes identificados en cada uno de los pisos.

LOCACIÓN	ASPECTOS CON LOS QUE CUENTA DATA CENTER	PISO 8 (Cuartos de comunicación)				PISO 6 (Cuartos de comunicación)		PISO 7 (Cuartos de comunicación)		PISO 2 (Datacenter)	
		Norte		Sur							
		SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
Infraestructura física	Sistema de seguridad física. (control de acceso biométrico)	X		X		X		X		X	
	Unidades de distribución de energía (UPS y generados de respaldo).	X		X		X		X		X	
	Sistema de climatización.(Aire acondicionado)	X		X		X		X		X	
	Confinamiento (Separación física del aire frío y aire caliente)		X		X		X		X	X	
	Piso elevado	X		X		X		X		X	
	Almacenamiento									X	
	Software de backup									X	
	Servidores hiperconvergencia									X	
	Switch	X		X		X		X		X	
	Rack-Gabinete	X		X		X		X		X	
	Extintores	X		X		X		X		X	
	Panel de detección de incendios	X		X		X		X		X	
	Biométricos	X		X		X		X		X	
	Puerta contra fuego	X		X		X		X		X	
	Access Point	X		X		X		X		X	
	Firewall									X	
	Sensores de humedad									X	
	Transformador									X	
Infraestructura de red.	Cables, cableado estructurado	X		X		X		X		X	
Seguridad y control.	Sistema de control de acceso	X		X		X		X		X	
	Planilla de registro de a datacenter	X		X		X		X		X	
	Videovigilancia		X		X	X		X		X	
	Sistema de detección y extinción de incendios	X		X		X		X		X	

Fuente: Tabla de creación propia para inspección de Datacenter- Cuartos técnicos.

Durante la revisión del Data Center y los cuartos técnicos se identificó que uno de los controles de ingreso físico se realiza de forma manual mediante una planilla denominada *"Lista de control de ingreso de personal"*; al verificarla, se evidenciaron las siguientes situaciones:

1. Falta especificar el piso en la planilla de control de ingreso de personal: Se identificó que las planillas de control para el ingreso al Data Center y a los cuartos técnicos no especifican el piso correspondiente, lo que limita la trazabilidad de registros de control de accesos.

2. Se requiere mayor precisión en la columna "motivo de ingreso", al diligenciar la planilla de control de ingreso de personal, especialmente en los casos registrados como "revista", que corresponden al ingreso del personal de seguridad para realizar rondas y realizar el apagado de luces de los pasillos.

3. Al indagar por planillas de control de ingreso del 2024, se observó ausencia de registros históricos: En 2024 no se efectuó un control efectivo sobre el diligenciamiento de la plantilla en el Data Center (piso 2). Este control se implementó de manera continua a partir de agosto de 2025, tras la adecuación de la infraestructura.

5.1.2 Inventario.

Durante la visita a los cuartos técnicos y al Data Center se identificaron bienes tecnológicos nuevos, evidenciando el fortalecimiento de la infraestructura tecnológica (TI), la cual fue adquirida mediante el "*Convenio derivado No. 02 del convenio marco interadministrativo No. 939 del 2023 celebrado entre la agencia nacional de infraestructura y la corporación agencia nacional de gobierno digital- ANI- CI-015 DE 2023*".

En relación con el inventario de equipos de cómputo, mediante el memorando radicado No. 2020256070197403 del 04-11-2025, se solicitó el inventario actualizado de activos tecnológicos de la entidad, (hardware, software, redes, servidores, estaciones de trabajo). En respuesta, el GIT de TI entregó el archivo denominado *"Inv y Clasif de Activ de Infor ANI_GTEC. xlsx",* que contiene el detalle del inventario de equipos de cómputo, con corte al 31 diciembre de 2024. Según este documento la entidad cuenta con un total de 751 equipos distribuidos de la siguiente manera: 718 computadores portátiles y 33 computadores de escritorio.

Al realizar un análisis sobre el inventario de equipos de cómputo, se identificó que algunos colaboradores tienen a su cargo más de un equipo de cómputo registrado a su nombre en este inventario. Dentro de los casos más relevantes observados está:

- 1 funcionario del GIT Tecnologías de la Información y las Telecomunicaciones, tiene registrado a su nombre 25 equipos.
- 1 contratista del GIT Tecnologías de la Información y las Telecomunicaciones, tiene registrado a su nombre 15 equipos.
- 1 funcionario del GIT Administrativo y Financiero, tiene registrado a su nombre 9 equipos
- 1 especialista de mesa de ayuda del GIT Tecnologías de la Información y las Telecomunicaciones, tiene registrado a su nombre 7 equipos.
- 2 funcionarios del GIT Administrativo y Financiero, tienen registrado cada uno a su nombre 6 equipos.
- 1 funcionario de la Vicepresidencia de Estructuración tiene registrado a su nombre 5 equipos.

Nota: El detalle del personal que presentan las situaciones se muestra en el archivo anexo *"1- inventario equipos cómputo"*.

Esta situación refleja una concentración significativa de activos tecnológicos vinculados a determinado personal, el cual requiere revisión para garantizar una adecuada administración y optimización de los recursos.

5.2. REVISAR LA EXISTENCIA, FUNCIONALIDAD Y EFECTIVIDAD DE LAS HERRAMIENTAS DE MONITOREO IMPLEMENTADAS PARA SUPERVISAR LA INFRAESTRUCTURA TECNOLÓGICA.

Se efectuó reunión del día 13-11-2025 en la que se observó que se cuenta con 2 herramientas de monitoreo, una es la plataforma Zabbix herramienta Open Source diseñada para supervisar el rendimiento y la disponibilidad de servidores, redes, aplicaciones y servicios On premise, y la otra es la herramienta Azure Monitor para garantizar la disponibilidad de los servicios en nube.

Indagando acerca del monitoreo realizado durante el año 2024, se identificó que el monitoreo se realizaba directamente en cada dispositivo, ya que éstos contaban con sus propios indicadores; y que, para verificar el estado de la infraestructura era necesario acceder individualmente a cada equipo, lo que implicaba un proceso manual, dedicado y disperso.

A partir de enero del 2025, la entidad empezó a utilizar la herramienta llamada Zabbix, encargada de centralizar el monitoreo de la infraestructura tecnológica. Esta solución permite supervisar infraestructura física, servidores (físicos y virtuales), equipos de comunicaciones, dispositivos de seguridad, controladoras Wi-Fi, entre otros componentes, consolidando la información en una única plataforma para una gestión más eficiente. De igual manera, se comenzó a utilizar la herramienta Azure Monitor para los servicios en la nube.

Aunque el monitoreo se esté realizando con las dos herramientas: Zabbix y Azure Monitor, Zabbix, al ser una solución Open Source, limita en automatización avanzada, escalabilidad y soporte. Además, el monitoreo hacia los componentes no se realiza durante el 100% del tiempo, lo que podría generar riesgos en la detección temprana de fallas o posibles incidentes.

Por otra parte, la ausencia de un Centro de Operaciones de Seguridad (SOC) limita las capacidades de monitoreo de los componentes tecnológicos lo que puede afectar la disponibilidad.

Igualmente, se realizó una revisión en la herramienta Zabbix para identificar los usuarios con privilegios de administración en el sistema de monitoreo de infraestructura. Durante esta verificación se observó:

1. Existen seis usuarios con privilegios elevados, es decir, con perfil de superadministrador.

2. Se observó que 1 cuenta está asociada al anterior administrador en la herramienta, lo que evidencia la necesidad de actualizar y depurar los perfiles para garantizar una adecuada gestión de privilegios y reducir riesgos asociados a cuentas con permisos elevados. Ver Anexo 2

5.3. VALIDAR LOS PROCEDIMIENTOS DE ALMACENAMIENTO DE INFORMACIÓN, COPIAS DE SEGURIDAD Y EL PLAN DE RECUPERACIÓN ANTE DESASTRES, ASEGURANDO SU ALINEACIÓN CON ESTÁNDARES DE SEGURIDAD Y CONTINUIDAD DEL NEGOCIO.

5.3.1 Revisión de procedimientos de almacenamiento de información, copias de seguridad.

El 19-11-2025 se llevó a cabo una reunión con el personal involucrado en los procesos de almacenamiento de información, copias de seguridad y plan de recuperación ante desastres. Durante la sesión se realizó una entrevista estructurada, en la cual se formularon diversas preguntas y se observaron las herramientas utilizadas.

Durante la entrevista se consultó sobre la existencia de una política, instructivo o documento que reglamente el almacenamiento de copias de seguridad. El personal confirmó la existencia del documento *"Instructivo Copias de Seguridad de los Sistemas de Información e Infraestructura Tecnológica (GTEC-I-005_Copias_de_Seguridad_de_TI_V2)"*, cuya última actualización corresponde al 26-10-22.

En la reunión se revisaron las herramientas utilizadas y los procedimientos actuales para la realización de copias de seguridad, su almacenamiento y los procesos de restauración. Asimismo, se evaluó el cumplimiento del instructivo "Copias de Seguridad de los Sistemas de Información e Infraestructura Tecnológica (GTEC-I-005)", en donde se identificó que:

Hallazgo 1: Desalineación entre el instructivo GTEC-I-005 y la práctica actual de copias de seguridad para On premise.

Al revisar las herramientas utilizadas para realizar las copias de respaldo y contrastarlas con lo establecido en el instructivo *"Copias de Seguridad de los Sistemas de Información e Infraestructura Tecnológica (GTEC-I-005)",* se identificó que actualmente se están realizando las copias de seguridad en On Premise con la herramienta Veeam Backup, lo cual no está definido en el numeral 2 del instructivo para On Premise.

Esta situación evidencia un incumplimiento en la aplicación del instructivo generando una brecha entre la práctica operativa y la documentación interna establecida.

5.3.2 Restauraciones.

En la misma reunión realizada el 19-11-2025, se evidenció que se han realizado restauraciones de información, las cuales se ejecutan bajo demanda. Sin embargo, se identificaron oportunidades de mejora en esta actividad, tales como programar pruebas periódicas durante el año siguiendo un cronograma establecido, para validar la efectividad de los respaldos. Estas pruebas deberían incluir la instalación de máquinas de prueba y la restauración completa de datos, con el fin de garantizar que los backups se encuentran operativos y cumplen con los objetivos de continuidad del negocio.

5.3.3 Plan de recuperación de desastres.

El Plan de Recuperación ante Desastres (DRP) en la ANI, de acuerdo con lo indicado por el experto G3 del GIT DE TI, se basa en dos pilares clave: herramientas tecnológicas que aseguran la protección y recuperación de la información, y un equipo con roles definidos para ejecutar acciones de manera rápida y eficiente, garantizando la continuidad operativa ante cualquier contingencia.

Al preguntar acerca de Planes de contingencia y continuidad del negocio de la infraestructura tecnológica en la respuesta allegada mediante memorando No 20256070197403 del 04-11-2025, se informó a la OCI que: *"Actualmente la entidad no cuenta con un Plan de Continuidad del Negocio (PCN) y un Plan de Recuperación de Desastres (DRP) de la infraestructura tecnológica formulados e implementados de manera integral. (.....), En resumen, se definió el modelo y la responsabilidad para el desarrollo de estos planes, pero su ejecución está pendiente de la activación del proceso por parte del área de Planeación, en línea con la articulación requerida. Es pertinente tener en cuenta que el proceso de construcción del Plan de Continuidad del Negocio es un requisito previo para la formulación del DRP tecnológico y que la reciente vinculación del CISO (en agosto), ha concentrado los esfuerzos en la estabilización de la gestión de seguridad."*

Igualmente, al indagar si se están efectuando pruebas de restauración del servicio utilizando infraestructura que opere fuera de la entidad, se identificó que la ANI no cuenta con infraestructura alterna, para restaurar copias de seguridad o realizar consultas posteriores a una restauración. Esta ausencia de infraestructura limita la capacidad de respuesta ante eventos de contingencia, afectando la continuidad operativa y la disponibilidad de información para la entidad.

En ese sentido, no se cuenta en la entidad con un Plan de Recuperación de Desastres (DRP) de la infraestructura tecnológica formulado e implementado de manera integral **.** Si bien el personal conoce el concepto y su relación con dos aspectos principales (herramientas para salvaguardar, recuperar la información y roles definidos para la ejecución de acciones), se evidenció la ausencia de un procedimiento documentado y formalizado donde este indique como esta formulado y se implemente el plan de recuperación de desastres (DRP) con las directrices, responsabilidades y pasos a seguir.

Igualmente, falta infraestructura alterna (fuera de la entidad) que permita garantizar la operación de los servicios tecnológicos ante contingencias, lo que representa un riesgo para la disponibilidad y operatividad de los servicios.

5.4. EVALUAR EL DISEÑO Y EFECTIVIDAD DE LOS CONTROLES DE GESTIÓN ASOCIADOS A LA INFRAESTRUCTURA TECNOLÓGICA.

En la reunión del 19-11-2025 el experto G3 presentó la matriz de riesgos del proceso de gestión tecnológica, elaborada por el Grupo Interno de Trabajo de Tecnología de la Información y las Telecomunicaciones. Esta matriz incluye el riesgo identificado junto con sus respectivos controles, relacionados para la infraestructura tecnológica.

RIESGO: RG-GTEC-03 Posibilidad de pérdida reputacional y económica por interrupción o falla en la continuidad de la prestación de los servicios de T.I. debido a fallas en equipos físicos, ataques o configuraciones que afecten la disponibilidad.

RESPONSABLE	ACCIÓN	COMPLEMENTO	N.	CONTROL
El equipo técnico del G.I.T de Tecnologías de la Información y las Telecomunicaciones.	revisan **permanentemente** las alertas generadas sobre los elementos de la infraestructura tecnológica y de los sistemas de información,	a través de la herramienta de monitoreo, de conformidad con el instructivo "Gestión de cambios de TI (GTEC-I-003)", a fin de evitar interrupciones en los servicios de TI, dejando como evidencias los documentos de la gestión del cambio en el repositorio asignado para tal fin.	1	El equipo técnico del G.I.T de Tecnologías de la Información y las Telecomunicaciones revisan permanentemente las alertas generadas sobre los elementos de la infraestructura tecnológica y de los sistemas de información, a través de la herramienta de monitoreo, de conformidad con el instructivo "Gestión de cambios de TI (GTEC-I-003)" , a fin de evitar interrupciones en los servicios de TI, dejando como evidencias los documentos de la gestión del cambio en el repositorio asignado para tal fin.
El equipo técnico del G.I.T de Tecnologías de la Información y las Telecomunicaciones	realizan permanentemente el monitoreo y seguimiento a la plataforma de seguridad de la infraestructura tecnológica,	a través de las herramientas de monitoreo y reportes de alertas de incidentes de seguridad realizando actividades preventivas y correctivas con el fin de reducir la probabilidad de ocurrencia, dejando como evidencias los registros de alertas gestionadas en el GLPI.	2	El equipo técnico del G.I.T de Tecnologías de la Información y las Telecomunicaciones realizan permanentemente el monitoreo y seguimiento a la plataforma de seguridad de la infraestructura tecnológica, a través de las herramientas de monitoreo y reportes de alertas de incidentes de seguridad, realizando actividades preventivas y correctivas con el fin de reducir la probabilidad de ocurrencia, dejando como evidencias los registros de alertas gestionadas en el GLPI.
El coordinador y equipo técnico del G.I.T de Tecnologías de la Información y las Telecomunicaciones	cada vez que reciba una solicitud de cambio sobre plataforma tecnológica, revisan la viabilidad del cambio y su impacto,	a través del análisis a la solicitud, autorizando la implementación del cambio y su ejecución, con el fin de reducir el riesgo de una interrupción de los servicios, dejando como evidencias, los documentos de la gestión del cambio en el repositorio asignado para tal fin.	3	El coordinador y equipo técnico del G.I.T de Tecnologías de la Información y las Telecomunicaciones cada vez que reciba una solicitud de cambio sobre plataforma tecnológica, revisan la viabilidad del cambio y su impacto, a través del análisis a la solicitud, autorizando la implementación del cambio y su ejecución, con el fin de reducir el riesgo de una interrupción de los servicios, dejando como evidencias, los documentos de la gestión del cambio en el repositorio asignado para tal fin.

Fuente: Imagen de matriz de riesgos de Gestión tecnológica.

Con ocasión de revisar el diseño de los controles, se tuvo en cuenta lo referenciado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas v7 (Agosto 2025) del Departamento Administrativo de la Función Pública (DAFP), así como también el instructivo metodológico para la administración de riesgos de gestión- fiscales V2 de la entidad (SEPG-I-015) del 22-05-2025.

Al evaluar el diseño de los controles, se observaron 3 controles en los cuales el G.I.T. Tecnologías de la Información y las Telecomunicaciones tuvo en cuenta la estructura que se menciona en el instructivo metodológico para la administración de riesgos de gestión- fiscales V2, (SEPG-I-015), en el punto 5.8 descripción de controles así::

5.8 DESCRIPCIÓN DE CONTROLES

Posterior a la valoración del riesgo, se deben implementar controles que disminuyan la probabilidad o impacto del riesgo. Un control es la medida que permite reducir o mitigar el riesgo. La identificación de controles debe realizarse en la parte del formato denominada "Descripción del control" para cada uno de los riesgos identificados, a través de mesas de trabajo al interior de cada equipo de riesgos, utilizando el criterio de experto, documentos formalizados en el Sistema de Gestión de Calidad, entre otras herramientas. Los responsables de implementar, realizar seguimiento y actualizar los controles definidos, son los líderes de proceso con el apoyo de su equipo de riesgos.

Tabla 13 Descripción del control

DESCRIPCIÓN DEL CONTROL				
RESPONSABLE	ACCIÓN	COMPLEMENTO	No.	CONTROL

Fuente: Elaboración propia, con el Mapa de riesgos por proceso y seguimientos a los riesgos SEPG-F-030.

La redacción del control debe tener en cuenta la estructura que se menciona a continuación, la cual facilitará identificar sus diferentes atributos:

Descripción del control = Responsable + Acción + Complemento.

- **Responsable:** Se debe relacionar el cargo del coordinador, gerente, o jefe del área responsable de ejecutar el control. Para los casos en los cuales el control lo ejecuta un servidor público en específico se debe relacionar su cargo, de lo contrario, se debe generalizar a todos los colabores del área asignados.
- **Acción:** Se debe iniciar con verbos que indiquen la acción que se realiza como parte del control. Por ejemplo: Verifica, valida, revisa, coteja, entre otros.
- **Complemento:** Se deben indicar todos los detalles que permitan entender claramente el objeto del control. Dentro de estos es obligatorio definir la periodicidad establecida para la ejecución del control, el propósito del control, la herramienta utilizada o la explicación de cómo se realiza la acción del control y la evidencia resultante de su ejecución.

Fuente: Imagen del instructivo SEP-I-015

Sin embargo, se observó que los controles No. 1 y 2 tienen como responsable el equipo técnico del G.I.T de Tecnología de la Información y Telecomunicaciones, según lo establecido en el instructivo:

***"Responsable:** Se debe relacionar el cargo del coordinador, gerente, o jefe del área responsable de ejecutar el control. Para los casos en los cuales el control lo ejecuta un servidor público en específico se debe relacionar su cargo, de lo contrario, se debe generalizar a todos los colabores del área asignados. "*

Adicionalmente, sobre la designación del responsable en la ejecución de los controles, la Guía para la gestión integral del riesgo en entidades públicas v7 del 2025 del Departamento Administrativo de la Función Pública (DAFP), señala lo siguiente[1]:

"Responsable: Determina el cargo del responsable que ejecuta el control, se deberá considerar la estructura organizacional y las diferentes denominaciones de empleos (Directores, asesores, profesionales, técnicos, asistenciales), así como su despliegue en grupos de trabajo internos e incluir coordinadores o gerentes de proyectos. Cuando se trate de controles automáticos se identificará el responsable de su calibración o parametrización periódica en el sistema de información o software a través del cual opere el control.

Su definición deberá igualmente considerar que éste cuenta con un nivel de autoridad apropiado de cara a la actividad de control, así como aspectos básicos de segregación de funciones para evitar que quién sea la fuente generadora de riesgo, sea el único que aplica alguna actividad de control."

Por lo anterior, como está establecida la responsabilidad actualmente sobre los controles No.1 y 2, no se tiene claridad sobre la responsabilidad de su ejecución, específicamente quien revisa permanentemente las alertas generadas sobre los elementos de la infraestructura tecnológica y de los sistemas de información para el control No.1 y quien realiza permanentemente el monitoreo y seguimiento a la plataforma de seguridad de la infraestructura tecnológica según el control No.2.

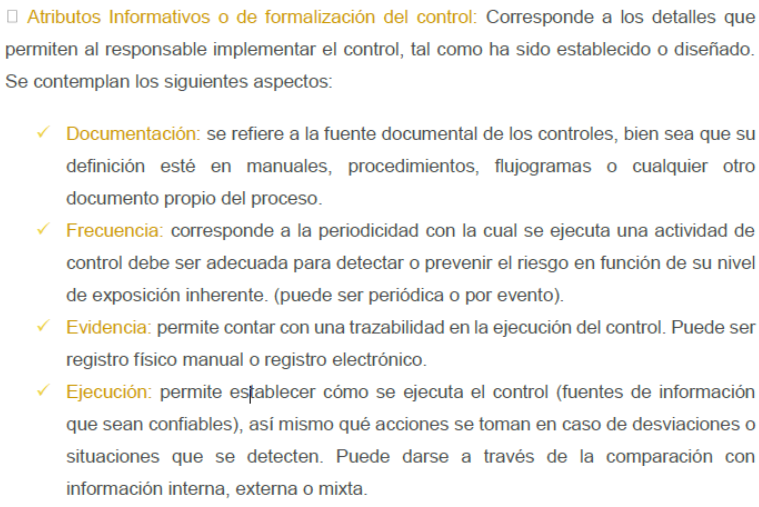
Ahora bien, en relación con la variable relacionada con la periodicidad del control, los controles No.1 y 2 señalan en la acción "permanentemente", lo cual evidencia que la periodicidad o frecuencia de ejecución del control no está acorde con lo establecido en el instructivo que señala:

*"**Complemento:** Se deben indicar todos los detalles que permitan entender claramente el objeto del control. Dentro de estos es obligatorio definir la periodicidad establecida para la ejecución del control, el propósito del control, la herramienta utilizada o la explicación de cómo se realiza la acción del control y la evidencia resultante de su ejecución"*

Y en la Guía para la gestión integral del riesgo en entidades públicas v7 del 2025 del Departamento Administrativo de la Función Pública (DAFP), que señala lo siguiente en frecuencia[2]:

[1] Guía para la gestión integral del riesgo en entidades públicas v7- página 61- Responsable.

[2] Guía para la gestión integral del riesgo en entidades públicas v7- página 62- Frecuencia.



- Atributos Informativos o de formalización del control: Corresponde a los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado. Se contemplan los siguientes aspectos:
  - ✓ Documentación: se refiere a la fuente documental de los controles, bien sea que su definición esté en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
  - ✓ Frecuencia: corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).
  - ✓ Evidencia: permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.
  - ✓ Ejecución: permite establecer cómo se ejecuta el control (fuentes de información que sean confiables), así mismo qué acciones se toman en caso de desviaciones o situaciones que se detecten. Puede darse a través de la comparación con información interna, externa o mixta.

Fuente: Imagen de la guía para la gestión integral del riesgo en entidades públicas v7

Así mismo, en cuanto a la acción descrita en el control No. 2 se encuentra definida como *"**realizan** permanentemente el monitoreo y seguimiento a la plataforma de seguridad de la infraestructura tecnológica"* (Negrilla fuera de texto); al respecto el instructivo establece:

"Acción: Se debe iniciar con verbos que indiquen la acción que se realiza como parte del control. Por ejemplo: Verifica, valida, revisa, coteja, entre otros."

Y en la Guía para la gestión integral del riesgo en entidades públicas v7 del 2025 del Departamento Administrativo de la Función Pública (DAFP), se señala lo siguiente:

"Acción: Determina para qué se realiza el control, se utilizan verbos fuertes como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar."

6. CONCLUSIONES, RECOMENDACIONES Y HALLAZGOS

El hallazgo, al igual que las conclusiones y recomendaciones resultantes del ejercicio de auditoría se presentan en esta sección.

6.1.Conclusiones.

En relación con el Objetivo 1, verificar el estado físico y lógico de los componentes de la infraestructura tecnológica, incluyendo inventario, condiciones operativas y controles de manejo.

- Durante la revisión del Data Center y los cuartos técnicos se evidenció que el control de ingreso físico, realizado mediante planillas manuales, presenta debilidades que afectan la trazabilidad y confiabilidad del registro, tales como la ausencia de información sobre el piso, falta de precisión en la descripción del motivo de ingreso. Estas situaciones reflejan la necesidad de

fortalecer el diseño y la aplicación del control para garantizar un adecuado seguimiento y documentación de los accesos.

- Tras el análisis del inventario de equipos de cómputo, algunos funcionarios y/o contratistas presentan múltiples equipos asignados a su nombre, lo que evidencia una concentración de activos asociados a una determinada persona. Esta situación podría indicar falta de control en la gestión y asignación de equipos.

En relación con el Objetivo 2, revisar la existencia, funcionalidad y efectividad de las herramientas de monitoreo implementadas para supervisar la infraestructura tecnológica.

- El monitoreo actual de la infraestructura tecnológica presenta limitaciones debido a la dependencia de Zabbix como herramienta, que, al ser una solución de código abierto, restringe funcionalidades avanzadas de automatización, escalabilidad y soporte especializado. Adicionalmente, la ausencia de un Centro de Operaciones de Seguridad (SOC) reduce de manera considerable la capacidad de supervisión integral y respuesta ante incidentes, lo que incrementa el riesgo de afectación a la disponibilidad y continuidad de los servicios tecnológicos**.**
- Existen seis usuarios con privilegios elevados en la herramienta de monitoreo Zabbix, con perfil de superadministrador y una de esas cuentas está asociada al anterior administrador en la herramienta, lo que evidencia la necesidad de actualizar y depurar los perfiles para garantizar una adecuada gestión de privilegios y reducir riesgos asociados a cuentas con permisos elevados.

En relación con el Objetivo 3, validar los procedimientos de almacenamiento de información, copias de seguridad y el plan de recuperación ante desastres, asegurando su alineación con estándares de seguridad y continuidad del negocio.

- La revisión evidenció que los procedimientos actuales para la realización de copias de seguridad no cumplen con lo establecido en el instructivo GTEC-I-005, lo que refleja una falta de alineación para las copias de seguridad On premise entre la normativa interna y la práctica operativa. Por lo que se requiere una actualización del instructivo y la implementación de controles que garanticen su cumplimiento, por lo tanto, se estableció el siguiente hallazgo:

HALLAZGO 1: Desalineación entre el instructivo GTEC-I-005 y la operación actual de copias de seguridad para On Premise.

Al revisar las herramientas utilizadas para realizar las copias de respaldo y contrastarlas con lo establecido en el instructivo *"Copias de Seguridad de los Sistemas de Información e Infraestructura Tecnológica (GTEC-I-005)",* se identificó que se debe actualizar el numeral 2. On Premise debido a que no se está llevando a cabo lo descrito en el instructivo para las copias de seguridad de los servicios On premise. Esta situación evidencia un incumplimiento en la aplicación del instructivo generando una brecha entre la práctica operativa y la normativa interna establecida.

- La ausencia de un Plan de Recuperación de Desastres (DRP) formalizado y documentado, junto con la falta de infraestructura alterna para garantizar la continuidad operativa, representa un riesgo crítico para la disponibilidad de los servicios tecnológicos. La falta de procedimientos establecidos limita la capacidad de respuesta ante contingencias, lo que hace indispensable la formulación e implementación integral del DRP y la adopción de soluciones que aseguren la operación fuera de la entidad ante un desastre.

En relación con el Objetivo 4, evaluar el diseño y efectividad de los controles de gestión asociados a la infraestructura tecnológica.

- Se evidenció que las variables para la evaluación del diseño de los controles No. 1 y 2, relacionados con responsable, el propósito del control y la periodicidad tienen debilidades teniendo en cuenta la Guía para la gestión integral del riesgo en entidades públicas v7. En relación con la variable asociada a la responsabilidad sobre la ejecución de los controles, la falta de claridad en la asignación de un responsable podría incrementar la exposición de los riesgos que se pretenden mitigar.

6.2. Recomendaciones.

- Actualizar las planillas de control de acceso de personal al Data Center y los cuartos técnicos incorporando la identificación del piso correspondiente a cada registro.
- Capacitar y socializar al personal que ingresa a las instalaciones restringidas el diligenciamiento de la plantilla de control de ingreso de personal con un mayor detalle en el diligenciamiento de la columna "motivo de ingreso", asegurando que se describa de forma clara y precisa el motivo.
- Establecer un procedimiento integral que contemple la validación y depuración del inventario de equipos de cómputo, con el fin de confirmar la necesidad real de los dispositivos asignados, el cual debe establecer límites definidos en la cantidad de equipos por colaborador según su rol, con el fin de optimizar la administración de recursos y asegurar un control eficiente y confiable.

- Realizar una depuración de perfiles en la herramienta Zabbix, donde se ajusten los privilegios con segmentación de usuarios. Adicionalmente, se sugiere implementar revisión periódica de usuarios, establecer controles trimestrales para verificar la vigencia y pertinencia de los perfiles. Así como también aprobara la política de derechos de acceso privilegiados.
- Para lograr un monitoreo integral, se recomienda establecer un Centro de Operaciones de Seguridad (SOC) y un Centro de Operaciones de Red (NOC) internos, o contratar servicios gestionados que aseguren la supervisión continua tanto de la seguridad como del rendimiento de la infraestructura tecnológica. Este enfoque permitirá prevenir, detectar, analizar y responder de manera proactiva a ciberamenazas las 24 horas del día, garantizando tiempos de reacción rápidos y efectivos, mientras se mantiene la disponibilidad, estabilidad y eficiencia de la red."
- Establecer un cronograma anual de pruebas de restauración que contemple fechas específicas para validar la funcionalidad de los respaldos, asignar responsables y roles definidos para la ejecución y supervisión de las pruebas de restauración y documentar los resultados de cada prueba en un registro formal, incluyendo incidencias y acciones correctivas.
- Actualizar el instructivo GTEC-I-005 en lo relacionado con las copias de seguridad On Premise y la implementación de controles que garanticen su cumplimiento, incorporando la obligatoriedad de pruebas periódicas y los procedimientos detallados para su ejecución; continuar implementando pruebas controladas en entornos aislados (máquinas de prueba) para asegurar la correcta restauración de los backups; fortalecer y madurar el proceso de copias de seguridad, asegurando que la infraestructura y los procedimientos estén preparados para necesidades futuras; y programar pruebas periódicas durante el año siguiendo un cronograma establecido para validar la efectividad de los respaldos.
- Elaborar un documento formal con base en las mejores prácticas, que describa el Plan de Recuperación ante Desastres (DRP) y definir el procedimiento detallado que indique como mínimo los objetivos, las actividades, responsables, herramientas y tiempos para la ejecución del DRP en caso de contingencia.
- Socializar el DRP y realizar pruebas periódicas para confirmar que el personal esté preparado y que el plan funcione correctamente. Adicionalmente, asegurar su monitoreo por parte de las instancias correspondientes para garantizar su vigencia y aplicabilidad.
- Establecer un sitio alterno (propio o mediante acuerdos con terceros) que cuente con infraestructura con requerimientos mínimos necesarios, para probar escenarios de contingencia y definir procedimientos claros para la restauración de servicios (BCP).
- Revisar el diseño de los controles, de acuerdo con lo establecido en la guía para la gestión integral del riesgo en entidades públicas v7.

Elaboró informe:

Andrea de Pilar Lozada Lugo

Auditor Oficina de Control Interno

Revisó y aprobó informe:

Judith Alejandra Vargas López

Jefe de Oficina de Control Interno

ANEXOS

A continuación, se presenta una lista de los documentos que se anexan más adelante:

- Anexo 1: Nombre de anexo 1.
- Anexo 2: Nombre de anexo 2.
- Anexo 3: Nombre de anexo 3.
- Anexo 4: Nombre de anexo 4.