AGENCIA NACIONAL DE DEFENSA JURIDICA DEL ESTADO

INFORME FINAL DE AUDITORIA AL PROCESO DE GESTION DE TECNOLOGIAS DE LA INFORMACIÓN

Enero de 2025
Oficina de Control Interno
Elaborado Por: Jorge Hernando Torres Ribero
Aprobado por: Adriana Milena Herrera Abril

1. Introducción

La Oficina de Control Interno de la Agencia Nacional de Defensa Jurídica del Estado, en el desarrollo de su Plan Anual de Auditorias 2024 – 2025, practicó la auditoria al Proceso de Gestión de Tecnologías para el periodo enero a junio de 2024, con el objetivo de verificar la eficacia y efectividad de la gestión, ejecución y control de los procedimientos que hacen parte de este.

Dicha auditoria se efectuó del 22 de julio al 3 de octubre de 2024 y sus resultados se presentan a continuación.

En comunicación por correo electrónico institucional del viernes 15/11/2024 05:27 p. m. dirigida a la jefe de la Oficina Asesora de Control Interno, el Líder del Proceso auditado envió respuesta al informe preliminar, con sus comentarios al respecto sobre las no conformidades y observaciones encontradas en la Auditoria, con el fin de que algunas sean retiradas o calificadas como observación o recomendación, solicitud a la que esta oficina procedió a su evaluación y se encuentra incluida en el presente informe.

2. Limitaciones del informe:

No aplica

3. Desarrollo del informe:

La Oficina de Control Interno a través de esta auditoría validó los sistemas críticos de TI, abarcando aspectos de desarrollo de software, mantenimiento de infraestructura tecnológica y soporte técnico. Además, evaluó la alineación estratégica de estos sistemas con los objetivos de la entidad.

Así las cosas, en revisión preliminar con la OASTI se procedió a elaborar lista de chequeo contentiva de los siguientes temas:

- **Evaluación de Sistemas Críticos**: Disponibilidad, redundancia, y seguridad de la infraestructura de TI.
- **Evaluación de Desarrollo y Mantenimiento de Software**: Control y adecuación en los desarrollos internos y en el ciclo de vida del software.
- **Evaluación de Soporte y Administración de Tecnologías**: Eficacia en los servicios de soporte técnico y cumplimiento de acuerdos de nivel de servicio.
- **Evaluación de Integración y Conformidad Estratégica**: Alineación de las tecnologías con los objetivos estratégicos de la entidad y cumplimiento normativo.

3.1. Análisis de normatividad

3.1.1. Justificación del Uso de Normas u Estándares Internacionales bajo Normas Superiores de la Administración Pública

Aunque no son obligatorias en Colombia, las normas internacionales empleadas en esta auditoría son criterios válidos debido a su relevancia técnica y su alineación con los principios constitucionales y administrativos aplicables a la gestión pública. Además, estas normas complementan y fortalecen el cumplimiento de las normativas nacionales obligatorias, como el **RETIE** y la **NSR-10**, aplicables a infraestructuras críticas.

3.1.2. Principios Constitucionales y Administrativos

- El **artículo 209 de la Constitución Política** exige que las entidades públicas actúen bajo los principios de eficiencia, eficacia y economía, adoptando las mejores prácticas para garantizar la protección de los recursos públicos y la continuidad de los servicios esenciales.
- La **Ley 80 de 1993 (Estatuto General de Contratación Pública)** obliga a las entidades a gestionar los recursos públicos con responsabilidad, lo que implica la adopción de estándares técnicos reconocidos que minimicen riesgos y optimicen el desempeño de las infraestructuras críticas.
- **La Ley 87 de 1993 (Control Interno)** exige mecanismos documentados para verificar la eficacia de los sistemas que garantizan la operación institucional.

3.1.3. Gestión de Riesgos y Continuidad Operativa

- La **Ley 1523 de 2012 (Gestión del Riesgo)** y la **Resolución 0312 de 2019 (SG-SST)** demandan que las entidades públicas implementen medidas proactivas para mitigar riesgos en infraestructuras críticas. Las normas internacionales, como **ASHRAE TC 9.9** y **ANSI/TIA-942**, ofrecen herramientas técnicas para cumplir con estas obligaciones y garantizar la estabilidad operativa.

3.1.4. Normas Nacionales Obligatorias Complementadas por Normas Internacionales

- **Reglamento Técnico de Instalaciones Eléctricas (RETIE):** Exige que todas las instalaciones eléctricas en Colombia, incluidas aquellas en centros de datos y sistemas de infraestructura crítica, cumplan con requisitos específicos de seguridad, eficiencia y sostenibilidad energética. Las normas internacionales, como ANSI/TIA-942, refuerzan el cumplimiento del RETIE al establecer estándares para la organización y cableado eléctrico seguro.
- **Norma Colombiana de Construcción Sismo Resistente (NSR-10):** Obliga a garantizar la estabilidad estructural y la protección contra riesgos físicos en edificaciones que alberguen infraestructuras críticas, como datacenters. Las normas como ASHRAE TC 9.9 complementan la NSR-10 al establecer lineamientos para la gestión ambiental y térmica en estos espacios.

3.1.5. Valor Técnico de las Normas Internacionales

- **ASHRAE TC 9.9:** Establece parámetros específicos para el control térmico y de humedad en datacenters, asegurando condiciones ambientales óptimas para evitar fallas en los sistemas tecnológicos.
- **ANSI/TIA-942:** Proporciona una guía integral para el diseño y operación de datacenters, incluyendo requisitos de cableado estructurado, control ambiental y redundancia.

- **BICSI 002:** Detalla mejores prácticas para la organización y etiquetado de cableado, mejorando la eficiencia del mantenimiento y reduciendo riesgos de incendios.
- **NFPA 10:** Regula el uso y mantenimiento de equipos de extinción de incendios, garantizando la seguridad en instalaciones críticas. En Colombia, esta regulación se complementa con la **NTC 2885**, la cual es obligatoria mediante la **Resolución 0312 de 2019 (SG-SST)**.
- **NFPA 75:** Estándar para la protección contra incendios de equipos de tecnología de la información y la
- **NFPA 76**: Estándar para la protección contra incendios de las instalaciones de telecomunicaciones.

3.2. Análisis de Riesgos

3.2.1. Revisión de Riesgos Institucionales

En esta sección se presenta el listado de los riesgos institucionales revisados en la auditoría, correspondiente a riesgos de Sistemas de Información, Gestión y Corrupción, del Proceso de Gestión de Tecnologías de la Información detallando su tratamiento, controles asociados, impacto, probabilidad y la valoración final del riesgo. Se incluyen también los planes de acción asociados, identificados mediante sus códigos y estado actual. Dicha información se tuvo en cuenta durante el desarrollo de la auditoria.

Tabla 1. Riesgos Institucionales asociados al proceso

Código	Riesgo	Tratamiento del Riesgo	Controles Asociados	Impacto	Probabilidad	Valoración del Riesgo	Planes Asociados	Estado del Plan
SYPDLI045	Pérdida de la disponibilidad de la infraestructura tecnológica	Implementación de plan de recuperación de desastres y sistemas de respaldo	**ID 493**: Plan de recuperación de desastres **ID 16**: Mantenimiento preventivo diario de sistemas eléctricos	Alto	Alta	80-80	**PA230-151**: Plan de tratamiento de riesgos **PA230-152**: Mejora de infraestructura	Pendiente / Pendiente
SYPDLI044	Pérdida de confidencialidad, integridad y disponibilidad de la información	Análisis de vulnerabilidades y Ethical Hacking anual	**ID 492**: Análisis de vulnerabilidades **ID 491**: Monitoreo de seguridad mensual **ID 494**: Control de acceso de usuarios	Mayor	Alta	80-80	**PA230-150**: Tratamiento de riesgos **PA230-154**: Mejora de seguridad informática	Pendiente / En ejecución
SYPDLI048	Pérdida de confidencialidad de la información pública clasificada o reservada	Validación mensual de usuarios y mejora en la gestión de accesos	**ID 494**: Validación mensual de usuarios **ID 1**: Monitoreo constante de acceso	Moderado	Media	60-60	**PA230-154**: Tratamiento de riesgos	Pendiente

Código	Riesgo	Tratamiento del Riesgo	Controles Asociados	Impacto	Probabilidad	Valoración del Riesgo	Planes Asociados	Estado del Plan
G034	Pérdida reputacional por quejas y sanciones debido a pérdida de disponibilidad de servicios de TI	Monitoreo de eventos de seguridad (SIEM) y fortalecimiento de la infraestructura	**ID 134**: Sistema SIEM de monitoreo **ID 12**: Mantenimiento preventivo diario de infraestructura	Alto	Alta	80-80	**PA230-153**: Tratamiento de riesgos **PA230-160**: Fortalecimiento de infraestructura	En ejecución / Pendiente
G033	Pérdida económica y reputacional por adquisición o construcción de soluciones informáticas no alineadas	Alineación de soluciones tecnológicas con los objetivos estratégicos y monitoreo de proyectos PETI	**ID 131**: Procedimiento formulación de planes **ID 132**: Seguimiento a proyectos PETI	Alto	Alta	80-80	**PA230-152**: Alineación tecnológica **PA230-155**: Aprobación de PETI	Pendiente / En ejecución
G032	Pérdida reputacional por requerimientos de usuarios internos de la Agencia	Formalización del proceso de solicitud y aprobación de desarrollos de software	**ID 128-130**: Procedimiento GTI-P-03 de solicitudes de TI **ID 494**: Automatización del proceso de asignación	Moderado	Media	60-60	**PA230-156**: Optimización del desarrollo de software	Pendiente
G018	Pérdida reputacional por afectación de las metas y objetivos institucionales	Monitoreo y seguimiento continuo del avance de las metas institucionales	**ID 136**: Control del seguimiento de metas mediante herramientas de monitoreo **ID 137**: Auditoría interna	Alto	Alta	80-80	**PA230-158**: Plan de fortalecimiento de monitoreo de metas	En ejecución
G001	Pérdida de confidencialidad, integridad o disponibilidad de la información por ataques cibernéticos	Implementación de firewalls avanzados y herramientas de detección de intrusiones	**ID 145**: Firewalls y detección de intrusiones **ID 146**: Pruebas de penetración anuales	Alto	Alta	80-80	**PA230-159**: Plan de seguridad cibernética	En ejecución

Fuente: Elaboración propia, con información de Daruma

3.3. Evaluación de Sistemas Críticos

En cuanto a este aspecto se procedió a verificar como objetivo la capacidad del entorno tecnológico para soportar los sistemas críticos utilizados en la operación, incluyendo su disponibilidad, redundancia, y las medidas de seguridad física y lógica aplicadas.

3.3.1. Certificaciones y Cumplimiento Normativo de Datacenter Principal

3.3.1.1. Elementos revisados:

- Certificación UPTIME Tier del Data Center
- Certificaciones ISO/IEC 27001 (Seguridad de la Información) y ISO/IEC 20000 (Gestión de Servicios TI)
- Contrato CCE 308 AMP 2022 Acuerdo Marco para la adquisición de servicios de Nube Privada IV y OC121005 Centro de Datos

3.3.1.2. Evaluación:

- Certificación del Data Center: Se verificó que el proveedor de servicios del Data Center externo contratado posee una certificación TIER IV conforme a la documentación presentada. Este nivel asegura un 99.999% de disponibilidad, lo que representa un estándar de clase mundial para garantizar la continuidad operativa.
- ISO/IEC 27001 e ISO/IEC 20000: La verificación de los documentos muestra que el proveedor cumple con las normativas de seguridad de la información y gestión de servicios TI según lo exigido por las certificaciones.

3.3.1.3. Recomendaciones:

- **Revisión Anual de vigencia del Acuerdo marco de precios**: En el contexto de los contratos suscritos bajo el Acuerdo Marco de Precios de Colombia Compra Eficiente para el servicio de Datacenter, es importante considerar que estos acuerdos, aunque válidos en su origen, pueden caducar antes de que finalicen los contratos individuales con los proveedores. Para mitigar cualquier riesgo de no conformidad con las normativas de seguridad y gestión de servicios TI, se recomienda que la Entidad solicite anualmente al proveedor evidencia de la renovación y vigencia de sus certificaciones en seguridad y calidad de los servicios. Esta solicitud debería formar parte de las obligaciones contractuales continuas, para asegurar que el proveedor siga cumpliendo con los requisitos técnicos y normativos establecidos, incluso si el AMP ya no está vigente. De hecho el AMP CCE-308AMP-2022 de la Tienda Virtual del Estado Colombiano (“TVEC”); inició la operación a partir del 30 de diciembre de 2022 y termina el 30 de diciembre de 2024

3.3.1.4. Evidencia documental:

- **Certificación TIER IV** confirmada en contrato **CCE-308**
- Certificación de cumplimiento de **ISO/IEC 27001** y **ISO/IEC 20000** confirmada en contrato **OC121005 Centro de Datos**

3.3.2. Disponibilidad y Redundancia del Servicio de Data Center Remoto

3.3.2.1. Elementos revisados:

- SLA (Service Level Agreement) o ANS (Acuerdo de Niveles de Servicio), contratos de servicios (CCE-308), y documentos de monitoreo de disponibilidad de servicios.

3.3.2.2. Evaluación:

El SLA revisado garantiza una disponibilidad de 99.99%, con redundancias eléctricas y de conectividad. Durante la revisión del contrato CCE-308 se identificó que el proveedor garantiza redundancias eléctricas mediante generadores de emergencia con capacidad para 72 horas y sistemas de alimentación ininterrumpida (UPS). Además, las líneas de conectividad están diseñadas con enlaces redundantes para asegurar la continuidad en caso de una falla en los enlaces primarios.
En cuanto a las Capacidades energéticas: se comprobó que el proveedor asegura una capacidad eléctrica de 4 KVA por rack, lo cual es adecuado para los servidores alojados.

3.3.2.3. Recomendaciones:

Pruebas periódicas de redundancia: Es esencial que en conjunto con el proveedor se realicen pruebas periódicas de los sistemas de respaldo eléctrico y de conectividad, las cuales deberían ser reportadas de forma continua a la entidad para evitar posibles interrupciones.

3.3.2.4. Evidencia documental:

- SLA y contrato **CCE-308** donde se especifican las capacidades eléctricas y de conectividad del servicio.
- Documentos de monitoreo de disponibilidad de servicios, donde se reporta un tiempo de disponibilidad del **99.97%** entre junio y agosto de 2024

3.3.3. Seguridad Física y Lógica

3.3.3.1. Elementos revisados:

- Políticas de control de acceso físico
- Auditorías de seguridad lógica (CCE-308)
- Bitácoras de acceso al Data Center

3.3.3.2. Evaluación:

- **Seguridad física**: El contrato especifica los controles de acceso biométrico y los seis anillos de seguridad física con monitoreo **24/7** que protege la infraestructura del Data Center. El sistema de vigilancia incluye cámaras de monitoreo **360°** y personal de seguridad en puntos críticos. Las auditorías de seguridad lógica realizadas, relacionadas con el contrato CCE-308, muestran un cumplimiento adecuado en cuanto a protección de acceso a los sistemas.
- **Seguridad lógica**: El sistema incluye autenticación multifactor para acceso remoto y firewalls configurados en alta disponibilidad (HA).

  Se encontraron 2 firewalls Fortigate en la Sala de Comunicaciones del tercer piso de las instalaciones de la Entidad. En Fortisiem están implementados 75 activos, Controles Empresariales - COEM realiza monitoreo, las reglas de uso las monitorea Controles Empresariales - COEM, el caso se reporta al Oficial de seguridad y se toman

las acciones pertinentes; se presentan alrededor de 25 a 30 casos mensuales que requieren acciones de contención, mitigación y/o erradicación.

Se realizan reuniones casi diarias con Controles Empresariales - COEM por el Oficial de Seguridad y se elabora un informe mensual, por correo electrónico, se hacen las notificaciones de casos GLP (Aplicativo mesa de servicios) y se diligencia el formato GTI-F-10 SOLICITUD DE CAMBIOS RFC (Request For Change) y se genera un ticket.

3.3.3.3. Recomendaciones:

- Se recomienda realizar auditorías trimestrales de los logs de acceso y establecer indicadores para fortalecer el control sobre accesos no autorizados físicos y lógicos.
- Dado que los Firewalls Fortinet se encuentran en una sala de comunicaciones de la sede de la entidad, junto con servidores y unidades de almacenamiento en red, es necesario que dicha sala cuente con las recomendaciones y especificaciones de la norma BICSI 02 y se tenga una redundancia en el Datacenter remoto.

3.3.3.4. Evidencia documental:

- Bitácoras de acceso al Data Center que confirman el control de acceso físico y los registros de seguridad.

3.3.4. Sala de cableado Segundo Piso OASTI

3.3.4.1. Elementos revisados (Visita in situ):

Criterios de Auditoría Ajustados: Se revisaron las siguientes normativas y estándares aplicables:

- **Código Colombiano de Construcción Sismo Resistente (NSR-10):** Aplicable a infraestructuras críticas, establece requisitos para garantizar seguridad física y funcional.
- **Reglamento Técnico de Instalaciones Eléctricas (RETIE):** Requiere la certificación de todas las conexiones eléctricas en edificaciones.
- **Ley 1523 de 2012 (Gestión del Riesgo de Desastres):** Obliga a identificar y mitigar riesgos en infraestructuras críticas, como centros de telecomunicaciones, para prevenir emergencias como incendios.
- **Ley 1575 de 2012 (Ley General de Bomberos de Colombia):** Establece lineamientos generales para la prevención, protección y atención de incendios en el territorio nacional. Obliga a implementar medidas de seguridad contra incendios en edificaciones públicas y privadas, incluyendo el cumplimiento de reglamentos técnicos aplicables a cada tipo de instalación.
- **Resolución 0312 de 2019 - SG-SST**: Establece estándares mínimos para garantizar la seguridad y salud en áreas de trabajo, incluyendo infraestructura tecnológica.
- **NTC 2885 (Extintores Portátiles):** Regula los requisitos para la recarga, inspección y mantenimiento de extintores portátiles. Es obligatoria a través de la Resolución 0312 de 2019 (SG-SST).

- **Resolución 500 de 2021 del MinTIC:** establece lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). Este modelo orienta a las entidades públicas en la adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de gestionar adecuadamente el ciclo de vida de la seguridad de la información.
- **Código Nacional de Policía y Convivencia (Ley 1801 de 2016):** Regula la seguridad en edificaciones, exigiendo medidas preventivas contra incendios, especialmente en instalaciones con afluencia de público o almacenamiento de equipos críticos.
- **Buenas prácticas internacionales: BICSI 002, TIA-606-C,** (No obligatorias, pero recomendadas para la organización y etiquetado del cableado estructurado en centros de datos)
- **Registros de mantenimiento de equipos y extintores**.
- **Inspección física de cableado, instalaciones eléctricas, sistemas de seguridad y protección contra incendio**s.
- **Principio de Precaución (Constitución, Artículo 209):** Las entidades públicas deben actuar de manera preventiva frente a riesgos previsibles, adoptando medidas que minimicen las amenazas a la infraestructura y la continuidad de los servicios.

3.3.4.2. Evaluación:

- **Desorganización en el cableado**: El cableado no estaba debidamente organizado ni etiquetado. Se encontró enredado y no seguía el orden adecuado. Estableciéndose en el informe preliminar una **No Conformidad**
- **Material inflamable:** Se encontraron cajas de cartón almacenadas cerca de los equipos electrónicos, representando un alto riesgo de incendio. Estableciéndose en el informe preliminar una **No Conformidad**
- **Conexiones eléctricas no certificadas:** Se detectaron conexiones eléctricas no certificadas conforme a RETIE, con instalaciones improvisadas y hoyos en las paredes. Estableciéndose en el informe preliminar una **No Conformidad**
- **Extintor vencido:** El extintor de dióxido de carbono tiene vencimiento en junio de 2024. Incumpliendo la NORMA TÉCNICA COLOMBIANA NTC 2885 que se hace obligatoria a través de la Resolución 0312 de 2019 (SG-SST)
- La norma anteriormente citada está vigente y es obligatoria, en virtud de la norma sismorresistente NSR-10 establecida en la ley 400 de 1997 y por ende en el SGSST, no se ha documentado su inspección recientemente, por lo cual se configura en el informe preliminar una **No Conformidad**
- **Seguridad física con llave:** El acceso a la sala está controlado mediante una chapa con llave, lo cual no garantiza un nivel de seguridad óptimo para esta área crítica. Estableciéndose en el informe preliminar una **Observación.**

3.3.4.3. Respuesta del líder del proceso auditado al informe preliminar respecto a la Desorganización en el cableado:

"Las normas BICSI 002 y TIA-606-C no son de obligatorio cumplimiento para la Agencia, de acuerdo con la normativa de Mintic. De igual manera todas las conexiones eléctricas certificadas están siendo utilizadas exclusivamente para la infraestructura de TI, que incluye servidores, dispositivos de red y otros equipos críticos. Las conexiones no certificadas no se utilizan para soportar ninguna de las funciones relacionadas anteriormente y se realiza los mantenimientos correspondientes.

Por lo anterior, respetuosamente se solicita ajustar la NO CONFORMIDAD a una RECOMENDACIÓN, ya que la Agencia no está sujeta a la normatividad BICSI 002 y TIA-606-C. No obstante, se acoge la recomendación de mejorar la organización del cableado."

3.3.4.4. Análisis de Respuesta de la OASTI:

En su respuesta, la OASTI reconoció que el cableado requiere mejoras y aceptó reorganizarlo siguiendo las mejores prácticas de la industria. Asimismo, informó que **las conexiones eléctricas no certificadas no están siendo utilizadas para funciones críticas**. No obstante, no aportó evidencia sobre medidas documentadas que respalden estas afirmaciones. De igual manera se estableció por parte de esta oficina que la normativa de MINTIC se refiere al MSPI especialmente la **Resolución 500 de 2021.**

Teniendo en cuenta la respuesta de la OASTI, **la auditoria se ratifica en la No conformidad**. Esto considerando que, al momento de la auditoría, se encontraron situaciones que representan riesgos latentes para la seguridad y continuidad operativa de los cuales no se aporta evidencia de que se hayan subsanado. Cabe anotar que, aunque la Agencia asegura no estar obligada a cumplir con las normas BICSI 002 y TIA-606-C, aunque si el Reglamento Técnico de Instalaciones Eléctricas (RETIE), las mismas constituyen mejores prácticas aplicables y de acuerdo con la **Resolución 500 de 2021** del MinTIC que establece lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). Este modelo orienta a las entidades públicas en la adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de gestionar adecuadamente el ciclo de vida de la seguridad de la información. En cuanto a la mejora de la organización del cableado sugerida por la OASTI en su respuesta, es válida su formulación como parte del plan de mejoramiento sobre este asunto.

3.3.4.5. Respuesta del líder del proceso auditado al informe preliminar a la Presencia de material inflamable en área crítica

"Las normas NFPA 75 y NFPA 76 no son de obligatorio cumplimiento para la Agencia, de acuerdo con la normativa de MINTIC. Por lo anterior, se solicita respetuosamente cambiar la NO CONFORMIDAD por una OBSERVACIÓN o RECOMENDACIÓN. Se acogió la recomendación con el retiro del sitio del material identificado. "

3.3.4.6. Análisis de Respuesta del Auditado:

El líder del proceso argumentó que las normas **NFPA 75** y **NFPA 76** no son de obligatorio cumplimiento para la Agencia, y solicitó cambiar la No Conformidad por una Observación o Recomendación, destacando que el material inflamable ya fue retirado.

Sin embargo, este argumento no elimina la responsabilidad de garantizar controles efectivos en el almacenamiento, dado que:

- La **Resolución 0312 de 2019 (SG-SST)** obliga a mantener espacios libres de riesgos previsibles como incendios.
- La **Ley 1523 de 2012** exige medidas de prevención en infraestructuras críticas.
- Aunque las normas NFPA no sean obligatorias, representan buenas prácticas internacionales ampliamente adoptadas así: la NFPA 72 en lo referente a detección, instalación y mantenimiento; la NFPA 13 y 20 para todo lo referente a extinción a base de agua; la NFPA 2001 para los sistemas de Extinción a base de Agente Limpio; la NFPA 12 para los sistemas de extinción en base a CO2; la NFPA 75 estándar para la protección contra incendios de equipos de tecnología de la información y la NFPA 76 es el estándar para la protección contra incendios de las instalaciones de telecomunicaciones.

Luego de analizar el hallazgo y la respuesta del auditado, **se reclasifica la No Conformidad como Observación**, considerando que la situación ya fue subsanada, debido a que el material inflamable fue retirado. Sin embargo, es necesario resaltar que debe fortalecerse el control para estos riesgos.

3.3.4.7. Recomendaciones:

Se recomienda a la OASTI que se tomen medidas correctivas mencionadas en su respuesta, y con el objeto de que no se repitan sean documentadas mediante un procedimiento, instructivo o protocolo formal. Se sugiere:

- La reorganización del cableado conforme a estándares reconocidos.
- Certificación de las conexiones eléctricas según RETIE.
- Inspecciones regulares para garantizar el cumplimiento continuo de los estándares de seguridad.

Se recomienda que las acciones tomadas frente al material inflamable queden debidamente documentadas en un protocolo oficial y sean monitoreadas de forma continua.

3.3.4.8. Frente al Hallazgo Extintores vencidos y equipos inadecuados en salas críticas ver Numeral 3.3.6 (antiguo 3.2.6)

3.3.4.9. Evidencia:

Fotografía del cableado.

- Fotografía de las cajas de cartón almacenadas.
- Fotografía de las conexiones eléctricas improvisadas.
- Fotografía del extintor con fecha de vencimiento visible.
- Fotografía de la puerta con chapa de llave.

3.3.5. Sala Segundo Piso Secretaría General

3.3.5.1. Elementos revisados (Visita in situ):

Criterios de Auditoría Revisados: Se revisaron las siguientes normativas y lineamientos aplicables:

- **Código Colombiano de Construcción Sismo Resistente (NSR-10):** Establece requerimientos mínimos de seguridad para proteger infraestructuras críticas, incluyendo controles de acceso físico**.**
- **Resolución 0312 de 2019 - SG-SST:** Define estándares mínimos de seguridad y salud en el trabajo aplicables a espacios de trabajo, incluyendo áreas tecnológicas y su control de accesos.
- **Normativa interna – Instructivo GTI-I-01 (No vigente)** Formato GTI-F-08 (Bitácora de Ingreso al Centro de Datos) para registrar entradas y salidas.
- **Buenas prácticas internacionales: ,** (No obligatorias, pero recomendadas para la organización y seguridad en centros de datos) Normativa técnica: BICSI 002, TIA-606-C.
- Registros de mantenimiento de extintores.
- Inspección física del estado de limpieza, cableado y seguridad.

3.3.5.2. Evaluación:

- **Cableado bien organizado**: Cumple con las normativas BICSI 002 y TIA-606-C. El cableado está debidamente etiquetado y colocado en canaletas.
- **Extintor multipropósito:** El extintor tiene vencimiento en agosto de 2025. Aunque está en buen estado, no se ha documentado su inspección reciente y no es el más adecuado para equipos electrónicos y eléctricos. Estableciéndose una **Observación**. Los extintores de agentes limpios, como FM-200 o Novec 1230, son más adecuados para proteger equipos electrónicos sensibles.
- Sala de comunicaciones sucia, sin material inflamable: Aunque no se encontraron materiales inflamables, la sala presentaba suciedad acumulada que puede afectar el rendimiento de los equipos. Estableciéndose una **Observación**
- Seguridad física con llave: El acceso a la sala está controlado mediante una chapa con llave, lo cual no garantiza un nivel de seguridad óptimo para esta área crítica. Como tampoco se lleva un registro de entradas y salidas. Estableciéndose en el informe preliminar una **No Conformidad** frente al INSTRUCTIVO DE CONTROL DE ACCESOS A CENTRO DE DATOS GTI-I-01 y el diligenciamiento del formato GTI-F-08 Bitácora de Ingreso al centro de datos.

3.3.5.3. Respuesta del líder del proceso auditado:

"Se aclara que el instructivo GTI-I-01: INSTRUCTIVO DE CONTROL DE ACCESOS A CENTRO DE DATOS fue retirado de la OASTI el 25/07/2024. Además, dicho instructivo no contenía elementos relacionados con la afirmación de que "el control de acceso está limitado a una chapa con llave en áreas de fácil acceso de la entidad, según evidencia fotográfica lo que incumple con las normativas internas de seguridad como el Instructivo GTI-I-01". El propósito del GTI-I-01 era "proporcionar orientaciones para el acceso al centro de datos de la ANDJE, describiendo los aspectos que deben tenerse en cuenta para el ingreso a esta zona, con el fin de controlarlo y obtener un registro de las acciones realizadas por el personal autorizado que ingrese." Es importante indicar que el área administrativa confirma que la sala permanece cerrada y la llave está en custodia en el área.

Por lo anterior, solicitamos respetuosamente el retiro de la NO CONFORMIDAD."

3.3.5.4. Análisis de Respuesta de la OASTI:

En su respuesta, la OASTI reconoce que las salas carecían de control adecuado de acceso y señala que se encuentra en proceso de revisión y actualización del **Instructivo GTI-I-01**, con el objetivo de implementar medidas más efectivas. Asimismo, indica que se han iniciado ajustes en las políticas de operación para reforzar los controles, aunque no se entrega evidencia de un procedimiento formalizado que sustituya al instructivo vigente.

Teniendo en cuenta la respuesta de la OASTI, **se retira la no conformidad y se reclasifica como una observación** a la presentación de la evidencia del nuevo procedimiento. Esto considerando que al momento de la verificación se encontraron puertas sin llave y la ausencia de registro en la bitácora de ingreso por parte del auditor. Se precisa que el período auditado fue de enero a junio por lo que el Instructivo GTI-I-01 se encontraba vigente.

3.3.5.5. Recomendaciones:

Se recomienda que las medidas correctivas mencionadas por la OASTI sean formalizadas mediante un procedimiento, instructivo o protocolo actualizado, incluyendo:

- La actualización y documentación del **Instructivo de Control de Accesos a Centros de Datos (GTI-I-01)** o su equivalente.
- La inclusión de controles para garantizar que el formato **GTI-F-08** sea diligenciado por todo personal que acceda a las salas.
- Establecer sanciones o medidas correctivas en caso de incumplimientos del instructivo.
- **Seguimiento pendiente:** Dado que no se entregó evidencia del nuevo procedimiento o su equivalente que lo contenga, se infiere que este se encuentra en desarrollo dentro de las políticas de operación, según lo consignado en Daruma. Se recomienda que, una vez implementado, se realice una auditoría de seguimiento para verificar su eficacia y cumplimiento.

3.3.5.6. Evidencia documental (fotográfica):

- Fotografía del cableado bien organizado.
- Fotografía del extintor multipropósito con fecha de vencimiento visible.
- Fotografía del estado de suciedad en la sala.
- Fotografía de la puerta con chapa de llave.

3.3.6. Sala de Comunicaciones Tercer Piso

3.3.6.1. Elementos revisados (Visita in situ):

Criterios de Auditoría Revisados: Se evaluaron las siguientes normativas y estándares aplicables:

- **Código Colombiano de Construcción Sismo Resistente (NSR-10):** Regula las condiciones estructurales de edificios que albergan sistemas críticos, incluyendo los requerimientos de infraestructura para sistemas de climatización.
- **Resolución 0312 de 2019 - SG-SST:** Establece estándares de seguridad y salud en el trabajo aplicables a áreas técnicas, incluyendo control ambiental y protección de infraestructura tecnológica.
- **Ley 1562 de 2012:** Exige a las entidades implementar medidas preventivas que aseguren la protección de personas e infraestructura en el trabajo, incluyendo equipos contra incendios**.**
- **Resolución 2749 de 2017:** establece disposiciones relacionadas con la prohibición, eliminación y manejo adecuado de las sustancias que agotan la capa de ozono
- **Ley 80 de 1993 (Estatuto General de Contratación Pública):** Obliga a las entidades públicas a aplicar principios de eficiencia, eficacia y responsabilidad en el uso de recursos públicos.
- **Ley 87 de 1993 (Control Interno):** Exige prevenir riesgos y garantizar la protección de los recursos, adoptando estándares que minimicen vulnerabilidades operativas.
- **Resolución 0312 de 2019 (SG-SST):**
  - Exige la identificación, evaluación y control de riesgos relacionados con incendios en el marco del Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST).
  - Obliga a implementar medidas para prevenir y mitigar riesgos de incendio, incluyendo la inspección y mantenimiento de equipos de extinción.
- **NTC 2885 (Extintores Portátiles):**
  - Regula los requisitos para la recarga, inspección y mantenimiento de extintores portátiles.
  - Es obligatoria a través de la Resolución 0312 de 2019 (SG-SST).
- **Buenas prácticas internacionales (No obligatorias):**
  - **ASHRAE TC 9.9:** Guía de referencia para control térmico y de humedad en Datacenters.

- **BICSI 002:** Estándares de diseño y operación para infraestructuras críticas, incluyendo disposición de cableado, gestión de pasillos frío/caliente y equipos de precisión.
- **Registros de equipos de UPS y sistemas de aire acondicionado.**
- **Registros de mantenimiento de extintores.**
- **Se identifico la presencia de equipos firewall, servidores y unidades de almacenamiento en red en esta sala**
- **Extintores**
- **Sistema de Aire Acondicionado**
- **Dotación del Centro de Comunicaciones**

3.3.6.2. Evaluación:

- Desorden en el cableado detrás de los racks: Se observó desorden en el cableado ubicado detrás de los racks de servidores, lo que dificulta el mantenimiento y aumenta el riesgo de desconexiones accidentales. Es decir que, no se cumple con las mejores prácticas de organización de éste, establecidas por BICSI 002, que sugieren la instalación en canaletas para una gestión más eficiente. Estableciéndose en el informe preliminar una **No Conformidad** frente a las normas ANSI/TIA-942: Exige cableado estructurado y organizado en centros de datos para facilitar el mantenimiento y reducir riesgos de desconexiones., BICSI 002: Recomienda el uso de canaletas y soportes para mantener el cableado ordenado, minimizando el riesgo de errores y desconexiones accidentales., NTC 2050 (Código Eléctrico Colombiano): Basado en NFPA 70, requiere una adecuada gestión del cableado para evitar riesgos eléctricos en instalaciones críticas., NTC 5001 (SG-SST): Exige orden y seguridad en el lugar de trabajo, ya que el desorden aumenta el riesgo de fallos y accidentes
- Pasillo frío mal ubicado: El pasillo frío, que debe estar frente a los equipos para optimizar el flujo de aire y mejorar la refrigeración, está ubicado incorrectamente detrás de los racks. Esto afecta la eficiencia del sistema de enfriamiento y puede causar sobrecalentamiento en los equipos críticos, ya que el flujo de aire frío no está dirigiéndose correctamente a los servidores. Estableciéndose en el informe preliminar una **No Conformidad** frente a las normas: ANSI/TIA-942: Requiere la disposición de pasillos fríos frente a los equipos para optimizar la eficiencia de enfriamiento en centros de datos., ASHRAE TC 9.9: Establece directrices para la correcta circulación de aire frío y caliente, esencial para evitar sobrecalentamiento y mantener la eficiencia energética., NFPA 75: Incluye recomendaciones de diseño de ventilación y enfriamiento para proteger equipos de tecnología crítica. NTC 5001 (SG-SST en Colombia): Exige medidas para prevenir riesgos térmicos que podrían afectar la seguridad y disponibilidad de los equipos
- UPS con estado de banco de baterías externo e interno desconocido: El sistema de alimentación ininterrumpida (UPS) tiene un banco de baterías externas con 32 baterías, pero no se dispone de Etiquetas de Identificación en el Equipo, la UPS y su banco de baterías deben contar con etiquetas o placas visibles que indiquen el

tipo de baterías, cantidad, voltaje, y fecha del último mantenimiento realizado, para rápida referencia en sitio. Esto representa un riesgo, ya que la falta de mantenimiento o conocimiento de las baterías internas podría resultar en fallos imprevistos. Estableciéndose en el informe preliminar **una Observación** frente a las normas RETIE (Colombia) - Reglamento Técnico de Instalaciones Eléctricas:

- Exige seguridad, certificación y etiquetado adecuado en equipos eléctricos, aplicable a sistemas críticos como UPS en Colombia.
- Se encontró un Aire acondicionado de confort Mini Split YORK RVEC24DS-ADR en lugar de aire acondicionado de precisión, el instalado es de confort, diseñado para uso general, lo cual no es adecuado para centros de datos que deben ser de precisión. Además, no se cuenta con un medidor independiente de temperatura y humedad en cada pasillo para controlar las condiciones ambientales de manera efectiva. **Estableciéndose** en el informe preliminar **una Observación** frente a las normas y buenas prácticas de diseño de centro de datos ANSI/TIA-942: Incumplimiento de los requisitos para el control ambiental en centros de datos., NFPA 75: Falta de un control ambiental adecuado que podría incrementar el riesgo de sobrecalentamiento y, potencialmente, de incendio., ASHRAE TC 9.9: Falta de un sistema adecuado para mantener los parámetros recomendados de temperatura y humedad y la ISO/IEC 22237: No se cumple con los requisitos de control ambiental especificados para centros de datos**.**
- Extintor vencido en junio de 2024: El extintor de dióxido de carbono tiene una fecha de vencimiento de junio de 2024, por lo cual debe ser revisado y asegurar un mantenimiento regular antes de su vencimiento. Estableciéndose en el informe preliminar una **Observación** frente a las mejores prácticas de la norma La NFPA 75 - Standard for the Fire Protection of Information Technology Equipment y el **NTC 2050** (Código Eléctrico Colombiano) así como frente al Sistema de Gestión de Seguridad y Salud en el Trabajo o SG-SST.
- Seguridad biométrica sin registro de accesos: Aunque el acceso a la sala es mediante un sistema biométrico, no se lleva un registro de entradas y salidas, estableciéndose una **No Conformidad** frente al INSTRUCTIVO DE CONTROL DE ACCESOS A CENTRO DE DATOS GTI-I-01 y el diligenciamiento del formato GTI-F-08 Bitácora de Ingreso al centro de datos.

3.3.6.3. Respuesta del Lider del Proceso Auditado Frente a la No Conformidad “Sistemas de Refrigeración Inadecuados” en La Sala de Comunicaciones 3er Piso

“Las normas ASHRAE TC 9.9 y BICSI 002 no son de obligatorio cumplimiento para la Agencia, de acuerdo con la normativa de Mintic. Por lo anterior y respecto a la afirmación: “La auditoría evidenció que el pasillo frío estaba mal ubicado, detrás de los racks en lugar de estar frente a los equipos, afectando la eficiencia del sistema de enfriamiento y aumentando el riesgo de sobrecalentamiento”, se aclara que con base en el análisis realizado conjuntamente con el ingeniero Ramiro Rivera de la firma FAMOC en visita realizada el 14 de noviembre, se determinó que el sistema de refrigeración abarca la totalidad del centro de datos y que su ubicación fue diseñada

de acuerdo con los parámetros técnicos requeridos para mantener una adecuada distribución del aire frío y caliente. Adicionalmente, no se han presentado incidentes de sobrecalentamiento ni fallas relacionadas con el sistema de enfriamiento, lo que indica que su funcionamiento es efectivo.

Asimismo, cabe destacar que el sistema de climatización utilizado no es de tipo confort, el utilizado cumple con los requerimientos técnicos necesarios según las características del centro de datos. De igual manera, aunque las normativas ASHRAE TC 9.9 y BICSI 002 no son de obligatorio cumplimiento, la Agencia se asegura que se implementan buenas prácticas tanto en el centro de datos de la Agencia como en el centro de datos externo que aloja la infraestructura crítica, el cual cumple con los estándares de un centro de datos TIER 4.

Por lo anterior, solicitamos respetuosamente el retiro de la NO CONFORMIDAD."

3.3.6.4. Análisis de Respuesta de la OASTI

La Evidencia aportada fue la siguiente:

- Concepto técnico del Ingeniero Ramiro Rivera, operador del edificio (Famoc Depanel), que sostiene que los equipos instalados son suficientes para la operación. Sin embargo, no se presentaron memorias de cálculo o documentación técnica que respalden dicha afirmación.
- No se presenta ficha técnica del equipo de Aire Acondicionado que establezca que se trata de un equipo de precisión. (esto es, flujo volumétrico adaptado a diferencia de temperatura ΔT=5–7°C) ,control térmico de ±0.5 °C o menos, Humedad relativa entre 40%-60%, Índice de Eficiencia Energética – IEE > 10) y bajo condiciones de la ciudad de Bogotá. (derrateo por altitud)
- Los requisitos de control de temperatura y humedad para equipos de aire acondicionado de precisión se definen así:
- La norma BICSI 002 establece directrices para el diseño e implementación de centros de datos, incluyendo requisitos de enfriamiento y control ambiental. Algunos puntos relevantes son:
  Flujo Volumétrico: Adaptado a una diferencia de temperatura ΔT=5–7°C.
  Control Térmico: Precisión de ±0.5 °C o menos.
  Humedad Relativa: Controlada entre 40%-60%.
  Índice de Eficiencia Energética (IEE): Mayor a 10.
  Se pueden consultar más detalles en el documento BICSI 002-2019 https://www.bicsi.org/docs/default-source/publications/002-2019-preview.pdf
- La norma ASHRAE TC 9.9 proporciona directrices para el control de temperatura y humedad en centros de datos. Algunos puntos relevantes son:
  Temperatura: Rango recomendado de 18°C a 27°C.
  Humedad Relativa: Rango recomendado de 40% a 60%.
  Precisión Térmica: Control de temperatura con una precisión de ±0.5 °C.

Eficiencia Energética: Recomendaciones para mejorar la eficiencia energética en sistemas de enfriamiento.
Se pueden consultar más detalles en el documento ASHRAE TC 9.9. ASHRAE_TC0909_Power_White_Paper_22_June_2016_REVISED.pdf

- Se estableció por parte de esta oficina que la "**normativa de Mintic"** mencionada por el auditado se refiere al MSPI especialmente la **Resolución 500 de 2021** que establece lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

3.3.6.4.1. Validación del Auditor

A partir de lo argumentado por el área auditada se procedió a realizar validación de los equipos instalados, encontrando que no cumplen con los estándares ASHRAE TC 9.9 ni BICSI 002 (mejores prácticas) de acuerdo con las especificaciones que aparecen en las etiquetas de los equipos instalados y las especificaciones en los catálogos y manuales de Johnson Controls de 2007 ref. E-CAT-G2007 para equipos Split High Wall Everest Marca. York, confirmando que se trata de un equipo de confort. Adicionalmente, se confirman las inconsistencias citadas frente a la ubicación del flujo de aire (pasillos frío/caliente), lo que genera riesgos operativos como puntos calientes y recirculación de aire.

Sobre el particular se identificó que **e**xiste una disparidad de criterios técnicos en las políticas de operación del proceso, ya que la entidad ha contratado un Datacenter externo (nebula -HostDime) con certificación TIER IV (máxima categoría de disponibilidad y redundancia), mientras que el Datacenter interno no cumple con estándares básicos de la industria, desconociendo los principios de eficiencia y responsabilidad en el manejo de recursos públicos, como lo exige la Ley 80 de 1993.

La **Resolución 500 de 2021** que establece lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). Este modelo orienta a las entidades públicas en la adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de gestionar adecuadamente el ciclo de vida de la seguridad de la información.

Por lo tanto, se define como una **Observación** y se recomienda analizar alternativas para la debida instalación y cuidado de los equipos críticos, como su reubicación en el Datacenter contratado o mejorar las condiciones de operación en la sede de la Agencia.

3.3.6.5. Respuesta del Lider del Proceso Auditado sobre los "Extintores Vencidos o No Adecuados":
"Los extintores se encontraban en proceso de recarga y mantenimiento por parte del área administrativa en el momento de la verificación. A la fecha, esta actividad fue realizada y los extintores se encuentran vigentes."

3.3.6.6. Análisis de la Respuesta del Auditado:

El líder del proceso informó que los extintores estaban en proceso de recarga y mantenimiento al momento de la verificación, y actualmente se encuentran vigentes. Sin embargo, al momento de la verificación no se evidenciaba protección adecuada de las áreas, encontrándose:

- **Falta de controles preventivos:** La respuesta no aborda el incumplimiento del protocolo de mantenimiento y recarga (NTC 2885), Según la Resolución 0312 de 2019, las áreas críticas no deben quedar desprotegidas mientras los extintores están en proceso de recarga. Se deben instalar **extintores temporales** de capacidad y características equivalentes en los lugares donde se hayan retirado los equipos para recarga o mantenimiento. que exige mantener equipos alternativos mientras se realiza el proceso, evitando dejar áreas críticas desprotegidas. En el caso de la Agencia ya sea en los protocolos establecidos para el Grupo Interno de Trabajo Gestión Administrativa y Financiera, la OASTI o el Operador FAMOC.
- **Inadecuación de equipos:** No se presenta evidencia que justifique el uso de extintores de CO2 en espacios cerrados, ni un análisis que considere alternativas más seguras para las áreas críticas.

Después de analizar el hallazgo y la respuesta del auditado, **se define como Observación** debido a:

- La falta de controles preventivos en el mantenimiento y recarga de extintores, lo que dejó áreas críticas sin protección temporal adecuada pero que actualmente se encuentran vigentes
- El uso inadecuado de equipos como extintores de CO2 en espacios cerrados, que podrían representar un riesgo de asfixia para el operador a menos que cuente con un equipo de respiración autónoma (SCBA- mascara de oxígeno de protección personal y botella de rescate.) representa un riesgo latente para el operario.
- Se recomienda evitar la futura implementación de extintores Solkaflam debido a las restricciones normativas sobre el HCFC-123.(extintores de Color Blanco) que contraviene la normatividad ambiental **Resolución 2749 de 2017**

3.3.6.7. Respuesta del Líder del Proceso Auditado Frente a la Observación Numeral 3.2.6: Ausencia de Medidores de Temperatura y Humedad en la Sala de Comunicaciones (Datacenter) del 3er Piso:

"Las normas ANSI/TIA-942 y ASHRAE TC 9 no son de obligatorio cumplimiento para la Agencia, de acuerdo con la normativa de Mintic. Asimismo, se aclara que las verificaciones de temperatura se realizan a través del monitoreo específico de cada componente tecnológico, los cuales emiten alertas en caso de que la temperatura no sea adecuada para su funcionamiento. "

3.3.6.8. Análisis de la Respuesta del Auditado:

- **Insuficiencia de los sistemas internos de alerta:**
  Los sistemas integrados en los equipos no sustituyen a medidores independientes para el monitoreo ambiental. Esto limita la capacidad de detectar y anticiparse a condiciones adversas, como fluctuaciones de temperatura o niveles de humedad que puedan afectar la infraestructura tecnológica en caso de mal funcionamiento del componente tecnológico.
- **Normas superiores de la administración pública:**
  Las normas nacionales, como la Ley 1523 de 2012, exigen medidas proactivas para la gestión de riesgos. La ausencia de monitoreo específico constituye una omisión en el cumplimiento de estas obligaciones.
  Los principios constitucionales de eficiencia y eficacia (artículo 209 de la Constitución) obligan a la administración pública a seguir las mejores prácticas de la industria, especialmente en la gestión de recursos críticos como los Datacenters.
  Por lo tanto, se encuentra su aplicación en las **Normas:**
  BICSI 002-2014:
  Sección 7.3.3.2: Esta sección aborda la importancia de monitorear las condiciones ambientales, incluyendo la temperatura y la humedad, para asegurar el funcionamiento óptimo del equipo en centros de datos
  ASHRAE TC9.9:
  Capítulo 4: Este capítulo de la Guía Térmica para Ambientes de Procesamiento de Datos de ASHRAE destaca la necesidad de mantener rangos específicos de temperatura y humedad para la eficiencia y fiabilidad del equipo, la Tabla 1 de dicha norma: Proporciona los límites recomendados de temperatura y humedad para equipos de TI en centros de datos.

  Por lo tanto, se mantiene la **Observación**, y se efectúan las siguientes:

3.3.6.9. Recomendaciones:

- Reorganizar el cableado detrás de los racks: El cableado desorganizado debe colocarse adecuadamente en canaletas o racks específicos para cables, conforme a las normas BICSI 002. Esto facilitará el mantenimiento, reducirá el riesgo de desconexiones accidentales y mejorará la accesibilidad a los equipos.
- Reubicar el pasillo frío de frente a los equipos: El pasillo frío debe estar ubicado de frente a los servidores y racks de equipos, lo que permitirá que el aire frío se distribuya eficientemente, manteniendo los equipos a temperaturas óptimas y reduciendo el riesgo de sobrecalentamiento. Reorganizar la disposición de los racks es una prioridad para corregir esta deficiencia.
- Inspeccionar el UPS y obtener información completa del banco interno de baterías: Es necesario realizar una inspección técnica del UPS para identificar el estado del banco de baterías internas, documentar su cantidad y condición, y planificar el mantenimiento adecuado para evitar fallos inesperados.

- Reemplazar el aire acondicionado de confort por uno de precisión: Se recomienda instalar un aire acondicionado de precisión, diseñado específicamente para centros de datos, que mantenga una temperatura y humedad constantes. También se debe agregar un medidor independiente de temperatura y humedad para monitorear el ambiente en todo momento y garantizar que las condiciones sean óptimas para los equipos.
- Se debe realizar una inspección inmediata del extintor de dióxido de carbono (CO_2), asegurando que esté en condiciones óptimas de funcionamiento. El CO2 es un gas limpio que extingue el fuego eliminando el oxígeno. Es muy eficaz, pero su uso en áreas cerradas debe ser manejado con cuidado, ya que puede ser peligroso para las personas debido al desplazamiento del oxígeno en el ambiente debiéndose cumplir con lo establecido en el SGSST. Considerando el entorno crítico de la sala de comunicaciones, se recomienda la revisión del tipo de extintor instalado. Los extintores de agentes limpios, como FM-200 o Novec 1230, son más adecuados para proteger equipos electrónicos sensibles, ya que no dejan residuos ni son conductores de electricidad. Si bien este tipo de extintor cumple con la NTC 2050 - Código Eléctrico Colombiano se recomienda la instalación de un sistema de supresión de incendios completo, basado en agentes limpios y sistemas de detección temprana (Vesda- Very Early Smoke Detection Apparatus), que sería lo más adecuado de acuerdo con las mejores prácticas de la norma La NFPA 75 - Standard for the Fire Protection of Information Technology Equipment.
- Aunque el acceso biométrico proporciona una buena seguridad física, es esencial el uso del del formato GTI-F-08 Bitácora de Ingreso al centro de datos que registre todas las entradas y salidas de la sala. Esto permitirá una trazabilidad completa y mejorará la capacidad de auditoría sobre quién accede a la sala y en qué momentos.
- Instalar medidores independientes de temperatura y humedad para monitorear los pasillos frío y caliente en el datacenter del 3er piso, alineándose con los estándares reconocidos.
- Documentar e implementar un protocolo de monitoreo ambiental que garantice:
- Alertas tempranas de condiciones ambientales críticas.
- Reportes periódicos sobre el estado del ambiente en el datacenter.

3.3.6.10. Evidencia documental (fotográfica):

- Fotografía del cableado desorganizado detrás de los racks.
- Fotografía de la incorrecta ubicación del pasillo frío detrás de los equipos.
- Fotografía del UPS con baterías externas.
- Fotografía del aire acondicionado de confort.
- Fotografía del extintor con la fecha de vencimiento visible.
- Fotografía del sistema de seguridad biométrica.

3.4. Evaluación de Desarrollo y Mantenimiento de Software

Para este aspecto se propuso como objetivo verificar la efectividad de los controles sobre el ciclo de vida del desarrollo de software, la implementación de políticas de gestión de cambios, control de versiones, pruebas de respaldo, y restauración de datos para asegurar la continuidad de los servicios y la integridad de la información.

3.4.1. Políticas y Procedimientos en Desarrollo de Software

3.4.1.1. Elementos revisados:

- Documentación técnica de JIRA, SharePoint, y GitLab.
- Contratos de fábrica relacionados con el desarrollo de software.
- Herramientas y procesos internos para gestión de cambios y versiones.

3.4.1.2. Evaluación:

- **Gestión de Cambios:** La gestión de cambios se maneja mediante JIRA para la recepción y seguimiento de solicitudes. Existe un proceso que incluye casos de uso y el manejo de historias de usuario, documentadas en Enterprise Architect y Confluence. Sin embargo, el proceso no está completamente formalizado ni alineado con un sistema de SLAs internos, lo que podría generar falta de trazabilidad en cambios menores.
- **Control de Versiones:** El control de versiones se gestiona a través de GitLab y SharePoint, pero el proceso de versionamiento no está completamente estandarizado. Actualmente, están segregadas las instalaciones de desarrollo, pruebas y producción, lo cual minimiza el riesgo de errores en despliegues.
- **Pruebas de Software:** Las pruebas se realizan manualmente mediante scripts funcionales, sin automatización. Dado que la misión de la entidad no es el desarrollo de software, la automatización no es obligatoria, pero podría mejorar la eficiencia del proceso en desarrollos a gran escala. El equipo de calidad realiza validaciones antes del despliegue, pero aún no se han documentado oficialmente los procedimientos. De desarrollo y mantenimiento de software el cual se realiza al interior de la entidad a través de contratistas.

3.4.1.3. Recomendaciones:

- Documentación del proceso de gestión de cambios en el sistema de calidad de acuerdo con la Norma ISO 9001:2015: Puesto que la documentación del sistema de calidad no establece los detalles procedimentales, se recomienda al menos Implementar un registro formal para todos los cambios, independientemente de su criticidad y de que se estén tramitando por JIRA. Incluir la definición de SLAs internos para mejorar la trazabilidad según las secciones relevantes de la norma: Cláusula 7.5.1 – Control de la información documentada y Cláusula 8.5.1 – Control de la producción y prestación del servicio. Estandarización del control de versiones: Actualizar la política de control de versiones utilizando un enfoque como GitFlow, para definir ramas específicas para desarrollo, pruebas, y producción.

- Automatización de pruebas: Evaluar la pertinencia de nuevas herramientas para automatizar pruebas.

3.4.1.4. Evidencia documental:

- Documentación en JIRA de cambios recientes, con casos de uso y procedimientos
- Contratos de fábrica BID 049-2023 y otros relacionados y en proceso de contratación con gestión de cambios en eKOGUI en el área responsable de Gestión de Tecnologías de la Información
- No existencia de dichos procedimientos en el SGC

3.4.2. Pruebas de Restauración de Copias de Seguridad

3.4.2.1. Elementos revisados:

- Guía GTI-G-06 - Gestión de Respaldo y Restauración de Copias de Seguridad.
- Informe de pruebas de restauración.
- Sistema de respaldo implementado: Veeam.

3.4.2.2. Evaluación:

- Copia de seguridad de servidores y bases de datos:
  Se verificó que las copias de seguridad se realizan correctamente, con respaldo incremental y completo a través de Veeam. Sin embargo, algunos registros de restauración no contaban con documentación completa, comprometiendo la trazabilidad.
- Pruebas de restauración:
  Se realizan pruebas de restauración periódicamente,
- En casos de restauración por demanda en algunos casos (Ej. 33677 y 33664) carecen de evidencia trazable completa de las acciones ejecutadas en el reporte, sin embargo, es posible verificar la trazabilidad a través del sistema GLPI en caso de requerirse

3.4.2.3. Recomendaciones:

- Ninguna

3.4.2.4. Evidencia documental:

- Registros de pruebas de restauración en Veeam y los casos específicos

3.4.3. Ciclo de Vida de Desarrollo de Software (SDLC)

3.4.3.1. Elementos revisados:

- Diagrama de Ciclo de Vida de Desarrollo.
- Registros de pruebas de calidad.
- Guía de Desarrollo Interno.

3.4.3.2. Evaluación:

- Modelo de desarrollo: Se sigue un ciclo iterativo que incluye fases de análisis, diseño, desarrollo, pruebas y despliegue. Sin embargo, no se evidenció la formalización de un marco de gestión del ciclo de vida del software (SDLC), lo que genera variabilidad en la calidad de los entregables. Se entiende que el contrato con la fábrica de software incluye este ciclo.
- Pruebas de calidad: Las pruebas de calidad no están completamente estandarizadas y se realizan manualmente. No se cuenta con un plan formal de pruebas automatizadas, lo que puede generar riesgos al desplegar actualizaciones o nuevos desarrollos internos.

3.4.3.3. Recomendaciones:

- Formalizar el ciclo de vida del desarrollo (SDLC) para desarrollos internos: Implementar un marco de referencia estándar para todas las fases de desarrollo, asegurando la calidad y trazabilidad. Ver 3.3.1
- Automatización de pruebas: Establecer la pertinencia de un plan de pruebas automatizado que permita la validación de los desarrollos antes de su despliegue.

3.4.3.4. Evidencia documental:

- Plan de pruebas CRM y documentación Técnica

3.5. Evaluación de Soporte y Administración de Tecnologías

En relación con este aspecto, se evaluó la calidad del soporte técnico, la administración de infraestructuras y tecnologías críticas, así como el cumplimiento de los acuerdos de nivel de servicio (SLA) definidos en los contratos de la Agencia. Se revisaron los procedimientos de soporte, gestión de incidencias, administración de sistemas y monitoreo de servicios.

3.5.1. Gestión del Soporte Técnico y Administración de Incidencias

3.5.1.1. Elementos revisados:

- Sistema de gestión de incidencias (GLPI)
- Registros de soporte técnico del primer y segundo trimestre de 2024
- Acuerdos de Niveles de Servicio (SLA) establecidos en contratos de soporte

3.5.1.2. Evaluación:

- El sistema de gestión de incidencias GLPI es utilizado para la recepción, seguimiento y cierre de tickets relacionados con incidencias técnicas en los sistemas críticos. Durante la auditoría, se identificó que los tiempos de respuesta están alineados con lo definido en el SLA de soporte técnico (resolución de incidentes críticos en menos de 4 horas). Sin embargo, algunos tickets de baja prioridad muestran demoras en la resolución.
- Tiempos de resolución de incidencias: Según los registros, el 75% de los incidentes fueron resueltos dentro de los tiempos acordados, pero se identificó un 25% de tickets de prioridad baja que no fueron resueltos en el tiempo estipulado, lo que generó quejas internas documentadas.

3.5.1.3. Recomendaciones:

- Optimizar el proceso de escalamiento de incidencias: Revisar el proceso de priorización de tickets de baja criticidad para evitar demoras innecesarias, lo cual podría mejorarse mediante un mayor enfoque en la automatización de asignación de recursos a tareas de soporte rutinarias.
- Reforzar la capacitación del equipo de soporte: Es recomendable que el equipo técnico reciba formación continua en la gestión de incidencias para reducir los tiempos de respuesta.
- Para los tiempos de resolución de incidencias. Revisar la definición de los SLAS o aumentar el número de personas atendiendo, ya que de acuerdo con la Teoría de Colas no es posible cumplir con un SLA utilizando promedios para la planeación, el promedio o la mediana solo garantiza que se cumpla con alrededor del 50% de los casos en los tiempos asignados dado que el promedio o la mediana representan puntos centrales. Se recomienda utilizar metodologías adecuadas usando datos históricos, basadas en percentiles o variabilidad para evitar la insatisfacción con el servicio, de lo contrario todos los casos no resueltos se convertirán en “Atipicos”.

3.5.1.4. Evidencia documental:

- Informe de resolución de incidencias del segundo trimestre de 2024 (Anexo 11), donde se detalla que, de 632 casos gestionados, 158 superaron los tiempos establecidos en el SLA para tickets de baja prioridad.

3.5.2. Disponibilidad y Monitoreo de Servicios

3.5.2.1. Elementos revisados:

- SLA de Servicios Críticos
- Informes de monitoreo de infraestructura de junio a agosto de 2024
- Reportes de caídas del sistema

3.5.2.2. Evaluación:

- La infraestructura crítica, compuesta por servidores, almacenamiento SAN y servicios de red, es monitoreada mediante una herramienta de gestión de infraestructura en tiempo real. Se verificó que el nivel de disponibilidad alcanzado durante el periodo de auditoría fue del 98.25%, cumpliendo con lo acordado en los SLA de 99%.
- Mantenimiento preventivo: Se constató que los mantenimientos preventivos planificados se realizaron en tiempo y forma, lo cual contribuyó a mantener la disponibilidad del servicio. Sin embargo, en el informe de monitoreo de junio de 2024, se evidenció una caída del servicio que duró 3 horas, no registrada adecuadamente en el sistema de monitoreo. Sin embargo, por medio de reporte con el proveedor de Internet se estableció que los incidentes revisados muestran que las fallas no se debieron a problemas en la infraestructura del proveedor, sino a la desconexión de equipos en la sede del cliente. Si bien el monitoreo y la resolución de problemas por parte del proveedor fueron efectivos

3.5.2.3. Recomendaciones:

- Mejora en la notificación de mantenimientos para evitar caídas: es necesario que la entidad implemente mejores prácticas de gestión y supervisión de equipos para evitar que estas desconexiones se repitan en el futuro.
- Auditorías de monitoreo más frecuentes: Se sugiere realizar auditorías trimestrales sobre el sistema de monitoreo para asegurar que todas las caídas se registren y gestionen adecuadamente.

3.5.2.4. Evidencia documental:

- Reporte de disponibilidad del sistema (Anexo 12), donde se refleja una caída de **3 horas** no registrada correctamente el día 12 de junio de 2024, afectando parcialmente la disponibilidad mensual. Y adecuadamente explicado por el proveedor de servicios de Internet o Servicie Manager de Claro.

3.5.3. Mantenimiento Preventivo y Correctivo

3.5.3.1. Elementos revisados:

- Informe de Mantenimiento Preventivo – julio 2024
- Lista de chequeo de mantenimiento de servidores
- Contrato de mantenimiento de equipos críticos

3.5.3.2. Evaluación:

- El mantenimiento preventivo es ejecutado de manera mensual sobre servidores, sistemas de almacenamiento y redes críticas. El Informe de Mantenimiento de julio de 2024 muestra actividades tales como la limpieza interna de servidores, actualización de firmware y verificación de las fuentes de energía y sistemas de redundancia eléctrica.
- Mantenimiento correctivo: Aunque el plan de mantenimiento preventivo se cumple adecuadamente, el informe destaca que no se realizaron pruebas exhaustivas en los sistemas UPS y generadores eléctricos. Se observaron también dos fallos eléctricos en la infraestructura del cliente que no fueron atendidos dentro de los plazos acordados.

3.5.3.3. Respuesta del Auditado:

"Se solicita precisar en qué consiste un programa formal que contemple pruebas exhaustivas, con el propósito de trasladar esa solicitud al operador FAMOC."

3.5.3.4. Aclaración a la Respuesta del Auditado:

- Falta de pruebas documentadas de acuerdo con las buenas prácticas de la industria:
  - Aunque se realiza mantenimiento preventivo, no se evidencia un programa formal de pruebas que simule condiciones de emergencia.
  - Esto incumple con la Ley 87 de 1993, que exige documentación que garantice la continuidad operativa.

Por lo tanto y de acuerdo con las buenas prácticas tenemos que la norma BICSI 02 se centra en las mejores prácticas para el diseño e instalación de infraestructuras de centros de datos. En particular, las secciones que se pueden revisar incluyen:

- **Capítulo 6: Sistemas Eléctricos**: Este capítulo aborda la infraestructura eléctrica, incluyendo UPS y generadores, y las pruebas necesarias para asegurar su funcionamiento adecuado.
- **Capítulo 10: Mantenimiento y Operaciones**: Aquí se detallan las prácticas recomendadas para el mantenimiento preventivo y correctivo, incluyendo la documentación y pruebas de sistemas críticos

La norma ASHRAE TC9 se enfoca en las prácticas de ingeniería para sistemas de HVAC en centros de datos. Las secciones relevantes incluyen:

- **Sección 6: Distribución de Energía Eléctrica**: Esta sección cubre las recomendaciones para la distribución de energía, incluyendo pruebas de equipos como UPS y generadores
- **Sección 8: Pruebas y Mantenimiento**: Aquí se detallan las directrices para realizar pruebas periódicas y mantenimiento de sistemas críticos para asegurar su continuidad operativa

- **Relación con terceros (FAMOC):**
  - A pesar de que el mantenimiento está delegado, la entidad sigue siendo responsable de verificar que:
  - Existan pruebas regulares documentadas.
  - Los informes de pruebas y mantenimiento estén disponibles para auditorías.
  - La infraestructura provista por el tercero sea la adecuada.

3.5.3.5. Recomendación

- **Establecer un programa formal de pruebas exhaustivas:**
  - Incluir simulaciones periódicas en condiciones reales para verificar la funcionalidad de los UPS y generadores eléctricos.
  - Documentar los resultados de las pruebas
- **Garantizar la gestión con el operador FAMOC:**
  - Exigir al operador la implementación y documentación de pruebas en condiciones controladas.
  - Solicitar fichas de mantenimiento e informes de pruebas para garantizar que cumplen con las normativas nacionales y mejores prácticas internacionales.

3.5.3.6. Evidencia Documental cerca de los equipos:

- No se encontró.

3.5.4. Gestión de Personal Técnico y Políticas de Seguridad

3.5.4.1. Elementos revisados:

- Políticas de control de acceso y seguridad del personal
- Contratos de servicio y nómina de personal técnico

3.5.4.2. Evaluación:

- Las políticas de seguridad del personal técnico incluyen el control de acceso a las instalaciones críticas mediante autenticación biométrica y registros de ingreso/salida. Durante la auditoría, se verificó que todos los técnicos cumplen con los controles de acceso establecidos y que la seguridad social de los contratistas está debidamente documentada en los contratos.
- Al ingresar el auditor a las Salas de Comunicaciones de la sede de la ANDJE no se le requirió el diligenciamiento del formato GTI-F-08 Bitácora de Ingreso al centro de datos.
- Verificación de cumplimiento de normas de seguridad: Los registros muestran que los técnicos cuentan con los accesos necesarios y han seguido las normativas internas de la entidad. Sin embargo, se detectó que, en dos casos, técnicos externos accedieron al Data Center sin la debida supervisión, lo cual infringe los protocolos de acceso a áreas críticas.

3.5.4.3. Recomendaciones:

- Reforzar el control de acceso para personal externo: Se recomienda que el acceso de cualquier personal externo al Data Center esté siempre supervisado por un miembro del equipo técnico autorizado para evitar cualquier incumplimiento de las políticas de seguridad.
- Realizar el diligenciamiento del formato GTI-F-08 Bitácora de Ingreso al centro de datos para las salas de comunicaciones de la sede de la ANDJE.
- Capacitación en políticas de seguridad: Es recomendable llevar a cabo capacitaciones anuales sobre políticas de acceso y seguridad del personal, incluyendo a contratistas y terceros.

3.5.4.4. Evidencia documental:

- Bitácoras de acceso al Data Center donde se observan dos casos de ingreso de técnicos externos sin supervisión en junio de 2024.
- Evidencias fotográficas de las salas visita in situ

3.6. Evaluación de Integración y Conformidad Estratégica

Sobre este aspecto se verificó la alineación de los sistemas y procesos tecnológicos con los objetivos estratégicos de la entidad, así como el cumplimiento de las normativas legales, regulatorias y de seguridad aplicables. Además, se revisó la implementación de las políticas de transformación digital, la protección de datos y la seguridad de la información.

3.6.1. Alineación con los Objetivos Estratégicos

3.6.1.1. Elementos revisados:

- Plan Estratégico de la Agencia 2022-2025
- Manual de Gobierno Digital - MinTic
- Plan de Transformación Digital (Decreto 1008 de 2018)

- Lineamientos generales de la Política de Gobierno Digital (Decreto 767 de 2022)
- PETI 2024 - 2027

3.6.1.2. Evaluación:

- La evaluación muestra que los proyectos tecnológicos en curso, como la implementación de los sistemas Ekogui y Mercurio, están alineados con los objetivos estratégicos definidos en el Plan Estratégico 2022-2025 de la Agencia, particularmente en lo que respecta a la eficiencia operativa y la automatización de procesos.
- Transformación digital: Se ha iniciado la implementación de estrategias digitales conforme al Plan de Transformación Digital establecido en el Decreto 1263 de 2022. Las iniciativas actuales incluyen la digitalización de procesos internos y la migración a soluciones en la nube.

3.6.1.3. Recomendaciones:

- Fortalecer la integración de sistemas: Se recomienda avanzar hacia una mayor integración entre los sistemas clave (Ekogui, Orfeo, Dynamics 365 CRM y otros) que faciliten la interoperabilidad y la consolidación de datos.
- Revisión periódica del Plan de Transformación Digital: Se sugiere que la Agencia establezca una revisión periódica del plan de transformación digital para asegurar que los objetivos estratégicos estén siendo alcanzados y ajustar cualquier desvío que se presente.

3.6.1.4. Evidencia documental:

- Plan Estratégico de la Agencia 2022-2025 (Anexo 15), que detalla los objetivos de eficiencia operativa y automatización.
- Reportes de progreso del Plan de Transformación Digital, donde se evidencian las metas alcanzadas en la digitalización de procesos hasta el primer semestre de 2024.

3.6.2. Cumplimiento de Normativas de Seguridad de la Información

3.6.2.1. Elementos revisados:

- Ley 1581 de 2012 (Protección de Datos Personales)
- Decreto 1078 de 2015 (Gobierno Digital)
- Modelo de Seguridad y Privacidad de la Información - MinTic
- Normativa ISO/IEC 27001:2013 – No Obligatoria
- Políticas de Gestión ANDJE Cap. 6 Seguridad de la Información

3.6.2.2. Evaluación:

- Se verificó el cumplimiento de la Ley 1581 de 2012, que regula la protección de datos personales en la Agencia. La política de privacidad de la entidad ha sido actualizada conforme a los requisitos de dicha ley, incluyendo la creación de una Matriz de Activos de Información para identificar y clasificar los datos sensibles, clasificados y reservados.

- Normativa ISO/IEC 27001:2013: La Agencia ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) conforme al Modelo de Seguridad y Privacidad de la Información – MinTic, al no ser obligatoria la norma ISO/IEC 27001:2013 en su totalidad se entiende el MSPI como un mínimo de cumplimiento dejando abierta la posibilidad de la realización de las auditorías técnicas del SGSI lo cual generaría una seguridad adicional en cuanto al cumplimiento continuo de los controles de seguridad.

3.6.2.3. Recomendaciones:

- Políticas de Protección de datos: Continuar fortaleciendo las políticas de protección de datos personales y de seguridad de la información, conforme a la Ley 1581 y al Modelo de Seguridad y Privacidad de la Información - MinTic
- Fortalecer el SGSI: Fortalecer la frecuencia de las revisiones del Sistema de Gestión de Seguridad de la Información, asegurando que las medidas de mitigación de riesgos se implementen de manera continua y documentada.

3.6.2.4. Evidencia documental:

- Matriz de Activos de Información donde se detallan los datos sensibles y su clasificación.
- Documentos de implementación del SGSI conforme a ISO/IEC 27001 (Anexo 1 MSPI).

3.6.3. Cumplimiento de Leyes y Reglamentos de Transparencia y Gobierno Digital

3.6.3.1. Elementos revisados:

- Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información Pública)
- Decreto 1244 de 2021 (Creación de la Oficina Asesora de Sistemas y Tecnologías de la Información)
- Normativa de Gobierno Digital
- Indicadores de Gobierno Digital 2024

3.6.3.2. Evaluación:

- La Agencia ha mostrado avances en la implementación de la Ley 1712 de 2014, con la publicación regular de informes y datos en sus portales institucionales. Sin embargo, ciertos documentos críticos como el informe de gestión de riesgos, el plan de auditoría interna de 2024 y el informe de seguimiento de contratación del tercer trimestre de 2023 no han sido actualizados en el portal de transparencia desde el segundo trimestre de 2023.
- Cumplimiento de la política de Gobierno Digital: La Agencia ha implementado los principios de gobierno digital según el Manual de Gobierno Digital del MinTic, pero algunos indicadores de cumplimiento, como la participación ciudadana y la disponibilidad de servicios electrónicos, no han alcanzado los niveles esperados según la información publicada en el tablero interactivo de Gobierno Digital.

3.6.3.3. Recomendaciones:

- Actualizar el portal de transparencia: Asegurarse de que todos los documentos requeridos por la Ley 1712 de 2014 estén actualizados y disponibles para el público. Se recomienda designar un responsable dentro de la Oficina Asesora de Sistemas para monitorear el cumplimiento de las actualizaciones del portal.
- Incrementar la disponibilidad de servicios electrónicos: Desarrollar una estrategia para mejorar la participación ciudadana y la disponibilidad de servicios en línea, incluyendo encuestas, foros y mecanismos de retroalimentación en los portales públicos.

3.6.3.4. Evidencia documental:

- Informe de cumplimiento de la Ley de Transparencia, que detalla los documentos publicados hasta el segundo trimestre de 2023.
- Capturas de pantalla
- Reportes de seguimien.to de la implementación del Manual de Gobierno Digital

4. EFECTIVIDAD DE LOS CONTROLES:

A continuación, se presenta el análisis de los riesgos asociados a los resultados de la Auditoria

Tabla 2. Riesgos Institucionales asociados al proceso

Sección Evaluación	Resultados Evaluación	Riesgo Asociado	Control Asociado	Incumplimiento / Inefectividad	Impacto	Clasificación	Conclusión
3.3.6 (anterior 3.2.6)	Fallas en los sistemas de respaldo eléctrico (UPS y generadores)	**SYPDLI045 - Pérdida de la disponibilidad de la infraestructura tecnológica.**	**ID 493**: Plan de recuperación de desastres **ID 16**: Mantenimiento preventivo de sistemas eléctricos	Falta de pruebas exhaustivas en los UPS y generadores; el mantenimiento preventivo no es suficiente.	Alto	No conformidad	**Materializable**.
3.2.7 (anterior 3.2.6)	Sobrecalentamiento y fallas por condiciones ambientales inadecuadas	**SYPDLI045 - Pérdida de la disponibilidad de la infraestructura tecnológica.**	**ID 19**: Mantenimiento preventivo del sistema de aire acondicionado	El sistema de refrigeración es inadecuado y faltan medidores de temperatura y humedad.	Alto	No conformidad	**Materializable**..
3.5.4 (anterior 3.4.4)	Accesos no autorizados al Data Center	**SYPDLI048 - Pérdida de confidencialidad de la información pública clasificada o reservada.**	**ID 494**: Validación mensual de usuarios **ID 1**: Monitoreo de acceso	Técnicos accedieron sin supervisión, lo que indica fallos en el control de acceso.	Alto	No conformidad	**Materializable**..

Sección Evaluación	Resultados Evaluación	Riesgo Asociado	Control Asociado	Incumplimiento / Inefectividad	Impacto	Clasificación	Conclusión
3.4.1 (anterior 3.3.1)	Falta de formalización en la Documentación de gestión de cambios de software	**SYPDLI044 - Pérdida de confidencialidad, integridad y disponibilidad de la información.**	**ID 492**: Análisis de vulnerabilidades	El proceso de gestión de cambios no está documentado, generando inconsistencias y errores.	Moderado	No conformidad	**Materializable**.
3.3.4 (anterior 3.2.4)	Conexiones eléctricas no certificadas y materiales inflamables	**SYPDLI045 - Pérdida de la disponibilidad de la infraestructura tecnológica.**	**ID 16**: Mantenimiento preventivo del sistemaeléctrico **ID 17**: Certificación de instalaciones eléctricas	Conexiones no certificadas y materiales inflamables en áreas críticas; los controles no se aplican adecuadamente.	Alto	No conformidad	**Materializable**..
3.5.1 (anterior 3.4.1)	Acumulación de incidencias de baja prioridad	**G032 - Pérdida reputacional por requerimientos de usuarios internos.**	**ID 128-130**: Procedimiento GTI-P-03 **ID 494**: Automatización del proceso de asignación	Las incidencias de baja prioridad se acumulan, afectando la percepción del servicio.	Moderado	Observación	**Potencialmente materializable**...
3.3.4, 3.3.5, 3.3.6 (anterior 3.2.4, 3.2.5, 3.2.6)	Extintores vencidos e inadecuados	**SYPDLI045 - Pérdida de la disponibilidad de la infraestructura tecnológica.**	**ID 26**: Mantenimiento preventivo del sistema contraincendios	Se encontraron extintores no adecuados para equipos electrónicos, lo quecompromete la seguridad.	Alto	No conformidad	**Materializable**..
3.3.4, 3.3.5, 3.3.6 (anterior 3.2.4, 3.2.5, 3.2.6)	Ausencia de un sistema VESDA o similar de detección de humo	**SYPDLI045 - Pérdida de la disponibilidad de la infraestructura tecnológica.**	**ID 28**: Implementación del plan de emergencias	No hay un sistema de detección temprana de humo, lo que retrasa la respuesta ante incendios.	Alto	Recomenda-ción	**Materializable**.
3.5.1 (anterior 3.4.1)	Falta de automatización en la resolución de incidencias críticas	**G032 - Pérdida reputacional por requerimientos de usuarios internos.**	**ID 128-130**: Procedimiento de escalamiento de incidencias	Las incidencias críticas cumplen con SLA, pero el proceso podría optimizarse con automatización adicional.	Moderado	Observación	**Potencialmente materializable**..
3.4.2 (anterior 3.3.2)	Falta de monitoreo de calidad en sistemas de respaldo	**SYPDLI045 - Pérdida de la disponibilidad de la infraestructura tecnológica.**	**ID 493**: Plan de recuperación de desastres **ID 16**: Mantenimiento preventivo de sistemas eléctricos	No se realiza monitoreo continuo para verificar la eficiencia del respaldo en situaciones de emergencia.	Alto	Observación	**Potencialmente materializable**.

Fuente: Elaboración propia

Del cuadro anterior podemos concluir que el entorno de infraestructura crítica de la Agencia Nacional revela varios factores que afectan la **disponibilidad, confidencialidad e integridad** de los sistemas de TI, así como la seguridad física de las instalaciones y del personal. Las observaciones y no conformidades detectadas se concentran, en gran medida, en la **gestión del respaldo eléctrico, control ambiental, seguridad contra incendios y control de accesos**.

Específicamente, los sistemas de respaldo eléctrico (UPS y generadores) presentan deficiencias en las pruebas exhaustivas de funcionamiento, lo que expone a los sistemas a fallos durante cortes de energía prolongados. Los controles actuales, basados principalmente en mantenimiento preventivo, no son suficientes para garantizar la disponibilidad operativa en situaciones críticas, y la ausencia de un monitoreo continuo limita la capacidad para detectar problemas de manera proactiva. La falta de medidores de temperatura y humedad, combinada con un sistema de refrigeración de confort, incrementa el riesgo de sobrecalentamiento y reduce la eficiencia operativa del centro de datos, vulnerando su disponibilidad y la vida útil de los equipos.

Adicionalmente, se identificaron **inconsistencias en el control de accesos** a los Data Centers local y remoto, donde la falta de supervisión permitió que técnicos ingresaran sin el control requerido. Esto representa un riesgo significativo, pues compromete la **confidencialidad** de los datos almacenados y la **integridad** física de los sistemas críticos, exponiéndolos a posibles incidentes o manipulación no autorizada.

Un punto de particular relevancia en seguridad física y seguridad y protección en el trabajo es el **uso de extintores de CO_2 en áreas cerradas**. Aunque estos elementos pueden ser efectivos en la protección de equipos electrónicos, **el CO_2 representa un peligro de muerte para las personas que operen los extintores durante emergencias debido a sus efectos asfixiantes en espacios no ventilados.** Esto subraya la necesidad de utilizar sistemas de extinción que protejan tanto los activos de TI como la seguridad de los operadores, tales como **agentes limpios** (por ejemplo, FM-200 o Novec 1230).

Finalmente, en cuanto a la **gestión de incidencias y cambios de software**, se observa una falta de formalización en la documentación de los procesos de gestión de cambios y un retraso en la resolución de incidencias de baja prioridad, lo que afecta la percepción de calidad del servicio. La acumulación de incidencias menores podría llegar a afectar la operatividad si no se resuelve a tiempo.

En resumen, el análisis evidencia que, aunque la Agencia cuenta con mecanismos para gestionar la infraestructura crítica, la efectividad de los controles en áreas clave requiere optimización. Las recomendaciones propuestas abordan los puntos vulnerables que afectan la seguridad, disponibilidad y resiliencia del centro de datos y de los sistemas críticos.

5. NO CONFORMIDADES, OBSERVACIONES Y RECOMENDACIONES

Conforme con cada uno de los aspectos evaluados anteriormente se determinaron las siguientes, a saber:

5.1. No Conformidades

5.1.1. No Conformidad 1: Desorganización del cableado y seguridad física en Sala del 2° Piso OASTI Sección del informe: 3.3.4 (anterior 3.2.4)

La auditoría detectó que el cableado en la Sala OASTI se encuentra sin organización adecuada, lo que incumple las normas BICSI 002 y TIA-606-C, además de presentar conexiones eléctricas no certificadas bajo el Reglamento Técnico de Instalaciones Eléctricas (RETIE). La causa de esta situación radica en la falta de mantenimiento adecuado para el cableado y el descuido en las instalaciones eléctricas. Esta condición representa un alto riesgo de incendios y cortocircuitos, y dificulta el mantenimiento y la accesibilidad de los equipos, lo que podría afectar la continuidad operativa de los sistemas críticos de la Agencia. **RESOLUCIÓN MINTIC 500**

Conforme lo analizado en la sección 3.3.4.5 (anterior 3.2.4) **Se ratifica la No conformidad**

5.1.2. No Conformidad 2: Conexiones eléctricas no certificadas en la Sala del 2° Piso OASTI Sección del informe: 3.3.4 (Anterior 3.2.4)

Se detectaron conexiones eléctricas no certificadas en la Sala de Comunicaciones del Tercer Piso, en incumplimiento del Reglamento Técnico de Instalaciones Eléctricas (RETIE), con instalaciones improvisadas que incluyen hoyos en las paredes. La causa principal de esta no conformidad es la falta de supervisión técnica adecuada durante las instalaciones eléctricas. Esta situación representa un riesgo elevado de cortocircuitos y posibles incendios, lo que podría poner en peligro tanto al personal como la infraestructura tecnológica alojada en dicha sala.

Conforme la revisión de los documentos y la normativa aplicable revisados en la sección 3.3.4. 5 (anterior 3.2.4) Teniendo en cuenta la respuesta de la OASTI, **la auditoria se ratifica en la conformidad.**

5.2. Observaciones:

5.2.1. Observación 1: Ausencia de medidores de temperatura y humedad en la Sala de Comunicaciones (datacenter) 3er Piso. Sección del informe: 3.3.6 (anterior 3.2.6)

Se constató por medio de visita y evidencia fotográfica que en la Sala de Comunicaciones del Tercer Piso no existen medidores independientes de temperatura y humedad, tanto para pasillos frio como caliente, lo cual contraviene los lineamientos de control ambiental establecidos en las normas ANSI/TIA-942 y ASHRAE TC 9.9 para centros de datos. Esto genera un riesgo elevado de sobrecalentamiento y corrosión de los equipos, lo que podría derivar en fallas técnicas que afecten la disponibilidad y rendimiento de los sistemas misionales críticos.

Conforme con lo expuesto en la sección 3.3.6.8 (anterior 3.2.6) Se mantiene la **Observación**

5.2.2. Observación 2: Inconsistencias en el monitoreo de disponibilidad de servicios. Sección del informe: 3.5.2 (anterior 3.4.2)

En el monitoreo de disponibilidad de servicios críticos, se detectó un evento de caída de tres horas, ocurrido en junio de 2024, el cual no fue registrado correctamente. Pues se identificó que, fue por desconexión por parte del cliente. Esta inconsistencia incumple las prácticas recomendadas para la gestión y el monitoreo continuo de la disponibilidad de servicios críticos. Esta situación se debe a la falta de sincronización entre los reportes generados por el sistema de monitoreo interno y los registros del proveedor de servicios de Internet. Como consecuencia, la falta de precisión en el monitoreo de la disponibilidad aumenta el riesgo de que no se detecten caídas de servicio de manera oportuna, lo que podría comprometer el cumplimiento de los SLA y afectar la continuidad de los servicios.

Conforme con lo expuesto en la sección 3.5.2.2 (anterior 3.4.2) Se mantiene la **Observación** sin perjuicio en la toma de las medidas preventivas correspondientes.

5.2.3. Observación 3: Ausencia de pruebas regulares en sistemas de respaldo eléctrico
Sección del informe: 3.5.3 (anterior 3.4.3)

Se observó que, aunque el mantenimiento preventivo de los sistemas de respaldo eléctrico, como los UPS y los generadores, se realiza de manera regular, no se documentan pruebas exhaustivas para verificar su funcionamiento en situaciones de emergencia. Pues dependen de un tercero. Esta falta de pruebas contraviene las mejores prácticas de continuidad operativa, ya que impide la verificación efectiva de que los sistemas funcionarán adecuadamente cuando se produzca un corte eléctrico prolongado. Esta situación se debe principalmente a la falta de un programa formal que contemple la realización periódica de estas pruebas en conjunto con la copropiedad dueña de los equipos. En consecuencia, existe un riesgo elevado de que los sistemas de respaldo no funcionen adecuadamente en emergencias, lo que afectaría la operatividad de los sistemas críticos.

Conforme con lo expuesto en la sección 3.5.3.4 (Anterior 3.4.3) Se mantiene la **Observación**

Observación 4: Control insuficiente en accesos a áreas críticas del Datacenter
Sección del informe: 3.5.4 (anterior 3.4.4)

Se detectó que, a pesar de que las salas de comunicaciones cuentan con un sistema de autenticación biométrica para el control de accesos, algunos técnicos accedieron al Data Center sin la debida supervisión, lo que incumple las normativas internas de seguridad. Esta falta de control incrementa el riesgo de accesos no autorizados, lo que podría comprometer tanto la seguridad física como la integridad lógica de los sistemas críticos que se alojan en el Data Center. Esta situación se debe a la falta de supervisión constante sobre el personal externo que accede a áreas críticas.

Conforme con lo expuesto en la sección 3.5.4.2 (anterior 3.4.4) Se mantiene la **Observación**

5.2.4. Observación 5 (anteriormente No Conformidad 2) : Seguridad física insuficiente en Salas 2° Piso OASTI y Secretaría General
Sección del informe: 3.3.4 y 3.3.5 (anteriores 3.2.4 y 3.2.5)

En las Salas OASTI y Secretaría General del y Segundo Piso, el control de acceso está limitado a una chapa con llave, en áreas de fácil acceso de la entidad según evidencia fotográfica lo que incumple con las normativas internas de seguridad como el Instructivo GTI-I-01, que requiere controles de acceso más estrictos para áreas críticas. La causa de esta deficiencia es la falta de actualización de los controles de acceso en relación con las nuevas exigencias de seguridad. Como consecuencia, se incrementa el riesgo de accesos no autorizados o daños que podrían comprometer la seguridad de los equipos críticos alojados o conectados a la sala, afectando tanto la integridad de los datos como la operatividad de los sistemas.

Conforme con lo analizado en la sección 3.3.5.2 (anterior 3.2.5) y Teniendo en cuenta la respuesta de la OASTI, **se retira la no conformidad y se reclasifica como una observación** no obstante la actualización del nuevo procedimiento.

5.2.5. Observación 6 (Anteriormente No Conformidad 5) Material inflamable almacenado en la Sala del 2° Piso OASTI
Sección del informe: 3.3.4 (anterior 3.2.4)

Se constató la presencia de cajas de cartón, un material inflamable, en la Sala de Comunicaciones del Segundo Piso OASTI. Esta condición incumple con las normativas internacionales de seguridad, tales como **NFPA 75** y **NFPA 76**, que establecen que los centros de procesamiento de datos y áreas de telecomunicaciones deben estar libres de materiales combustibles para minimizar el riesgo de incendio. La causa de esta situación es la falta de control en la política de almacenamiento dentro de áreas críticas, permitiendo que se almacenen materiales inadecuados en dichas zonas. Como consecuencia, la presencia de elementos inflamables incrementa considerablemente el riesgo de incendio, lo que podría afectar gravemente la integridad de los equipos y la continuidad de los servicios alojados en la sala.

Luego de analizar el hallazgo y la respuesta del auditado sección 3.3.4.7 (anterior 3.2.4) , **se reclasifica la No Conformidad como Observación**

5.2.6. Observación 7 (anteriormente No Conformidad 6): Extintores de CO2 vencidos en la Sala 3er Piso y Sala del 2° Piso OASTI Sección del informe: 3.3.4.2 y 3.3.6.6 (anteriores 3.2.4 y 3.2.6)

Durante la auditoría se constató que los extintores de dióxido de carbono (CO2) en la Sala del Tercer en la Sala Segundo Piso OASTI están vencidos, lo que incumple con las normas de seguridad contra incendios, específicamente las recomendaciones de la **NFPA 10 y el SGSST** Resolución 0312 de 2019. para el mantenimiento y revisión de equipos de extinción de incendios. Por otra parte, estos extintores no son adecuados ya que desplazan el oxígeno en espacios cerrados, poniendo en peligro de muerte por asfixia a quien lo opera. Esta situación se debe a la falta de un control adecuado de las fechas de vencimiento y la falta de

inspecciones regulares de seguridad y salud en el trabajo de los equipos contra incendios. Como consecuencia, existe un alto riesgo de que, en caso de emergencia, los extintores no funcionen adecuadamente, comprometiendo la seguridad de las instalaciones y los equipos críticos alojados en ambas salas, lo que podría ocasionar daños graves a la infraestructura y poner en peligro al personal presente.

Después de analizar el hallazgo en la sección 3.3.6.6 (anterior 3.2.6) y la respuesta del auditado, Después de analizar el hallazgo y la respuesta del auditado, **se reclasifica como Observación** sin perjuicio de las acciones preventivas correspondientes.

5.2.7. Observación 8 Anterior (No Conformidad 3: Sistemas de refrigeración inadecuados en la Sala de Comunicaciones 3er Piso Sección del informe: 3.3.6 (anterior 3.2.6))

La auditoría evidenció que el **pasillo frío** estaba mal ubicado, detrás de los racks en lugar de estar de frente a los equipos, afectando la eficiencia del sistema de enfriamiento y aumentando el riesgo de sobrecalentamiento, se encontró también que el sistema de refrigeración en la Sala de Comunicaciones del Tercer Piso utiliza un aire acondicionado de confort en lugar de un sistema de climatización de precisión, lo que incumple con las normativas de ASHRAE TC 9.9 y BICSI 002 para centros de datos. El uso de un sistema no diseñado para mantener condiciones estables en centros de datos genera un riesgo considerable de sobrecalentamiento y corrosión, que podría causar interrupciones en los servicios tecnológicos de la entidad.
Tras revisar la documentación y las normativas aplicables (sección **3.3.6.4**, anterior **3.2.6**), **se considera necesario dejar constancia de esta observación como una advertencia formal, con el objetivo de evidenciar el hallazgo y resguardar las responsabilidades institucionales frente a posibles afectaciones futuras**. Dado su impacto potencial, esta situación se clasifica como crítica, considerando el riesgo de interrupciones en los servicios críticos para la entidad.

5.3. Recomendaciones:

Se presentan algunas de las recomendaciones más importantes derivadas del ejercicio de auditoría. No obstante, en las secciones del desarrollo del informe se incluyeron otras recomendaciones adicionales:

5.3.1. Recomendación 1 Formalización del proceso de gestión de cambios y documentación de procedimientos de desarrollo y mantenimiento de software en el SGC Sección del informe: 3.4.1.2 y 3.4.3.2 (anteriores 3.3.1 y 3.3.3)

Se recomienda formalizar y documentar los procedimientos relacionados con el desarrollo de software, gestión de cambios y control de versiones dentro del Sistema de Gestión de la Calidad (SGC), alineados con los requisitos de la NTC ISO 9001:2015. Actualmente, aunque la Agencia utiliza herramientas como JIRA para la gestión de cambios y GitLab y SharePoint para el control de versiones, estos procesos no están formalizados ni documentados en el SGC, lo que genera riesgos de falta de trazabilidad y control. La ausencia de un procedimiento

que especifique tiempos de respuesta (SLAs), responsabilidades y un proceso estandarizado de control de versiones aumenta la posibilidad de errores en los despliegues y afectaciones a la calidad de los desarrollos, particularmente en los sistemas críticos.

La norma ISO 9001:2015 exige que todos los procesos que impacten la calidad del servicio estén debidamente documentados y controlados en el SGC. No formalizar estos procedimientos podría resultar en observaciones negativas en futuras auditorías y recertificaciones, ya que estos procesos podrían ser auditables debido a su influencia en el giro ordinario de la entidad. La implementación de esta recomendación reducirá el riesgo de errores y mejorará la robustez en el desarrollo, mantenimiento y entrega de software, garantizando un cumplimiento normativo sólido.

5.3.2. Recomendación 2: Automatización de pruebas de software

Sección del informe: 3.4.3.3 (anterior 3.3.3)

Se recomienda que el equipo de desarrollo evalúe la implementación de herramientas de automatización de pruebas en lugar de depender exclusivamente de scripts funcionales manuales. Aunque la misión de la entidad no está centrada en el desarrollo de software, la automatización de pruebas podría mejorar significativamente la eficiencia del proceso, especialmente para pruebas repetitivas y en proyectos de mayor escala y para la recepción de entregables de fábrica. Actualmente, las pruebas no están formalizadas y dependen del equipo de calidad, lo que puede generar riesgos de inconsistencias en los resultados y tiempos de entrega más largos. Al automatizar las pruebas, se incrementará la confiabilidad y agilidad del proceso de validación de software.

5.3.3. Recomendación 3: Mejora en la supervisión de incidencias de bajo riesgo

Sección del informe: 3.5.1.2 (anterior 3.4.1)

Durante la auditoría se identificó que, aunque los incidentes críticos se resuelven dentro de los tiempos establecidos en el SLA, algunos tickets de baja prioridad presentan demoras significativas. Esto incumple lo acordado en los acuerdos de nivel de servicio. Como resultado, estas demoras afectan la percepción general del servicio y generan insatisfacción interna, lo que aumenta el riesgo de que las incidencias no resueltas se acumulen, complicando su eventual resolución y afectando potencialmente la operación. Por lo tanto, es necesario optimizar el proceso de escalamiento de incidencias y automatizar la asignación de recursos a tickets de baja criticidad para garantizar que el servicio mantenga su calidad y se respeten los tiempos establecidos.

5.3.4. Recomendación 4: Manejo de riesgos:

Sección del informe: 4

Teniendo en cuenta tanto el análisis de riesgos inherentes como aquellas situaciones encontradas en la auditoria se recomiendan los siguientes puntos:

- Mejorar el control de acceso mediante auditorías y supervisión constante.
- Automatizar los procesos de resolución de incidencias y gestión de cambios de software.

- Actualizar y certificar sistemas eléctricos, sistemas de respaldo y sistemas de refrigeración y medición ambiental del Datacenter local, salas de comunicación o cableado.
- Implementar sistemas de detección temprana de humo y extinción de incendios en áreas críticas como el Datacenter local, salas de comunicación o cableado.
- Dar Aplicación a las normas que regulan estas instalaciones como las ANSI/TIA-942 - Infrastructure Standard for Data Centers, ANSI/BICSI 002 - Best Practices for Data Centers, el RETIE (Reglamento Técnico de Instalaciones Eléctricas), la norma NTC 2050 - Código Eléctrico Colombiano, normas ambientales del SGSST, normas sobre extintores NTC 2885 y NTC 3808

6. CONCLUSIONES

Como resultado de la Auditoría al Proceso de Gestión de Tecnologías de la Información, donde se evaluaron los sistemas críticos de TI y se analizaron aspectos de desarrollo de software, mantenimiento de infraestructura tecnológica y soporte técnico, se concluye que, aunque la Agencia ha implementado un entorno tecnológico sólido y con certificaciones relevantes en seguridad, aún existen áreas críticas que requieren atención inmediata. En cuanto a **sistemas críticos y seguridad física**, se identificaron deficiencias relacionadas con el incumplimiento de la normativa RETIE en conexiones eléctricas, la desorganización del cableado, la falta de mantenimiento de extintores en varias áreas, así como un sistema de refrigeración ineficiente en la Sala del Tercer Piso, que afecta la eficiencia energética y el adecuado mantenimiento de los equipos secciones, 3.2.4 y 3.2.6 (anteriores3.1.4 y 3.1.6).

Respecto al **ciclo de desarrollo y mantenimiento de software**, aunque existen políticas de control, no se han formalizado completamente algunos procesos dentro del Sistema de Gestión de la Calidad (SGC), lo cual limita la trazabilidad y el cumplimiento de la norma ISO 9001:2015. Es fundamental documentar y formalizar prácticas de mantenimiento y control de cambios, dado el soporte que estos procesos brindan a los sistemas críticos, secciones 3.3.1 y 3.3.3 (anteriores 3.2.1 y 3.2.3).

En el área de **soporte técnico y gestión de incidencias**, se observó que si bien se cumplen los SLA para incidencias críticas, persisten demoras en la resolución de incidencias de baja prioridad. Asimismo, se requiere optimizar el respaldo eléctrico y mejorar el control de accesos para personal externo en áreas críticas, a fin de mantener la integridad de la infraestructura, secciones 3.4.1 y 3.4.4 (anteriores 3.3.1 y 3.3.4).

En cuanto a la **integración y conformidad estratégica**, se observó un alineamiento parcial con los objetivos del Plan Estratégico 2022-2025. Aunque se han implementado políticas de Gobierno Digital y Transformación Digital (Ley 1712 de 2014 y Decreto 1008 de 2018), se detectaron oportunidades de mejora en la actualización del portal de transparencia y la interoperabilidad entre sistemas internos. Estas áreas deben fortalecerse mediante revisiones semestrales del Plan de Transformación Digital, en cumplimiento del Decreto 1263 de 2022, para optimizar la eficiencia y asegurar la continuidad de los objetivos estratégicos, secciones 3.5.1, 3.5.2 y 3.5.3 (anteriores 3.4.1, 3.4.2 y 3.4.3).

Finalmente, se concluye que, si bien los riesgos no se han materializado, los controles actuales son insuficientes y, en ciertos casos, cortos para mitigar los identificados en áreas críticas de infraestructura y seguridad de la información. Por lo cual se recomienda optimizar la gestión de infraestructura crítica, formalizar los procedimientos internos y mejorar la integración de sistemas, garantizando así la eficiencia operativa y el cumplimiento normativo.

Para constancia se firma en Bogotá D.C., al 27 de enero de 2025.

_____

ADRIANA MILENA HERRERA ABRIL
Jefe de la Oficina de Control Interno
Nota. Los anexos al presente informe hacen parte integral.

Anexo No. 1

Informe de Auditoría al Proceso de Gestión de Tecnologías de la Información

Normatividad Examinada:

- Ley 1581 de 2012. disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Ley de Transparencia.
- Ley 1955 de 2019 Plan nacional de desarrollo 2018-2022 – Art.147 Transformación digital Art. 148 Gobierno digital como política de gestión.
- Ley 2052 de 2020 Servicios ciudadanos digitales - racionalización de trámites.
- Ley 2080 de 2021 - Reforma el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 734 de 2002 Código Disciplinario Único.
- Ley 610 de 2000 Define los procedimientos para determinar la responsabilidad fiscal de los servidores públicos y particulares que administran recursos públicos
- Ley 87 de 1993 Por la cual se establece el control interno en las entidades del Estado
- Decreto 1244 de 8 de octubre de 2021 creación de la Oficina Asesora de Sistemas y Tecnologías de la información en la Agencia
- Decreto 1008 de 2018, el cual modificó el Decreto 1078 de 2015, en su artículo 2.2.9.1.1.3 definió la seguridad de la información como principio de la Política de Gobierno Digital.
- Decreto 1244 de 8 de octubre de 2021 creación de la Oficina Asesora de Sistemas y Tecnologías de la información en la Agencia.
- Decreto Ley 4085 de 2011. Establecen los objetivos y la estructura de la Agencia..
- Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones - Gov.co.
- Decreto 1499 de 2017 modificó el Decreto 1083 de 2015 (Decreto Único Reglamentario del Sector de Función Pública), y adoptó el MIPG.
- Decreto 1008 de 2018, el cual modificó el Decreto 1078 de 2015, en su artículo 2.2.9.1.1.3 definió la seguridad de la información como principio de la Política de Gobierno Digital.
- Decreto Ley 2106 de 2019 - Simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública - Sedes electrónicas.
- Decreto 1263 de 2022 lineamientos y estándares aplicables a la Transformación Digital Pública
- Manual de Gobierno Digital – MinTic
- Decreto 767 de 2022 lineamientos generales de la Política de Gobierno Digital
- Guía para la administración del riesgo y el diseño de controles en entidads públicas
- Modelo de Seguridad y Privacidad de la Información – MinTic
- Directiva presidencial 02 de 2019. Simplificación De La Interacción Digitalmente Los Ciudadanos y el Estado - Portal Único GOV.CO.
- Directiva presidencial 03 de 2021 Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

- Directiva presidencial 02 de 2022, Reiteración de la Política Púbica en Materia de Seguridad Digital.
- Resolución 1519 de 2020 Información y seguridad Digital.
- Resolución 2893 de 2020 Estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y Gov.co.
- Resolución 2160 de 2020 Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos.
- Resolución 500 de 2021 lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital. Orienta la adopción de buenas prácticas internacionales.
- Resolución 312 de 2021, por el cual se adopta el Nuevo Sistema Integrado de Gestión Institucional – SIGI en la Agencia Nacional de Defensa Jurídica del Estado. SGS – SGSPI.
- Resolución 1126 de 2021 la cual modifica la Resolución 2710 de 2017 en cuanto al Plazo de adopción protocolo IPv6.
- Resolución 2749 de 2017 Regula la eliminación y manejo adecuado de sustancias que agotan la capa de ozono, aplicable en sistemas de supresión de incendios.
- CONPES 3854 de 2017 Política Nacional De Seguridad Digital se desarrollan con la implementación del Modelo de Gestión de Riesgos de Seguridad Digital-MGRSD.
- CONPES 3995 de 2020 Política Nacional De Confianza Y Seguridad Digital.
- Marco de transformación digital – Política de Gobierno Digital.
- Marco de mejores prácticas en Tecnología alineados con COBIT 5, ITIL V3 2011 E ISO 27000:2013.
- Guía de Conceptos y criterio mínimos para los documentos aportados al PAI/MIPG, referencia DE-G-05. Decreto 1263 de 2022, "Por el cual se adiciona el Título 23 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública
- RETIE (Reglamento Técnico de Instalaciones Eléctricas)
- NTC 2050 - Código Eléctrico Colombiano
- NTC 2885 y NTC 3808 Normativa sobre extintores Son Obligatorias conforme a la norma sismorresistente NSR-10 establecida en la ley 400 de 1997
- Normas Voluntarias:
  - ISO/IEC 22237 - Centros de Procesamiento de Datos
  - ANSI/TIA-942 - Infrastructure Standard for Data Centers
  - ANSI/BICSI 002 - Best Practices for Data Centers
  - NTC 5001 Estándares aplicados al Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST), con requisitos para garantizar la seguridad en el lugar de trabajo.
  - Uptime Institute Tier Standards niveles de TIER (I a IV)
  - ISO/IEC 27001 - Sistema de Gestión de Seguridad de la Información
  - ISO 50001 - Gestión Energética

- ISO/IEC 20000 Estándar internacional para la gestión de servicios TI, que define las mejores prácticas para el diseño, entrega y mejora continua de servicios tecnológicos.
- NFPA 70 / NEC (National Electrical Code)
- IEC 60364 - Instalaciones Eléctricas de Baja Tensión
- ASHRAE 90.4 - Energy Standard for Data Centers
- ASHRAE TC 9.9 - Thermal Guidelines for Data Centers
- ISO 14644 - Limpieza del Aire en Ambientes Controlados
- NFPA 75 - Standard for the Protection of Information Technology Equipment
- NFPA 76 - Standard for the Fire Protection of Telecommunications Facilities
- ISO 22301 - Gestión de la Continuidad del Negocio

➢ Demás normatividad interna y externa aplicable

- **Documentos Examinados:**
  - ➢ Documentos asociados al proceso
  - ➢ Portal de Gobierno digital https://app.powerbi.com/view?r=eyJrIjoiOTg4ZThhMDItM2YzNi00MzliLWI4NWUtODZjMGZmZGQzOTQyIiwidCI6IjFhMDY3M2M2LTI0ZTEtNDc2ZC1iYjRkLWJhNmE5MWEzYzU4OCIsImMiOjR9