**INSTITUTO DISTRITAL DE RECREACIÓN Y DEPORTE – IDRD**

**OFICINA DE CONTROL INTERNO - OCI**

# INFORME FINAL AUDITORIA PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN (INCLUIR CONTROLES A TERCEROS)

**Período Auditado**
**1 de Mayo de 2023 y el 30 de septiembre de 2024.**

**Diciembre 2024**

## TABLA DE CONTENIDO

## 1. INTRODUCCIÓN

La Oficina de Control Interno – OCI desarrolla sus actividades con un enfoque sistemático y disciplinario, de manera objetiva e independiente, en cumplimiento de sus roles y en el marco del Sistema de Control Interno. En virtud de lo anterior y dando cumplimiento al Plan Anual de Auditoría del año 2024, esta oficina desarrolló una Auditoria al Proceso Gestión de la Tecnología de la Información (Incluir controles a terceros), para lo cual se solicitó el apoyo del líder del proceso evaluado respecto al acceso irrestricto a la información, atención oportuna a los requerimientos formulados por el equipo auditor y suministro de las evidencias suficientes, confiables, relevantes y útiles para respaldar los resultados finales del trabajo de auditoría. El presente informe contiene los resultados finales en relación con el objetivo, alcance y criterios definidos, con el fin de mejorar y proteger el valor institucional.

## 2. OBJETIVO Y ALCANCE

Evaluar el proceso Gestión de la Tecnología de la Información, con alcance cubre el período del 1 de mayo de 2023 al 30 de septiembre de 2024.

Con el fin de llevar cabo el cumplimiento del objetivo general, se definieron los siguientes objetivos específicos:

**2.1** Evaluar la alineación del Plan Estratégico de Tecnologías y Comunicaciones (PETI) con los objetivos y necesidades organizacionales del IDRD y el seguimiento al cronograma establecido.

**2.2** Evaluar la efectividad del Modelo de Seguridad y Privacidad de la Información (MSPI) en la protección de los datos y activos de información.

**2.3** Seguimiento a la capacidad de respuesta ante incidentes y desastres a través del Plan de Recuperación ante Desastres (DRP).

**2.4** Seguimiento al Plan de Continuidad del Negocio (BCP) para garantizar la resiliencia operativa del IDRD en situaciones de emergencia o interrupciones prolongadas.

**2.5** Verificar el aprovisionamiento de servicios (sistemas de información y capacidad de cómputo, licenciamiento, almacenamiento) de la entidad y control de terceros.

**2.6** Evaluar la gestión de riesgos frente a un incidente de datos personales del IDRD y el cumplimiento de controles en sus mapas de riesgos de gestión y corrupción.

## 3. CRITERIOS DE AUDITORIA/SEGUIMIENTO/EVALUACIÓN

- Ley 1581 de 2012” Ley de protección de datos personales”.
- Decreto 415 de 2016 “*Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones*”.
- Decreto 1008 de 2018 "Política Pública de Transformación Digital del Estado".
- Ley 1341 de 2009 "Ley General de las Tecnologías de la Información y las Comunicaciones" (TIC).
- Ley 1712 de 2014 "Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional".
- Decreto 1083 de 2015 "Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- Decreto 1078 “Reglamento Único del Sector Administrativo de Tecnologías de la Información y las Comunicaciones (TIC)”.
- Manual Operativo del Modelo Integrado de Planeación y Gestión v4 numeral 3.2.1.2.- 3.2.1.3. y v5, numeral 3.3.4 y 3.4.2 para la Política Gobierno Digital y Política de Seguridad Digital respectivamente.
- Manual MINTIC - MGPTI.G.GEN.01-Documento Maestro Modelo de Gestión de Proyectos TI.
- Resolución Número 00500 del 10 de marzo de 2021 normatividad emitida por la Agencia Nacional de Defensa Jurídica del Estado (ANDJE) en Colombia. “directrices para la implementación de políticas de seguridad digital en las entidades pública”.
- MGGTI.GE.ES.03 – Guía para la Construcción del PETI v3.0.
- La Resolución 746 de 2022 es la "Resolución por la cual se dictan disposiciones relacionadas con la protección de datos personales en Colombia".
- Guía para la preparación de las TIC para la continuidad del negocio.
- Plan estratégico de tecnologías de la información PETI 2021-2024.
- Plan estratégico de tecnologías de la información PETI 2024-2027.
- Documento Maestro del Modelo de Seguridad y Privacidad de la Información–MINTIC oct. 2021.
- Procedimientos: Gestionar Incidentes de Seguridad de la Información v5 de 2022, Gestionar la Capacidad de Infraestructura Tecnológica v3 de 2022, Asegurar el Backup de la Sede Administrativa v7 de 2021, Realizar el Mantenimiento de Infraestructura Tecnológica v5 de 2021 y Controlar los Activos Información del IDRD v2 de 2021.
- Mapa de Riesgos de Gestión y Corrupción del Proceso Gestión de Tecnologías de la Información.

## 4. METODOLOGÍA

La auditoría se desarrolló siguiendo las normas internacionales para la práctica de la auditoría interna, con el fin de obtener evidencias suficientes y objetivas, las cuales fueron objeto de verificación. Se realizó un análisis de lo general a lo específico, utilizando técnicas como solicitud

de información al proceso, revisión documental, entrevistas y mesas de trabajo, entre otras.

## 5. LIMITACIONES DE ALCANCE

Durante el trabajo de auditoría no se presentaron limitaciones de alcance que pudieran afectar los resultados y conclusiones.

## 6. INFORME EJECUTIVO

Considerando el objetivo general y el alcance de la presente evaluación, este informe abordó las principales debilidades identificadas en la gestión de Tecnologías de la Información y Comunicaciones (TIC) en el IDRD. Se reitera la observación previamente emitida en el Informe de Auditoría de 2023 relacionada con implementar lineamientos para fortalecer institucionalmente las áreas TI, incluyendo la creación de un área especializada en Tecnologías y Sistemas de Información y una gestión estratégica que garantice la gobernabilidad de las TIC.

A través de las observaciones y análisis realizados, se evidenció que la gestión actual de las TIC no cuenta con una alineación adecuada entre proyectos, iniciativas y el Plan Estratégico de Tecnologías de Información (PETI), lo que limita el avance y cumplimiento de sus objetivos. Adicionalmente, se identificaron brechas significativas en la actualización de políticas de seguridad digital y en el cumplimiento de normativas como la Ley 1712 de 2014 y la Ley 1581 de 2012, generando riesgos de incumplimiento normativo y afectaciones a la seguridad de la información, en especial de datos sensibles.

Este informe también destaca la urgencia de actualizar el Manual de Políticas de Seguridad Digital, establecer un Plan de Continuidad del Negocio (BCP) y alinear el Plan de Recuperación de Desastres (PRD) con los estándares técnicos, asegurando así la sostenibilidad de los servicios críticos. Finalmente, se enfatiza la importancia de fortalecer la infraestructura digital del IDRD y adoptar herramientas que faciliten la gestión de derechos de los titulares y la mejora continua de la seguridad de la información.

Con el fin de mejorar y proteger el valor institucional, se identifican las siguientes observaciones, oportunidades de mejora y recomendaciones para su consideración y definición de acciones de mejora. Así mismo, se resaltan las siguientes fortalezas identificadas durante la ejecución del trabajo de auditoría.

**Fortalezas:**

Se destaca que el Proceso de Gestión de Tecnología, a pesar de no estar plenamente alineado estratégicamente dentro de la estructura organizacional del IDRD, aporta un valor significativo al desarrollo misional de la entidad. Este proceso ha demostrado su capacidad para crear y formular mejoras importantes como la gestión realizada en el aplicativo Portal Contratista del IDRD; así como el desarrollo de otros sistemas de información. También se resalta el alto grado de compromiso y dedicación de los colaboradores del equipo TIC.

## Observaciones:

**Tabla No. 01 observaciones**

| No. | Observación | Recomendación |
|---|---|---|
| 1 | La revisión de las iniciativas del PETI revela una falta de soporte en la medición de indicadores clave, lo cual compromete la evaluación efectiva del progreso y desempeño de las iniciativas. Este problema se origina, en parte, porque la gestión de las Tecnologías de la Información no está estructurada como una oficina estratégica dentro del IDRD, limitando su capacidad de actuar como un habilitador clave de los objetivos organizacionales. Comprometiendo el cumplimiento del ***responsable de liderar la implementación de la Política de Gobierno Digital***: *El Director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, de la respectiva entidad, tendrá la responsabilidad de liderar la implementación de la Política de Gobierno Digital. Las demás áreas de la respectiva entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.*<br><br>*El Director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad, de acuerdo a lo establecido en el artículo 2.2.3.5.4. del Decreto Único Reglamentario de Función Pública 1083 de 2015.* Estas normativas consolidan la creación y el rol estratégico de las Oficinas TIC en las entidades públicas de Colombia, enfatizando su responsabilidad en la planificación, implementación y gestión de las tecnologías de la información para el cumplimiento de los objetivos institucionales y la mejora de los servicios a la ciudadanía. Además, se han observado retrasos en los cronogramas estipulados, lo que afecta el logro de las metas planificadas e incumplimiento de la misionalidad de la Entidad. Estos retrasos son consecuencia de una falta de planificación estratégica centralizada y supervisión directa desde un área especializada en TIC que articule, priorice y garantice el cumplimiento de los compromisos establecidos en el PETI que es regido principalmente por el MinTIC y el DAFP, con el respaldo de normativas como el *Decreto 1008 de 2018, el Decreto 1078 de 2015 y la Ley 1341 de 2009.* Su implementación está a cargo de las Oficinas TIC de las entidades públicas, quienes deben alinearlo con la estrategia institucional y la transformación digital. | Se recomienda implementar un modelo estratégico para la gestión de TIC, que contemple la creación de una oficina de Tecnologías y Sistemas de Implementar un modelo estratégico para la gestión de TIC, que contemple la creación de una oficina de Tecnologías y Sistemas de Información con enfoque estratégico. Esta oficina debe estar empoderada para liderar la planificación, ejecución y monitoreo de proyectos TIC, así como para garantizar el cumplimiento de los indicadores clave de desempeño y cronogramas estipulados. La consolidación de esta estructura fortalecerá el alineamiento de las iniciativas del PETI 2024-2027 con los objetivos estratégicos del IDRD, optimizando la gestión de los recursos tecnológicos y contribuyendo al logro de las metas institucionales. |

| No. | Observación | Recomendación |
|---|---|---|
| 2 | La falta de documentación formalizada dentro del sistema de gestión ISOLUCIÓN, junto con las inconsistencias en la medición de indicadores y los retrasos en los cronogramas de las iniciativas del PETI, plantea serios desafíos para el cumplimiento normativo y la gestión eficiente de los procesos del IDRD. Esta situación no solo dificulta la estandarización de procesos, sino que también compromete el cumplimiento de la *Ley 1712 de 2014*, que exige la transparencia y accesibilidad de la información pública. La ausencia de normatividad completa en los documentos del PETI genera un posible riesgo de aplicar normas derogadas o en su defecto la inobservancia respecto a nuevas directrices que a futuro pueden ocasionar sanciones por parte de los entes de control y podría afectar negativamente la toma de decisiones estratégicas y el logro de los objetivos institucionales. | Formalizar la "*Política de manejo de documentos electrónicos"* en el sistema ISOLUCIÓN para asegurar la estandarización de los procesos y el cumplimiento de la normativa vigente. Se recomienda implementar un sistema de seguimiento y medición de indicadores para garantizar una evaluación precisa del progreso de las iniciativas, y ajustar los cronogramas para evitar futuros incumplimientos. Además, es crucial completar la normatividad en los documentos del PETI, asegurando su fácil acceso y cumplimiento con la *Ley 1712 de 2014*, para mejorar la transparencia y reducir el riesgo de aplicar normas derogadas o en su defecto la inobservancia respecto a nuevas directrices que a futuro pueden ocasionar sanciones por parte de los entes de control y podría afectar negativamente la toma de decisiones estratégicas y el logro de los objetivos institucionales |
| 3 | De acuerdo con la revisión efectuada por el equipo auditor, se identificó que el Manual de Políticas de Seguridad Digital y de la Información, en su versión de 2019, no ha sido revisado ni actualizado desde el 31 de diciembre de ese año. Esta situación se debe a la falta de un proceso establecido para llevar a cabo revisiones periódicas. La ausencia de actualizaciones ha generado una desalineación con lo establecido en el *Decreto 1083 de 2015*, Sector de Función Pública, específicamente en el *artículo 2.2.35.3, numeral 3,* que dispone la necesidad de desarrollar lineamientos tecnológicos que definan políticas, estrategias y prácticas para mejorar la gestión institucional y garantizar la prestación efectiva de servicios. Además, dicho artículo enfatiza la importancia de asegurar el cumplimiento y la actualización de políticas y estándares relacionados con las Tecnologías de la Información y las Comunicaciones (TIC), lo cual no se está cumpliendo en su totalidad. | Implementar un proceso formal y documentado para la revisión y actualización anual del Manual de Políticas de Seguridad Digital y de la Información, garantizando su alineación con el *Decreto 1083 de 2015, artículo 2.2.35.3, numeral 3* y la en la *Resolución Número 00500 del 10 de marzo de 2021*. Este proceso debe incluir la designación de un responsable para supervisar las revisiones, así como un cronograma claro y mecanismos de control que aseguren el cumplimiento de los objetivos normativos, promoviendo la pertinencia y efectividad de las políticas en la gestión de las Tecnologías de la Información y las Comunicaciones (TIC). |

| No. | Observación | Recomendación |
|---|---|---|
| 4 | Se observó que, aunque existe una política de seguridad publicada y roles definidos, revisada por última vez en 2022, presenta brechas significativas en su actualización, incumpliendo la *Resolución Número 00500 del 10 de marzo de 2021* que requiere el uso del *"Formato Manual de Políticas de Seguridad de la Información" y se especifica que "las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente".* Esta situación, junto con la falta de protocolos actualizados para tareas críticas y la ausencia de especificaciones de seguridad en acuerdos con proveedores, compromete la eficacia de las políticas de seguridad en mantener la confidencialidad, integridad y disponibilidad de la información. Además, existen deficiencias en la gestión de acceso, criptografía, seguridad física, y otras áreas clave, que requieren atención para cumplir con las normativas vigentes y asegurar una adecuada protección de los datos. | Actualizar la política de seguridad de la información para cumplir con *Resolución Número 00500 del 10 de marzo de 2021 y la resolución 746 de 2022, en su artículo 6.1,* asegurando revisiones periódicas y una socialización efectiva entre los empleados mediante capacitación y comunicación interna. Además, se deben desarrollar protocolos actualizados para tareas críticas, integrar evaluaciones de riesgos en todas las etapas de los proyectos, y aplicar controles compensatorios donde no sea viable separar tareas. En el ámbito de las relaciones con proveedores, es crucial actualizar los ANS para incluir cláusulas de seguridad y ciberseguridad y establecer auditorías periódicas. También se recomienda mejorar las políticas de control de acceso, criptografía, y realizar pruebas regulares de sistemas de seguridad física y de recuperación de datos para asegurar la resiliencia de la infraestructura del IDRD. |
| 5 | La auditoría identificó que el Plan de Recuperación de Desastres (PRD) del IDRD no cumple con estándares técnicos adecuados, comprometiendo la imagen reputacional del instituto al carecer de integración con documentos críticos relacionados, como el Análisis de Impacto al Negocio y un inventario de recursos críticos necesarios para consolidar prioridades y garantizar la continuidad operativa. Así mismo, se evidenció la falta de estrategias claras para la validación de respaldos y la ausencia de procedimientos específicos para actualizar y probar periódicamente el PRD, elementos esenciales para cumplir con el *Decreto 1078 de 2015*, que exige la mitigación de riesgos y la continuidad de servicios bajo la Política de Gobierno Digital. Estas carencias, unidas a la falta de un desglose preciso de roles y responsabilidades y un plan de comunicación efectivo, dificultan la respuesta ante incidentes críticos, condicionando la capacidad de la entidad para anticiparse y responder a las necesidades de la ciudadanía de forma oportuna lo que podría dejar al IDRD expuesta a nuevas amenazas. | Incorporar un Análisis de Impacto al Negocio (BIA) permitirá identificar y priorizar los procesos críticos al documentar las interdependencias entre procesos, tecnología y personal, asegurando así una base sólida para la continuidad operativa. Además, es fundamental fortalecer el inventario de recursos críticos mediante el desarrollo de un registro que incluya hardware, software, servicios en la nube, instalaciones, proveedores externos y personal clave, garantizando su disponibilidad en situaciones de crisis. Se recomienda, además, definir roles y responsabilidades claras para la ejecución del PRD, implementar estrategias específicas para la validación periódica de respaldos y establecer un plan de comunicación que facilite la coordinación durante incidentes críticos. Finalmente, incluir un cronograma de pruebas periódicas y mecanismos para actualizar el PRD ante cambios en el entorno tecnológico o normativo permitirá garantizar su eficacia y alineación con los requisitos establecidos en el Decreto 1078 de 2015. |
| 6 | La ausencia de un Plan de Continuidad del Negocio (BCP) documentado y específico para el IDRD, particularmente en el ámbito de las Tecnologías de la Información y Comunicación (TIC), limita su capacidad para manejar y recuperarse de interrupciones significativas. Esto pone en riesgo la continuidad operativa de servicios críticos, lo cual podría tener consecuencias negativas en la prestación de servicios esenciales a la comunidad. Además, esta situación no cumple con normativas vigentes, como el Decreto 1078 de 2015 y *el Plan* | Desarrollar e implementar un Plan de Continuidad del Negocio (BCP) enfocado en las Tecnologías de la Información y Comunicación (TIC), alineado con el Decreto 1078 de 2015 y el Plan Distrital de Gestión del Riesgo. Este plan debe incluir un Análisis de Impacto al Negocio (BIA) que permita identificar procesos críticos y sus interdependencias, así como estrategias para mitigar riesgos asociados con la continuidad operativa. Así mismo, es necesario definir procedimientos claros para la respuesta y recuperación ante interrupciones, establecer roles y |

| No. | Observación | Recomendación |
|---|---|---|
| | *Distrital de Gestión del Riesgo*, que exigen planes de continuidad en entidades públicas. Actualmente, no existen mecanismos efectivos para evaluar y mitigar los riesgos asociados con la continuidad operativa de los servicios TIC del IDRD. | responsabilidades específicas, y diseñar un plan de comunicación que facilite la coordinación en situaciones de crisis. Adicionalmente, se sugiere implementar un cronograma de pruebas periódicas y un mecanismo para actualizar el plan de forma continua, asegurando su relevancia frente a cambios tecnológicos, organizacionales o normativos. Finalmente, la creación de un comité de continuidad encargado de gestionar, supervisar y promover la cultura de resiliencia garantizará la sostenibilidad operativa del IDRD frente a posibles interrupciones. |
| 7 | En el análisis de los riesgos asociados a los sistemas operativos cercanos al fin de su soporte, se evidenció que está comprometida la continuidad operativa de la infraestructura tecnológica al dificultar la respuesta ante vulnerabilidades emergentes. Esta situación aumenta los riesgos de seguridad y condiciona la capacidad de la entidad para mantener servicios estables y confiables. Así mismo, la falta de una estrategia de migración clara y la complejidad añadida por la diversidad de plataformas limitan la implementación uniforme de actualizaciones y el control de accesos, poniendo en riesgo el cumplimiento de la conformidad con normativas como la *Ley 1581 de 2012*, que exige medidas técnicas y administrativas para proteger los datos personales de posibles incidentes. Como consecuencia, el IDRD podría enfrentar interrupciones en sus servicios críticos, una mayor exposición a ciberataques y sanciones legales por el incumplimiento de sus obligaciones normativas, afectando la confianza de la ciudadanía en la entidad. | Actualizar los sistemas operativos que están próximos a quedarse sin soporte es crucial para garantizar la seguridad y funcionalidad de las plataformas tecnológicas. Por ejemplo, Windows Server 2016 Datacenter debe ser actualizado a una versión más reciente, como Windows Server 2019 o 2022, lo que permitirá continuar recibiendo actualizaciones de seguridad y acceder a nuevas funcionalidades que mejoren el rendimiento y la protección del entorno. De manera similar, es necesario planificar la transición de sistemas como CentOS 7 para asegurar que estos sistemas sigan siendo seguros y eficientes.<br><br>En el caso de equipos de cómputo que aún operan con sistemas obsoletos como Windows 7, cuyo soporte finalizó en enero de 2020, es fundamental actualizarlos, ya que estos representan una grave vulnerabilidad en materia de seguridad de la información. La falta de actualizaciones expone estos sistemas a riesgos significativos, como la pérdida de confidencialidad, integridad y disponibilidad de datos sensibles y personales.<br><br>Tomar estas medidas de actualización reducirá significativamente los riesgos de seguridad y garantizará un entorno tecnológico confiable y eficiente dando cumplimiento a la *Ley 1581 de 2012.* |

| No. | Observación | Recomendación |
|---|---|---|
| 8 | Se ha identificado que la falta de actualización y alineación de las políticas de protección de datos con la normativa vigente está comprometiendo la seguridad de los datos personales, en especial los de menores de edad, lo que constituye un incumplimiento de la *Ley 1581 de 2012*, que exige garantizar medidas técnicas, humanas y administrativas para la protección de esta información. Además, el uso de sistemas operativos desactualizados expone estos datos a riesgos significativos de seguridad, incrementando la probabilidad de brechas de datos y accesos no autorizados. Esta situación pone en riesgo tanto la integridad de la información gestionada por el IDRD como el cumplimiento de sus obligaciones legales, afectando la confianza de la ciudadanía. Es fundamental implementar de inmediato una matriz para la clasificación de incidentes y optimizar las herramientas de monitoreo para mitigar estos riesgos. | Verificar y actualizar la política de protección de datos del IDRD, garantizando su alineación con las directrices más recientes de la Superintendencia de Industria y Comercio (SIC) y cualquier cambio legislativo o jurisprudencial posterior a 2018, aplicable a Bogotá. Esta actualización debe incluir medidas específicas para la protección de datos de menores de edad y la integración de sistemas tecnológicos seguros. Además, se sugiere realizar un diagnóstico de los sistemas operativos y avanzar en un plan de actualización tecnológica para garantizar la seguridad de la información y el cumplimiento de las normativas vigentes, minimizando riesgos legales y operativos. |

Fuente: Elaboración propia OCI.

## Oportunidades de Mejora:

**Tabla No. 02 oportunidades de mejora**

| No. | Oportunidad de Mejora | Recomendación |
|---|---|---|
| 1 | Revisar y mejorar las prácticas de gestión de proyectos en el PMO es crucial para asegurar que los proyectos se desarrollen dentro de los plazos y recursos previstos. | Desde la Alta Dirección, analizar la importancia de implementar lineamientos para el fortalecimiento institucional en materia de TIC, a través del posicionamiento de líderes de TI y la estructuración de un área propia de Tecnologías y Sistemas de Información. Centralizar la supervisión de los proyectos de TI, articulados con las iniciativas del PETI 2024-2027, permitirá un control directo desde la formulación hasta el cierre, optimizando la gestión de proyectos. |
| 2 | Desarrollar mecanismos más efectivos para la participación ciudadana, permitiendo que los ciudadanos accedan y contribuyan a la toma de decisiones de manera eficiente. | Estructurar un repositorio central de documentos de los proyectos que cumpla con los estándares definidos. Este repositorio facilitará a los ciudadanos el acceso a la información necesaria para participar activamente en la toma de decisiones, mejorando así la transparencia y la colaboración ciudadana. |
| 3 | Mejorar la implementación del Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) es esencial para asegurar el cumplimiento con las normativas y recomendaciones pertinentes, facilitando el acceso y gestión documental. | Aprobar, actualizar y formalizar el estado actual del proceso de Gestión de Tecnologías de la Información en el Sistema de Gestión ISOLUCIÓN. Esto garantizará que el SGDEA sea utilizado de manera efectiva, mejorando la organización y accesibilidad de los documentos electrónicos de archivo. |

Fuente: Elaboración propia OCI.

**Recomendaciones:**

- Diseñar un plan de comunicación estructurado que establezca guías claras para notificar a las partes interesadas y defina canales de comunicación alternativos durante emergencias. Así mismo, es crucial establecer procedimientos de recuperación alternativos, documentando acciones específicas para restaurar sistemas desde backups, asegurando la realización de pruebas de integridad de datos y funcionalidad para garantizar una recuperación eficiente y coordinada (Recomendación No. 08).

- Llevar a cabo pruebas periódicas para evaluar la eficiencia del plan de recuperación, lo que permitirá identificar y ajustar cualquier deficiencia detectada, asegurando así que el plan se mantenga efectivo y alineado con las mejores prácticas y necesidades organizacionales (Recomendación No. 09).

- Definir e implementar indicadores clave de desempeño (KPIs) de continuidad, como el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO), para medir la eficacia del proceso de recuperación y asegurar que el plan se mantenga alineado con las mejores prácticas y necesidades organizacionales (Recomendación No. 10).

- Actualizar el Plan de Recuperación de Desastres (DRP) mediante un mecanismo de revisión continua que se adapte a nuevas tecnologías y cambios organizacionales. Además, se debe formalizar una política de recuperación que refleje el compromiso de la organización con la implementación y mantenimiento del DRP, asegurando su alineación con las normativas vigentes (Recomendación No. 11).

- Reducir la diversidad de distribuciones Linux en uso ayudará a simplificar la administración y el mantenimiento de los sistemas. Consolidar en distribuciones como Ubuntu LTS o alternativas Red Hat/CentOS, según las necesidades específicas de la organización, puede mejorar la eficacia operativa y facilitar la gestión de parches y actualizaciones (Recomendación No. 14).

- Implementar una Política Robusta de Gestión de Parches: Automatizar las actualizaciones críticas en los sistemas soportados es fundamental para minimizar el riesgo de explotación de vulnerabilidades conocidas. Una política eficaz debe asegurar que todos los sistemas estén actualizados de manera oportuna, reduciendo así la exposición a amenazas de seguridad (Recomendación No. 15).

- Verificar la configuración de cada sistema operativo para garantizar la seguridad. Esto incluye la implementación de contraseñas seguras y la autenticación multifactorial (MFA), así como la configuración adecuada de firewalls internos y externos. Además, desactivar servicios

innecesarios puede reducir la superficie de ataque, contribuyendo a un entorno más seguro (Recomendación No. 16).

- Utilizar herramientas como Zabbix para el monitoreo en tiempo real de los sistemas asegura la detección y respuesta rápida a incidentes. Es importante garantizar que todos los sistemas tengan backups frecuentes y probados, cubriendo bases de datos críticas y sistemas clave, para asegurar la recuperación rápida ante fallos (Recomendación No. 17).

- Para sistemas que no ofrecen soporte extendido definir plazos claros para actualizar o reemplazar antes de que se conviertan en vulnerabilidades críticas. Este enfoque asegura la continuidad operativa y la seguridad del entorno tecnológico (Recomendación No. 18).

- Migrar instancias de Ubuntu 20.04 LTS a 22.04 o superior antes del fin de soporte en abril de 2025 es crucial para mantener el soporte. También se debe considerar la consolidación de Debian y Ubuntu en una única distribución para simplificar la administración y optimizar recursos. (Recomendación No. 19).

- Implementar controles centralizados para monitorear actualizaciones de seguridad en todas las versiones activas de Ubuntu y Debian es necesario. Establecer una estrategia de seguridad unificada para todos los entornos Linux asegura consistencia en la protección y mejora la respuesta ante incidentes. (Recomendación No. 20).

- Consolidar sistemas de pruebas para reducir la duplicación de recursos y costos es una medida eficaz. Implementar medidas de seguridad específicas, como el aislamiento de red, garantizará un entorno de pruebas seguro y controlado (Recomendación No. 21).

- Monitorear el vencimiento de la licencia de PanOS y planificar renovaciones con anticipación es crucial para evitar interrupciones de servicio. Además, asegurar el cumplimiento de términos en Oracle Linux evitará penalidades costosas (Recomendación No. 22).

- Ampliar el esquema de backups más allá de Veeam Backup es vital para asegurar una cobertura completa para bases de datos críticos y sistemas esenciales como Orfeo BD y GitLab, garantizando así la recuperación rápida y efectiva ante cualquier fallo (Recomendación No. 23).

- Implementar un proceso continuo para evaluar los riesgos asociados al tratamiento de datos personales, especialmente en proyectos que involucran tecnologías emergentes o nuevas actividades del IDRD. Esto es crucial para mitigar los riesgos identificados en la observación sobre la seguridad de los datos personales de menores (Recomendación No. 25).

- Asegurar la comprensión y el cumplimiento de las políticas de tratamiento de datos por parte de todos los empleados y contratistas a través de sesiones regulares de capacitación. Esto fortalecerá la cultura de protección de datos dentro del IDRD (Recomendación No. 26).

- Desarrollar protocolos detallados para la recolección, uso y almacenamiento de datos sensibles y de menores, con un enfoque particular en actividades específicas del IDRD, como deportes o eventos culturales. Esto abordará directamente la preocupación sobre la seguridad de los datos de menores (Recomendación No. 27).

- Integrar herramientas digitales avanzadas para facilitar la gestión de derechos de los titulares, como formularios electrónicos fácilmente accesibles desde la página web oficial del IDRD. Esto mejorará la accesibilidad y la gestión eficiente de los derechos de los ciudadanos (Recomendación No. 28).

- Reforzar los avisos de privacidad, asegurando que estén redactados en un lenguaje claro y comprensible para los ciudadanos, especialmente en actividades públicas organizadas por el IDRD. Esto fomentará la confianza y la transparencia en el manejo de datos personales (Recomendación No. 29).

## 7. RESULTADOS

La Oficina de Control Interno – OCI, dentro del marco de la Auditoria Proceso Gestión de la Tecnología de la Información realizó la solicitud de información mediante el radicado No. 20241500499443 del 13-11-2024, para lo cual se brindó respuesta por parte del proceso auditado mediante el cargue de todos los soportes al drive creado por la OCI https://drive.google.com/drive/folders/1KAVLrRsYzlKzE2fvLq4JriNNPU_Jn75n el 18-11-2024.

De conformidad con la información suministrada por el Proceso Gestión de la Tecnología de la Información, la OCI procedió a realizar el análisis y evaluación mediante el Informe Preliminar remitido por la OCI con memorando radicado N° 20241500548003 del 12-12-2024, con respuesta por parte del proceso de Gestión de la Tecnología de la Información mediante radicado No. 20243000555393 del 17-12-2024, la oficina de control Interno procedió a realizar el siguiente análisis y evaluación para realizar la entrega de este informe final.

### 7.1 EVALUAR LA ALINEACIÓN DEL PLAN ESTRATÉGICO DE TECNOLOGÍAS Y COMUNICACIONES (PETI) CON LOS OBJETIVOS Y NECESIDADES ORGANIZACIONALES DEL IDRD Y EL SEGUIMIENTO AL CRONOGRAMA ESTABLECIDO.

Uno de los objetivos específicos de esta auditoría fue verificar el cumplimiento de la gestión efectuada por el IDRD en el desarrollo e implementación de Proyectos y Gobierno Digital, a través de la evaluación del Plan Estratégico de Tecnologías y Comunicaciones (PETI).

**Generalidades del PETI:** Siguiendo la Resolución 04 de 2017 y el Decreto 415 de 2016, esta oficina verificó la implementación y seguimiento del Plan Estratégico de Tecnologías de la Información. La información del documento fue comparada con los entregables previstos en la Guía para la construcción del PETI versión 2019 del Ministerio de Tecnologías de la Información y las Comunicaciones, así como con la información proporcionada por el proceso a través de correo electrónico, en relación con las siguientes iniciativas:

**Tabla 3. Iniciativas PETI 2021 – 2024.**

| INICIATIVA | DESCRIPCIÓN |
|---|---|
| Consolidación estratégica de TI | Reestructurar el Área de TI para que se convierta en un proceso Estratégico y cuente con las herramientas necesarias para la formulación y gestión de Proyectos de TI que generen un alto impacto en la entidad. |
| Implementación Marco de Transformación Digital | Asegurar el cumplimiento de los lineamientos del Marco de Transformación Digital. |
| Definición y dimensionamiento de la Arquitectura Empresarial | Ejecutar de forma incremental, un ejercicio de Arquitectura Empresarial que cubra de manera priorizada las Áreas de la institución. |
| Arquitectura de Sistemas de Información | Implementar las herramientas tecnológicas de la entidad en todo su potencial, ajustando sus funcionalidades e interoperabilidad entre los sistemas de Información. |
| Participación ciudadana | Implementar mecanismos para habilitar la participación ciudadana, recopilando las comunicaciones generadas en los diversos canales, con el objetivo de mejorar la toma de decisiones estratégicas. |
| Fortalecimiento SIM | Implementar mejoras en el SIM, ampliar sus funcionalidades para incluir servicios geográficos, permitir una comunicación más efectiva con la ciudadanía y de análisis de datos para la toma de decisiones estratégicas. |
| Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) | Habilitar las capacidades tecnológicas necesarias en el IDRD para la gestión documental electrónica del archivo de la entidad, que contemple las recomendaciones, conceptos y normativas expedidas por el Archivo General de la Nación y los referentes internacionales competentes e idóneos en la materia. |
| Seguridad e Infraestructura | Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas |

Fuente: Elaboración propia con base en Información suministrada por el proceso.

Ahora bien, El Plan Estratégico de Tecnologías de la Información (PETI) 2021–2024 detalló los entregables, indicadores, recursos y cronogramas para cada iniciativa, alineados con los objetivos del IDRD. Durante esta auditoría, se realizó un análisis y validación de las evidencias documentales y se llevaron a cabo mesas de trabajo colaborativas. Estas acciones confirmaron la correcta implementación de los componentes del PETI, asegurando que las acciones estén en línea con las metas establecidas y garantizando la efectividad del plan estratégico, como se muestra en la siguiente tabla:

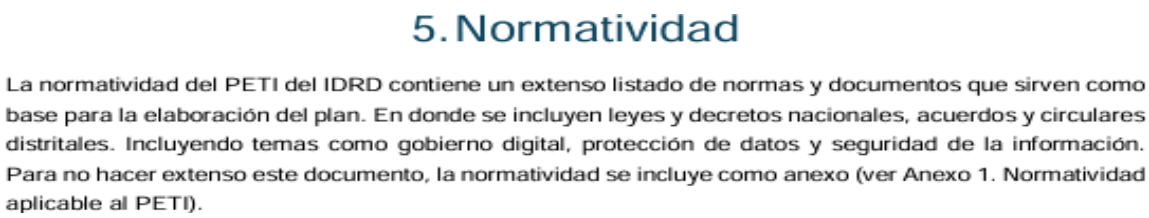
**Tabla 4. Validación Iniciativas PETI 2021 – 2024.**

| INICIATIVA | VALIDACIÓN ENTREGABLES | VALIDACIÓN INDICADORES | VALIDACIÓN CRONOGRAMA |
|---|---|---|---|
| Consolidación estratégica de TI | - No se cuenta con el Acto administrativo que reclasificó el área de TI como un proceso estratégico.<br><br>- Se cuenta con manuales e instructivos para la Gestión de Proyectos TI; no obstante, éstos no están formalizados en el Sistema de Gestión ISOLUCIÓN.<br><br>- El IDRD cuenta con la oficina de proyectos – PMO, táctica para gestionar los proyectos priorizados en PETI 2021-2024 | No se evidenció soportes de medición a la fecha, de los tres (3) indicadores establecidos en la Ficha de Iniciativa P01 del PETI. | **Fecha inicio:** 01-jun-2021<br>**Fecha fin:** 26-may-2022<br>No se cumplió con el cronograma inicial establecido en el PETI, teniendo en cuenta la fecha de finalización del proyecto de Gobierno TI, tiene fecha de finalización a 29-dic-2023. |
| Implementación Marco de Transformación Digital | - No se evidencia documento donde se defina y prioricen los lineamientos no cubiertos en otras iniciativas.<br><br>- No se cuenta con soporte de estudio y dimensionamiento para la definición de recursos requeridos. | No se evidenció soportes de medición a la fecha, del indicador establecido en la Ficha de Iniciativa P02 del PETI. | **Fecha inicio:** 1-may-2021<br>**Fecha fin:** 15-abr-2024<br>Si bien la iniciativa aún se encuentra dentro de tiempo de ejecución, no es claro a cuál es el estado de avance, pues los soportes remitidos dan cuenta del avance de los proyectos asociados a la misma (los cuales no hacen parte del alcance del PETI ni se encuentran formalmente documentados). **(*)** |
| Definición y dimensionamiento de la Arquitectura Empresarial | Los entregables definidos en PETI 2021-2024 no se cumplieron en razón a que el proyecto se cerró, para lo cual el proceso señaló: "*Se realizó proceso de cotización a través de la plataforma SECOP y se realizó un análisis de precios que condujo a la decisión de no llevar a cabo el ejercicio en razón a los costos asociados al mismo, los cuales no se encontraban presupuestados. Así mismo el Instituto no cuenta con el personal idóneo para llevarlo a cabo de manera interna*". | No se evidenció soportes de medición a la fecha, de los tres (3) indicadores establecidos en la Ficha de Iniciativa P03 del PETI. | **Fecha inicio:** 28-sep-2021<br>**Fecha fin:** 21-mar-2023<br>El proceso manifestó a través del documento soporte allegado *"PMO_ Consolidado de avances PETI_V1",* que la iniciativa fue cerrada, por ende, no hay trazabilidad reciente sobre su ejecución. |
| Participación ciudadana | Se definieron tres (3) entregables los cuales no se cumplieron dentro de las fechas iniciales establecidas en la Ficha de Iniciativa P05 del PETI. Lo anterior, toda vez que, los proyectos asociados a la iniciativa, aún se encuentran en ejecución. **(*)** | Se formularon dos (2) indicadores, los cuales no fue posible validar dado que no se hizo entrega de su medición. | **Fecha inicio:** 27-mar-2022<br>**Fecha fin:** 21-mar-2023<br>Los proyectos que hacen parte de esta iniciativa terminaron en diciembre de 2023. **(*)** |
| Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) | Actividad cumplida: Se observó que el IDRD cuenta con la *"Política de manejo de documentos electrónicos",* aprobada en Comité Institucional de Gestión y Desempeño mediante Acta No 03 el 07 de diciembre de 2022; sin embargo, el | De los cuatro (4) indicadores formulados en la Ficha de Iniciativa P07 del PETI, se valida el cumplimiento | **Fecha inicio:** 27-mar-2022<br>**Fecha fin:** 15-mar-2024<br>El Proyecto aún se encuentra en términos para su culminación. |

| INICIATIVA | VALIDACIÓN ENTREGABLES | VALIDACIÓN INDICADORES | VALIDACIÓN CRONOGRAMA |
|---|---|---|---|
| | documento no se encuentra formalizado en el Sistema de Gestión ISOLUCIÓN. Ahora bien, en relación con los tres (3) entregables restantes establecidos en la Ficha de Iniciativa P07 del PETI, no fue posible realizar su verificación, toda vez que el proceso no se hizo entrega puntual de cada uno. | del *"Porcentaje de avance en definición de política de manejo de documentos Electrónicos"*. No obstante, no se evidencia soportes de medición a la fecha, de los tres (3) indicadores restantes establecidos en la Ficha. | |

Fuente: INFORME FINAL DE AUDITORÍA IINTERNA A LAS TIC DEL IDRD, FORMULACIÓN Y CUMPLIMIENTO PETI, POLÍTICA DE SEGURIDAD INSTITUCIONAL, CONTROLES IMPLEMENTADOS Y FUNCIONAMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA – agosto 2023

Siguiendo lo establecido en la Resolución 04 de 2017 y el Decreto 415 de 2016, esta oficina llevó a cabo la validación de la implementación y seguimiento del Plan Estratégico de Tecnologías de la Información. Al cotejar la información del documento con los entregables especificados en la Guía para la construcción del PETI versión 2023 del Ministerio de Tecnologías de la Información y las Comunicaciones, y con la información proporcionada por correo electrónico, se identificó que el documento carece de la normatividad descrita en la guía. Esta omisión se evidencia claramente en la captura de pantalla que se muestra a continuación.




Fuente: Plan-Estrategico-de-Tecnologias-de-la-Informacion-IDRD-PETI-2024-2027v1.9

Para evaluar la alineación del Plan Estratégico de Tecnologías y Comunicaciones (PETI) con los objetivos y necesidades del IDRD, es esencial cumplir con la actividad 6.1 de la guía del MinTIC. En particular, el numeral 3 de la actividad 6.1.1, que se centra en "*Identificar y levantar el listado de normatividad que afecta e incide en la operación de la entidad*," debe estar claramente reflejado en el documento. Esto es fundamental para cumplir con la Ley 1712 de 2014 (Ley de Transparencia y Derecho al Acceso a la Información Pública Nacional), que exige que los sistemas de información y documentos electrónicos aseguren un acceso eficiente y accesible a la información pública. Actualmente, al encontrarse en un anexo de difícil ubicación, se dificulta el acceso eficiente para la ciudadanía, además se evidenció lo siguiente:

- **Falta de Documentación Formalizada**: De acuerdo con la revisión del sistema de gestión ISOLUCIÓN y los manuales e instructivos evaluados, se observó que estos documentos no están formalizados correctamente. Esta situación dificulta la estandarización de procesos y el

cumplimiento normativo, lo cual podría ocasionar inconsistencias en la ejecución de las iniciativas del PETI.

- **Inconsistencias en la Medición de Indicadores**: Según los registros de las iniciativas del PETI, no se evidenció el soporte de medición para varios indicadores establecidos. Esta falta de documentación compromete la evaluación eficaz del progreso y desempeño de las iniciativas, lo que puede llevar a una interpretación inexacta de sus resultados y afectaciones en la toma de decisiones estratégicas.

- **Retrasos en Cronogramas**: De los cronogramas revisados, se constató que algunas iniciativas no cumplieron con los plazos estipulados. Este incumplimiento puede generar desalineación con los objetivos estratégicos del IDRD y afectar el logro de las metas planificadas, incrementando el riesgo de desviaciones presupuestarias y operativas.

- **Documentación Incompleta sobre Normatividad**: En la comparación del documento del PETI 2023 con las guías normativas, se identificó la ausencia de normatividad completa. Esta deficiencia puede limitar el cumplimiento de la Ley 1712 de 2014 y afectar la transparencia y accesibilidad de la información pública, genera un posible riesgo de aplicar normas derogadas o en su defecto la inobservancia respecto a nuevas directrices que a futuro pueden ocasionar sanciones por parte de los entes de control y podría afectar negativamente la toma de decisiones estratégicas y el logro de los objetivos institucionales.

**OBSERVACIÓN No. 01:** La revisión de las iniciativas del PETI revela una falta de soporte en la medición de indicadores clave, lo cual compromete la evaluación efectiva del progreso y desempeño de las iniciativas. Este problema se origina, en parte, porque la gestión de las Tecnologías de la Información no está estructurada como una oficina estratégica dentro del IDRD, limitando su capacidad de actuar como un habilitador clave de los objetivos organizacionales. Comprometiendo el cumplimiento de: ***el responsable de liderar la implementación de la Política de Gobierno Digital****: El Director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, de la respectiva entidad, tendrá la responsabilidad de liderar la implementación de la Política de Gobierno Digital. Las demás áreas de la respectiva entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.* |

*El Director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad, de acuerdo a lo establecido en el artículo 2.2.3.5.4. del Decreto Único Reglamentario de Función Pública 1083 de 2015.* Estas normativas consolidan la creación y el rol estratégico de las Oficinas TIC en las entidades públicas de Colombia, enfatizando su responsabilidad en la planificación, implementación y gestión de las tecnologías de la información para el cumplimiento de los objetivos institucionales y la mejora de los servicios a la ciudadanía. Además, se han observado retrasos en los cronogramas estipulados, lo que afecta el logro de las metas planificadas e incumplimiento de la misionalidad de la Entidad. Estos retrasos son consecuencia

de una falta de planificación estratégica centralizada y supervisión directa desde un área especializada en TIC que articule, priorice y garantice el cumplimiento de los compromisos establecidos en el PETI que es regido principalmente por el MinTIC y el DAFP, con el respaldo de normativas como el *Decreto 1008 de 2018, el Decreto 1078 de 2015 y la Ley 1341 de 2009.* Su implementación está a cargo de las Oficinas TIC de las entidades públicas, quienes deben alinearlo con la estrategia institucional y la transformación digital.

**RECOMENDACIÓN No. 01:** Implementar un modelo estratégico para la gestión de TIC, que contemple la creación de una oficina de Tecnologías y Sistemas de Información con enfoque estratégico. Esta oficina debe estar empoderada para liderar la planificación, ejecución y monitoreo de proyectos TIC, así como para garantizar el cumplimiento de los indicadores clave de desempeño y cronogramas estipulados. La consolidación de esta estructura fortalecerá el alineamiento de las iniciativas del PETI 2024-2027 con los objetivos estratégicos del IDRD, optimizando la gestión de los recursos tecnológicos y contribuyendo al logro de las metas institucionales.

**RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

*"(…) Desde el proceso, se tiene asociada una iniciativa dentro del PETI que busca elevar la gestión de tecnologías de la información a un nivel estratégico. Para ello, se han desarrollado diversas acciones orientadas a cumplir este objetivo.*

*No obstante, se aclara que este es un elemento complejo debido a la necesidad de gestionar la modificación ante el Servicio Civil, lo que excede el alcance del proceso auditado. Esta aclaración se realiza con el fin de establecer claramente los límites de responsabilidad del proceso en cuestión "(…).*

**ANÁLISIS DE LA OFICINA DE CONTROL INTERNO FRENTE A LA RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

De acuerdo con la respuesta del área, el equipo auditor no evidenció avances en la elaboración de un cronograma o plan específico que aborde los hitos necesarios para la creación de dicha oficina en el IDRD, ni gestión ante el Departamento Administrativo del Servicio Civil, sobre el particular. Adicionalmente en la iniciativa N° 7, "*Integración Estratégica de TI*" del PETI 2024-2027, se contempla la integración y formulación de la Oficina de Tecnologías de la Información y las Comunicaciones (TIC). Durante la auditoría, no fue posible verificar la gestión requerida para la creación de la Oficina de Tecnologías de la Información y las Comunicaciones del IDRD, conforme a lo estipulado en el artículo 46 del Decreto 19 de 2012, el cual señala:

*"Las reformas de plantas de personal de empleos de las entidades de la Rama Ejecutiva de los órdenes nacional y territorial deberán motivarse y fundarse en necesidades del servicio o en razones de modernización de la Administración. Estas reformas deben basarse en justificaciones*

*o estudios técnicos que así lo demuestren, elaborados por las respectivas entidades bajo las directrices del Departamento Administrativo de la Función Pública y de la Escuela Superior de Administración Pública (ESAP)."*

De acuerdo con el análisis expuesto anteriormente, **se mantiene la observación** y su respectiva recomendación.

**OBSERVACIÓN No. 02:** La falta de documentación formalizada dentro del sistema de gestión ISOLUCIÓN, junto con las inconsistencias en la medición de indicadores y los retrasos en los cronogramas de las iniciativas del PETI, plantea serios desafíos para el cumplimiento normativo y la gestión eficiente de los procesos del IDRD. Esta situación no solo dificulta la estandarización de procesos, sino que también compromete el cumplimiento de la *Ley 1712 de 2014*, que exige la transparencia y accesibilidad de la información pública. La ausencia de normatividad completa en los documentos del PETI genera un posible riesgo de aplicar normas derogadas o en su defecto la inobservancia respecto a nuevas directrices que a futuro pueden ocasionar sanciones por parte de los entes de control y podría afectar negativamente la toma de decisiones estratégicas y el logro de los objetivos institucionales.

**RECOMENDACIÓN No. 02:** Formalizar la "*Política de manejo de documentos electrónicos"* en el sistema ISOLUCIÓN para asegurar la estandarización de los procesos y el cumplimiento de la normativa vigente. Se recomienda implementar un sistema de seguimiento y medición de indicadores para garantizar una evaluación precisa del progreso de las iniciativas, y ajustar los cronogramas para evitar futuros incumplimientos. Además, es crucial completar la normatividad en los documentos del PETI, asegurando su fácil acceso y cumplimiento con la *Ley 1712 de 2014*, para mejorar la transparencia y reducir el riesgo de aplicar normas derogadas o en su defecto la inobservancia respecto a nuevas directrices que a futuro pueden ocasionar sanciones por parte de los entes de control y podría afectar negativamente la toma de decisiones estratégicas y el logro de los objetivos institucionales

**RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

*"(…)En la formulación del nuevo PETI 2024 - 2027, se contempla la definición de cronogramas y actividades específicas, las cuales están debidamente establecidas en el plan. Estas actividades son controladas y monitoreadas por el proceso, garantizando su cumplimiento y alineación con los objetivos estratégicos. Por otro lado, se tienen indicadores los cuales se han actualizado anualmente en Isolucion para los temas de calidad del proceso de acuerdo con las prácticas recomendadas por control interno y el área asesora de planeación en la entidad. "(…).*

**ANÁLISIS DE LA OFICINA DE CONTROL INTERNO FRENTE A LA RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

Esta auditoría resalta la importancia de mantener actualizada la información generada desde el proceso de Gestión de Tecnologías de la Información del IDRD, así como su publicación oportuna en los canales dispuestos para este propósito como la plataforma Isolución. En la respuesta del proceso no se hace referencia al cargue de a información publicada que presenta un rezago, ya que varios formatos disponibles corresponden a la vigencia de 2019. Esto pone de manifiesto la necesidad de su revaloración y actualización, en cumplimiento de los lineamientos establecidos en la Política de Gobierno Digital.

Cabe mencionar que la iniciativa que se tenga desde el proceso para adelantar la gestión de estas evidencias en el nuevo PETI 2024-2027 no se pudo verificar el avance de esta meta en el periodo auditado.

De acuerdo con el análisis expuesto anteriormente, **se mantiene la observación** y su respectiva recomendación.

**OPORTUNIDAD DE MEJORA 1:** Revisar y mejorar las prácticas de gestión de proyectos en el PMO es crucial para asegurar que los proyectos se desarrollen dentro de los plazos y recursos previstos.

**RECOMENDACIÓN No. 03:** Desde la Alta Dirección, analizar la importancia de implementar lineamientos para el fortalecimiento institucional en materia de TIC, a través del posicionamiento de líderes de TI y la estructuración de un área propia de Tecnologías y Sistemas de Información. Centralizar la supervisión de los proyectos de TI, articulados con las iniciativas del PETI 2021-2024, permitirá un control directo desde la formulación hasta el cierre, optimizando la gestión de proyectos.

**RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

*"(…)En la formulación del nuevo PETI 2024 - 2027, se la formulación de la mesa de gestión del cambio proceso que se lleva adelantado y del cual permitirá llevar esas mejores prácticas de gestión de proyectos y uso de metodologías ágiles.Mesa de Gestión del Cambio v1.0.docx usp=sharing&ouid=107689048745846013506&rtpof=true&sd=true "(…).*

**ANÁLISIS DE LA OFICINA DE CONTROL INTERNO FRENTE A LA RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

Aunque el proceso indica en su respuesta que se está avanzando en la mejora de la documentación mediante la creación de un documento titulado "*Mesa de Gestión de Cambios*", durante la auditoría no fue posible verificar su aprobación ni su publicación. Así mismo se evidenció que la documentación registrada en Isolución presenta un versionamiento superior a un año, lo que indica una posible desactualización que requiere atención inmediata. Adicionalmente en el

periodo de esta auditoria el documento mencionado por el proceso en drive compartido tiene fecha de creación del 22 de diciembre de 2024, fecha que supera el alcance de esta auditoría.

De acuerdo con el análisis expuesto anteriormente, **se mantiene la oportunidad de mejora** y su respectiva recomendación.

**OPORTUNIDAD DE MEJORA 2:** Desarrollar mecanismos más efectivos para la participación ciudadana, permitiendo que los ciudadanos accedan y contribuyan a la toma de decisiones de manera eficiente.

**RECOMENDACIÓN No. 04:** Estructurar un repositorio central de documentos de los proyectos que cumpla con los estándares definidos. Este repositorio facilitará a los ciudadanos el acceso a la información necesaria para participar activamente en la toma de decisiones, mejorando así la transparencia y la colaboración ciudadana.

**RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

*"(…)La oportunidad no será tenida en cuenta dado que los servicios de participación ciudadana no forman parte del proceso de GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN a cargo del área de sistemas, se aclara que esta área brinda apoyo con los componentes tecnológicos necesarios para facilitar y mejorar dicha participación; sin embargo, el liderazgo y la responsabilidad principal de este proceso no recaen en el área de sistemas, sino en las dependencias directamente encargadas de su ejecución. "(…).*

**ANÁLISIS DE LA OFICINA DE CONTROL INTERNO FRENTE A LA RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

Aunque el proceso manifiesta que "*los servicios de participación ciudadana no forman parte del proceso de GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN a cargo del área de sistemas*", la caracterización del proceso establece que su función es "*mantener la plataforma tecnológica existente y desarrollar proyectos de manera oportuna y eficaz, así como formular lineamientos relacionados con estándares y buenas prácticas para el manejo de la información, a fin de contribuir a la eficiencia de los procesos del IDRD*".

En este contexto, resulta necesario que el proceso asuma un rol de liderazgo en el mejoramiento y la gestión de la información que se produce, obtiene y transforma, alineándose con los principios de Seguridad de la Información y Gobierno Digital. Esto es esencial para garantizar la disponibilidad, confidencialidad e integridad de la información institucional.

De acuerdo con el análisis expuesto anteriormente, **se mantiene la oportunidad de mejora** y su respectiva recomendación.

**OPORTUNIDAD DE MEJORA 3:** Mejorar la implementación del Sistema de Gestión de

Documentos Electrónicos de Archivo (SGDEA) es esencial para asegurar el cumplimiento con las normativas y recomendaciones pertinentes, facilitando el acceso y gestión documental.

**RECOMENDACIÓN No. 05:** Aprobar, actualizar y formalizar el estado actual del proceso de Gestión de Tecnologías de la Información en el Sistema de Gestión ISOLUCIÓN. Esto garantizará que el SGDEA sea utilizado de manera efectiva, mejorando la organización y accesibilidad de los documentos electrónicos de archivo.

**RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

*"(…)La oportunidad no será tenida en cuenta por cuanto la implementación del SGDEA no forma parte del proceso de GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN a cargo del área de sistemas, se aclara que esta área de sistemas brinda apoyo con los componentes tecnológicos necesarios para facilitar y mejorar dicha participación; sin embargo, el liderazgo y la responsabilidad principal de este proceso no recaen en el área de sistemas, sino en las dependencias directamente encargadas de su ejecución. "(…).*

**ANÁLISIS DE LA OFICINA DE CONTROL INTERNO FRENTE A LA RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

Aunque el proceso manifiesta que: (…)"*por cuanto la implementación del SGDEA no forma parte del proceso de GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN*", la caracterización del proceso establece que su función es "*mantener la plataforma tecnológica existente y desarrollar proyectos de manera oportuna y eficaz, así como formular lineamientos relacionados con estándares y buenas prácticas para el manejo de la información, a fin de contribuir a la eficiencia de los procesos del IDRD*".

En este contexto, la oportunidad de mejora esta direccionada a que se coordine con demás procesos a cargo de dichas actividades, para garantizar el mejoramiento y la gestión de la información que se produce, obtiene y transforma, alineándose con los principios de Seguridad de la Información y Gobierno Digital. Esto es esencial para garantizar la disponibilidad, confidencialidad e integridad de la información institucional.

De acuerdo con el análisis expuesto anteriormente, **se mantiene la oportunidad de mejora** y su respectiva recomendación.

**7.2 EVALUAR LA EFECTIVIDAD DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) EN LA PROTECCIÓN DE LOS DATOS Y ACTIVOS DE INFORMACIÓN.**

La Oficina de Control Interno en desarrollo de la presente auditoria evaluó cómo el Modelo de Seguridad y Privacidad de la Información (MSPI) del Instituto Distrital de Recreación y Deporte (IDRD) protege eficazmente los datos y activos de información. A través de un análisis de sus políticas y controles, se busca garantizar que el IDRD mantenga altos estándares de seguridad y

responda adecuadamente a los desafíos actuales.

**7.2.1 Política de Seguridad de la Información:** En el *Manual de Políticas de Seguridad Digital y de la Información*, versión 2019, se evidencia la ausencia de un proceso de actualización que cumpla con lo dispuesto en la *Resolución Número 00500 del 10 de marzo de 2021*. Esta resolución establece que los sujetos obligados deben adoptar los modelos, guías y documentos técnicos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, en el marco del habilitador de seguridad y privacidad de la información de la Política de Gobierno Digital. Asimismo, exige la incorporación de estándares internacionales y sus respectivas actualizaciones, junto con marcos de trabajo que reflejen mejores prácticas en la materia. Además, según la resolución, se requiere el uso del *"Formato Manual de Políticas de Seguridad de la Información" y se especifica que "las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente".*

**Tabla 5. Dominios Seguridad Manual de Políticas de Seguridad Digital y de la Información.**

| DOMINIO | CUMPLIMIENTO |
|---|---|
| A.5. POLITICAS DE LA SEGURIDAD DE LA INFORMACIÓN | NO ACTUAL |
| A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | NO ACTUAL |
| A.7. SEGURIDAD DE LOS RECURSOS HUMANOS | NO ACTUAL |
| A.8. GESTIÓN DE ACTIVOS | NO ACTUAL |
| A.9. CONTROL DE ACCESO | NO ACTUAL |
| A.10. CRIPTOGRAFÍA | NO ACTUAL |
| A.11. SEGURIDAD FÍSICA Y DEL ENTORNO | NO ACTUAL |
| A.12 SEGURIDAD DE LAS OPERACIONES | NO ACTUAL |
| A.13 SEGURIDAD DE LAS COMUNICACIONES | NO ACTUAL |
| A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | NO ACTUAL |
| A.15 RELACIONES CON LOS PROVEEDORES | NO ACTUAL |
| A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | NO ACTUAL |
| A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO | NO ACTUAL |
| A.18 CUMPLIMIENTO | NO ACTUAL |

Fuente: Elaboración propia con base en Información suministrada por el proceso.

El análisis de la auditoría reveló que el documento titulado "*Manual de Políticas de Seguridad Digital y de la Información*", en su versión 2019, tenía como última fecha de revisión el 31 de diciembre de 2019. Se constató que las políticas incluidas en este manual no habían sido actualizadas desde entonces, resultando en una desactualización de más de cuatro años. Este desfase vuelve prioritario la actualización de dichas políticas para garantizar su alineación con todos los dominios establecidos en la *Resolución Número 00500 del 10 de marzo de 2021*, asegurando así que cumplan con los estándares actuales de seguridad de la información.

**OBSERVACIÓN No. 03:** De acuerdo con la revisión efectuada por el equipo auditor, se identificó que el Manual de Políticas de Seguridad Digital y de la Información, en su versión de 2019, no ha sido revisado ni actualizado desde el 31 de diciembre de ese año. Esta situación se debe a la falta de un proceso establecido para llevar a cabo revisiones periódicas. La ausencia de actualizaciones ha generado una desalineación con lo establecido en el *Decreto 1083 de 2015*, Sector de Función Pública, específicamente en el *artículo 2.2.35.3, numeral 3,* que dispone la necesidad de desarrollar lineamientos tecnológicos que definan políticas, estrategias y prácticas para mejorar la gestión institucional y garantizar la prestación efectiva de servicios. Además, dicho artículo enfatiza la importancia de asegurar el cumplimiento y la actualización de políticas y estándares relacionados con las Tecnologías de la Información y las Comunicaciones (TIC), lo cual no se está cumpliendo en su totalidad.

**RECOMENDACIÓN No. 06:** Implementar un proceso formal y documentado para la revisión y actualización anual del Manual de Políticas de Seguridad Digital y de la Información, garantizando su alineación con el *Decreto 1083 de 2015, artículo 2.2.35.3, numeral 3* y la en la *Resolución Número 00500 del 10 de marzo de 2021*. Este proceso debe incluir la designación de un responsable para supervisar las revisiones, así como un cronograma claro y mecanismos de control que aseguren el cumplimiento de los objetivos normativos, promoviendo la pertinencia y efectividad de las políticas en la gestión de las Tecnologías de la Información y las Comunicaciones (TIC).

**RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

*"(…)En la formulación del nuevo PETI 2024 - 2027, se contempla una iniciativa denominada Modelo de Ciberseguridad y MSPI donde se contempla la actualización del presente manual."(…).*

**ANÁLISIS DE LA OFICINA DE CONTROL INTERNO FRENTE A LA RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

Aunque el proceso indica en su respuesta que "*se contempla una iniciativa denominada Modelo de Ciberseguridad y MSPI, donde se incluye la actualización del presente manual*", de acuerdo con el alcance de esta auditoría, no evidenció la actualización documental requerida para dar cumplimiento a la normatividad señalada en la observación N° 03, ni avances sobre el particular.

De acuerdo con el análisis expuesto anteriormente, **se mantiene la observación** y su respectiva recomendación.

**7.2.2 Modelo de Seguridad y Privacidad de la Información MSPI 2023:** Durante la auditoría se realizó seguimiento al Modelo de Seguridad y Privacidad de la Información (MSPI) 2023 en el Instituto Distrital de Recreación y Deporte (IDRD), donde se evaluó la eficacia de las estrategias

implementadas para proteger la información crítica de la institución. Se examinó cómo el MSPI garantiza la confidencialidad, integridad y disponibilidad de los datos, y su alineación con las normativas vigentes. Los resultados del diagnóstico para los años 2023 y 2024 se presentarán en las siguientes tablas, proporcionando un análisis detallado del estado actual y las áreas de mejora identificadas.

**Tabla 6. Modelo de Seguridad y Privacidad de la Información MSPI 2023**

| No. | Evaluación de Efectividad de controles | | | |
|---|---|---|---|---|
| | DOMINIO | Calificación Actual | Calificación Objetivo | EVALUACIÓN DE EFECTIVIDAD DE CONTROL |
| A.5 | POLITICAS DE SEGURIDAD DE LA INFORMACIÓN | 80 | 100 | GESTIONADO |
| A.6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 71 | 100 | GESTIONADO |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | 74 | 100 | GESTIONADO |
| A.8 | GESTIÓN DE ACTIVOS | 69 | 100 | GESTIONADO |
| A.9 | CONTROL DE ACCESO | 78 | 100 | GESTIONADO |
| A.10 | CRIPTOGRAFÍA | 60 | 100 | EFECTIVO |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | 75 | 100 | GESTIONADO |
| A.12 | SEGURIDAD DE LAS OPERACIONES | 79 | 100 | GESTIONADO |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | 69 | 100 | GESTIONADO |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 63 | 100 | GESTIONADO |
| A.15 | RELACIONES CON LOS PROVEEDORES | 80 | 100 | GESTIONADO |
| A.16 | GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 66 | 100 | GESTIONADO |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | 77 | 100 | GESTIONADO |
| A.18 | CUMPLIMIENTO | 76,5 | 100 | GESTIONADO |
| ***PROMEDIO EVALUACIÓN DE CONTROLES*** | | **73** | **100** | GESTIONADO |

Fuente: Evaluacion_MSPI 2023 IDRD.

**Tabla 7. Modelo de Seguridad y Privacidad de la Información MSPI 2024**

| No. | Evaluación de Efectividad de controles | | | |
|---|---|---|---|---|
| | DOMINIO | Calificación Actual | Calificación Objetivo | EVALUACIÓN DE EFECTIVIDAD DE CONTROL |
| A.5 | POLITICAS DE SEGURIDAD DE LA INFORMACIÓN | 80 | 100 | GESTIONADO |
| A.6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 71 | 100 | GESTIONADO |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | 74 | 100 | GESTIONADO |
| A.8 | GESTIÓN DE ACTIVOS | 69 | 100 | GESTIONADO |
| A.9 | CONTROL DE ACCESO | 80 | 100 | GESTIONADO |
| A.10 | CRIPTOGRAFÍA | 70 | 100 | GESTIONADO |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | 77 | 100 | GESTIONADO |
| A.12 | SEGURIDAD DE LAS OPERACIONES | 79 | 100 | GESTIONADO |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | 69 | 100 | GESTIONADO |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 63 | 100 | GESTIONADO |
| A.15 | RELACIONES CON LOS PROVEEDORES | 80 | 100 | GESTIONADO |
| A.16 | GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 74 | 100 | GESTIONADO |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | 77 | 100 | GESTIONADO |
| A.18 | CUMPLIMIENTO | 80 | 100 | GESTIONADO |
| ***PROMEDIO EVALUACIÓN DE CONTROLES*** | | **74** | **100** | GESTIONADO |

Fuente: Evaluacion_MSPI 2024 IDRD.

Durante la auditoría se evidenció que, en cuanto a las políticas de seguridad de la información, el IDRD contaba con una política publicada en su sitio oficial, revisada por última vez en 2022. Aunque se habían definido roles y responsabilidades generales, se observó una calificación de 80 en la mayoría de los ítems, indicando un buen nivel de implementación, pero con brechas en actualizaciones regulares. Es importante actualizar la política de seguridad según la *Resolución*

*Número 00500 del 10 de marzo de 2021* que requiere el uso del *"Formato Manual de Políticas de Seguridad de la Información" y se especifica que "las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente".* También se debe socializar la política con más frecuencia mediante sesiones de capacitación y comunicación interna que garantizaran que los empleados comprendan sus responsabilidades, además de implementar controles adicionales para dispositivos móviles, como el uso de VPN y mecanismos de cifrado.

Respecto a la organización de la seguridad de la información, se encontraron roles y responsabilidades definidos en la *Resolución del IDRD 056 de 2022* por la cual Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Instituto Distrital de Recreación y Deporte y la existencia de un comité de gestión para temas de seguridad. No obstante, se carecía de protocolos actualizados para tareas críticas. Se recomendó integrar evaluaciones de riesgos en todas las etapas de los proyectos y aplicar controles compensatorios en áreas donde no es viable separar tareas, como revisiones independientes y auditorías periódicas. Además, se debe asegurar una asignación formal de recursos para actividades de sensibilización y formación.

En el ámbito de la seguridad de los recursos humanos, se constató que los contratos y procesos de desvinculación incluían cláusulas de confidencialidad y se ofrecía capacitación básica. Las calificaciones varían entre 60 y 80, lo que indicaba oportunidades de mejora. Se recomienda ampliar los temas de capacitación para incluir simulacros de incidentes y actualizaciones sobre amenazas emergentes, estandarizar contratos para que los empleados reconozcan las políticas de seguridad y documentar formalmente los procesos disciplinarios.

En la gestión de activos, aunque existía un inventario actualizado, faltaba la aprobación formal de la alta dirección, y las políticas para manejo de activos estaban en desarrollo. Se sugiere formalizar el inventario con la aprobación de la alta dirección, implementar un sistema de etiquetado y clasificación para activos físicos y digitales, y establecer un protocolo para la destrucción segura de medios de almacenamiento.

En relación con la continuidad del negocio, se disponía de un plan de recuperación de desastres (DRP) para TI, pero no para otros procesos, realizándose pruebas parciales. Se recomienda ampliar el DRP para cubrir todos los procesos críticos, coordinar simulacros anuales que incluyan procesos no tecnológicos y documentar lecciones aprendidas para incorporarlas en el plan.

Para el cumplimiento legal, se mantenía una matriz legal actualizada trimestralmente, cumpliendo con derechos de propiedad intelectual y protección de registros, aunque se debe reforzar la revisión de normativas de ciberseguridad y actualizar la política de tratamiento de datos personales según los cambios legislativos recientes.

Finalmente, en las relaciones con proveedores y o terceros se recomienda dar cumplimiento a toda la normatividad vigente según la *resolución 746 de 2022, en su artículo 6.1 aunque* existían ANS y acuerdos de confidencialidad, carecían de especificaciones para la seguridad de la información. Por esto se debe actualizar los ANS para incluir cláusulas de seguridad y ciberseguridad, identificar y mitigar riesgos en la cadena de suministro, y establecer auditorías periódicas a proveedores que manejen información sensible.

**7.2.3 Técnicas de Seguridad de la Información:** En el ámbito de las técnicas de seguridad de la información, se identificaron varias áreas clave que requieren atención y mejora.

- **Control de Acceso (A.9):** Aunque el nivel general de madurez es bueno, se observó que ciertos ítems no estaban completamente alineados con los requisitos, especialmente en el manejo de acceso privilegiado y la actualización de políticas de acceso. La gestión de credenciales, así como la revisión de derechos de acceso y control de acceso a sistemas y aplicaciones, está documentada, pero se recomienda mejorar el seguimiento y la realización de auditorías periódicas. Para abordar estas brechas, es esencial actualizar las políticas de control de acceso para incluir tecnologías avanzadas como autenticación biométrica y MFA en sistemas críticos, automatizar revisiones periódicas para detectar cuentas inactivas o con privilegios excesivos y mejorar la documentación de los procedimientos de control de acceso privilegiado.

- **Criptografía (A.10):** A pesar de utilizar métodos de cifrado, gestión de llaves y firmas digitales, se evidenció que la documentación y los procedimientos son limitados. No hay evidencia de una política formal sobre controles criptográficos que detalle procesos de generación, distribución y revocación de llaves. Se recomienda formalizar esta política, definir algoritmos permitidos y gestionar el ciclo de vida de las llaves. Además, se sugiere capacitar al personal clave en métodos criptográficos y realizar auditorías periódicas para evaluar la efectividad de los controles.

- **Seguridad Física y Ambiental (A.11):** Se han implementado controles para perímetros seguros y restricciones de acceso, pero no se especifican todos los controles en áreas sensibles como centros de datos. Falta evidencia sobre la prueba y monitoreo regular de alarmas y sistemas de detección de intrusos. Se recomienda realizar pruebas regulares de estos sistemas, integrar controles adicionales como biometría, y documentar procedimientos para la validación anual de controles físicos.

- **Gestión de Vulnerabilidades Técnicas (A.12.6):** Aunque se mencionan acciones como escaneo de vulnerabilidades, no hay un procedimiento sistemático para el seguimiento y priorización de vulnerabilidades. Se sugiere adoptar una herramienta de gestión de vulnerabilidades para integrar escaneos automáticos y vincular la gestión de vulnerabilidades con la matriz de riesgos. Además, incluir parches de seguridad en un procedimiento formal de control de cambios.

- **Gestión de Incidentes de Seguridad de la Información (A.16):** Los procedimientos de respuesta a incidentes están definidos, pero faltan planes de mejora continúa basados en lecciones aprendidas y evidencia de ejercicios simulados. Se recomienda incorporar simulacros regulares, desarrollar un proceso de retroalimentación y documentar los registros de incidentes con categorías claras.

- **Desarrollo Seguro y Pruebas (A.14):** Se cuenta con separación de ambientes y control de versiones, pero no hay evidencia de pruebas de seguridad específicas. Se sugiere establecer principios claros de desarrollo seguro, incorporar pruebas de seguridad regulares y documentar el entorno de desarrollo seguro con restricciones claras para el manejo de datos de prueba.

● **Copias de Respaldo y Recuperación (A.12.3):** Aunque se realizan respaldos y se almacenan externamente, falta una validación formal mediante pruebas de restauración. Es crucial establecer un calendario para pruebas de restauración, asegurar la clasificación y protección de respaldos, y ampliar los procedimientos de recuperación para incluir simulaciones de pérdida de datos.

**OBSERVACIÓN No. 04:** Se observó que, aunque existe una política de seguridad publicada y roles definidos, revisada por última vez en 2022, presenta brechas significativas en su actualización, incumpliendo la *Resolución Número 00500 del 10 de marzo de 2021* que requiere el uso del *"Formato Manual de Políticas de Seguridad de la Información" y se especifica que "las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente".* Esta situación, junto con la falta de protocolos actualizados para tareas críticas y la ausencia de especificaciones de seguridad en acuerdos con proveedores, compromete la eficacia de las políticas de seguridad en mantener la confidencialidad, integridad y disponibilidad de la información. Además, existen deficiencias en la gestión de acceso, criptografía, seguridad física, y otras áreas clave, que requieren atención para cumplir con las normativas vigentes y asegurar una adecuada protección de los datos.

**RECOMENDACIÓN No. 06:** Actualizar la política de seguridad de la información para cumplir con *Resolución Número 00500 del 10 de marzo de 2021 y la resolución 746 de 2022, en su artículo 6.1,* asegurando revisiones anuales y una socialización efectiva entre los empleados mediante capacitación y comunicación interna. Además, se deben desarrollar protocolos actualizados para tareas críticas, integrar evaluaciones de riesgos en todas las etapas de los proyectos, y aplicar controles compensatorios donde no sea viable separar tareas. En el ámbito de las relaciones con proveedores, es crucial actualizar los ANS para incluir cláusulas de seguridad y ciberseguridad y establecer auditorías periódicas. También se recomienda mejorar las políticas de control de acceso, criptografía, y realizar pruebas regulares de sistemas de seguridad física y de recuperación de datos para asegurar la resiliencia de la infraestructura del IDRD.

**RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

*"(…) En la formulación del nuevo PETI 2024 - 2027, se contempla una iniciativa denominada Modelo de Ciberseguridad y MSPI donde se contempla la actualización del presente manual."(…).*

**ANÁLISIS DE LA OFICINA DE CONTROL INTERNO FRENTE A LA RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

Aunque el proceso indica en su respuesta que "*se contempla una iniciativa denominada Modelo de Ciberseguridad y MSPI, donde se incluye la actualización del presente manual*", de acuerdo con el alcance de esta auditoría no evidenció la actualización documental requerida para dar cumplimiento a la normatividad señalada en la observación N° 04, ni avances sobre el particular.

De acuerdo con el análisis expuesto anteriormente, **se mantiene la observación** y su respectiva recomendación.

## 7.3 SEGUIMIENTO A LA CAPACIDAD DE RESPUESTA ANTE INCIDENTES Y DESASTRES A TRAVÉS DEL PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP).

La Oficina de Control Interno en desarrollo de la presente auditoria, identificó áreas de mejora crítica que son esenciales para garantizar la protección adecuada de los activos de información. Este capítulo ofrece una visión detallada de cómo se están implementando las medidas de seguridad actuales y proporciona recomendaciones específicas para alinear las prácticas con los estándares internacionales más reconocidos, garantizando así una gestión de la seguridad de la información robusta y efectiva.

En particular, el proceso de gestión de la continuidad del negocio se apoya en un documento clave denominado "*Plan de Recuperación de Desastres*". Sin embargo, durante la auditoría, se constató que este plan no está adecuadamente vinculado con los demás documentos del proceso en la plataforma Isolución, ni está disponible en la página web institucional. Esta desconexión limita su eficacia y disponibilidad para los usuarios pertinentes, quienes podrían necesitar acceder rápidamente a la información en situaciones críticas.

Además, se observó que no se está cumpliendo con lo dispuesto en el *Decreto 1078 de 2015*, el cual establece que los sujetos obligados a la Política de Gobierno Digital deben desarrollar capacidades que les permitan anticiparse a las necesidades de los ciudadanos y de la población en general, garantizando la prestación de servicios de calidad. Este decreto también subraya la importancia de mitigar riesgos relacionados con la continuidad y disponibilidad de los servicios, así como identificar los riesgos asociados a la regulación del sector.

Estas normas resaltan la importancia de integrar elementos más detallados y específicos dentro del plan, asegurando así su eficacia y alineación con las mejores prácticas globales para la continuidad del negocio.

### 7.3.1 Elementos faltantes según la norma:

- **Análisis de Impacto al Negocio (BIA):** El documento menciona riesgos generales y tiempos de recuperación, pero carece de un análisis exhaustivo de los procesos críticos, dependencias y niveles de impacto necesarios para priorizar adecuadamente las actividades de recuperación. Este análisis detallado es crucial para entender dónde enfocar los esfuerzos de recuperación de manera efectiva.

- **Identificación de Recursos Críticos:** No se incluye un inventario detallado de los recursos tecnológicos, humanos y de infraestructura esenciales para implementar las estrategias definidas. La falta de esta identificación limita la capacidad del plan para responder de manera eficiente a las contingencias.

- **Estrategias de Respaldo:** Aunque se hace mención del trabajo remoto y el uso de backups en la nube, el documento no detalla estrategias claras para la realización de pruebas, auditorías o

validaciones periódicas de estas soluciones, lo que podría comprometer su efectividad en situaciones de emergencia.

- **Matriz de Roles y Responsabilidades:** No se presenta un desglose claro de las funciones asignadas en cada etapa del Plan de Recuperación ante Desastres, ni se designan responsables principales y alternativos. Esta falta de claridad puede llevar a confusión y retrasos durante la ejecución del plan.

- **Plan de Comunicación:** Se carece de un plan detallado para informar a las partes interesadas, como empleados, directivos y proveedores, durante y después de una contingencia. Una comunicación efectiva es vital para manejar la situación y mantener todos los actores informados y alineados.

- **Pruebas y Simulacros:** No se especifican mecanismos para validar la eficacia del plan mediante simulacros o pruebas periódicas. Sin estas pruebas, es difícil garantizar que el plan funcionará como se espera en un evento real.

- **Gestión de Cambios:** El documento no aborda cómo el Plan de Recuperación ante Desastres será actualizado frente a cambios en el entorno de riesgos o en la infraestructura existente, lo cual es esencial para mantener el plan relevante y efectivo ante evoluciones en el contexto organizacional.

**OBSERVACIÓN No. 05:** La auditoría identificó que el Plan de Recuperación de Desastres (PRD) del IDRD no cumple con estándares técnicos adecuados, comprometiendo la imagen reputacional del instituto al carecer de integración con documentos críticos relacionados, como el Análisis de Impacto al Negocio y un inventario de recursos críticos necesarios para consolidar prioridades y garantizar la continuidad operativa. Así mismo, se evidenció la falta de estrategias claras para la validación de respaldos y la ausencia de procedimientos específicos para actualizar y probar periódicamente el PRD, elementos esenciales para cumplir con el Decreto 1078 de 2015, que exige la mitigación de riesgos y la continuidad de servicios bajo la Política de Gobierno Digital. Estas carencias, unidas a la falta de un desglose preciso de roles y responsabilidades y un plan de comunicación efectivo, dificultan la respuesta ante incidentes críticos, condicionando la capacidad de la entidad para anticiparse y responder a las necesidades de la ciudadanía de forma oportuna lo que podría dejar al IDRD expuesta a nuevas amenazas.

**RECOMENDACIÓN No. 07:** Incorporar un Análisis de Impacto al Negocio (BIA) permitirá identificar y priorizar los procesos críticos al documentar las interdependencias entre procesos, tecnología y personal, asegurando así una base sólida para la continuidad operativa. Además, es fundamental fortalecer el inventario de recursos críticos mediante el desarrollo de un registro que incluya hardware, software, servicios en la nube, instalaciones, proveedores externos y personal clave, garantizando su disponibilidad en situaciones de crisis. Se recomienda, además, definir roles y responsabilidades claras para la ejecución del PRD, implementar estrategias específicas para la validación periódica de respaldos y establecer un plan de comunicación que facilite la coordinación durante incidentes críticos. Finalmente, incluir un cronograma de pruebas periódicas y mecanismos para actualizar el PRD ante cambios en el entorno tecnológico o normativo permitirá garantizar su eficacia y alineación con los requisitos establecidos en el *Decreto 1078 de 2015.*

**RECOMENDACIÓN No. 08:** Se recomienda diseñar un plan de comunicación estructurado que establezca guías claras para notificar a las partes interesadas y defina canales de comunicación alternativos durante emergencias. Así mismo, es crucial establecer procedimientos de recuperación alternativos, documentando acciones específicas para restaurar sistemas desde backups, asegurando la realización de pruebas de integridad de datos y funcionalidad para garantizar una recuperación eficiente y coordinada.

**RECOMENDACIÓN No. 09:** Se recomienda llevar a cabo pruebas periódicas para evaluar la eficiencia del plan de recuperación, lo que permitirá identificar y ajustar cualquier deficiencia detectada, asegurando así que el plan se mantenga efectivo y alineado con las mejores prácticas y necesidades organizacionales.

**RECOMENDACIÓN No. 10:** Se recomienda definir e implementar indicadores clave de desempeño (KPIs) de continuidad, como el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO), para medir la eficacia del proceso de recuperación y asegurar que el plan se mantenga alineado con las mejores prácticas y necesidades organizacionales.

**RECOMENDACIÓN No. 11:** Es crucial actualizar el Plan de Recuperación de Desastres (DRP) mediante un mecanismo de revisión continua que se adapte a nuevas tecnologías y cambios organizacionales. Además, se debe formalizar una política de recuperación que refleje el compromiso de la organización con la implementación y mantenimiento del DRP, asegurando su alineación con las normativas vigentes.

**RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

*"(…)En la formulación del nuevo PETI 2024 - 2027, se contempla una iniciativa denominada Modelo de Ciberseguridad y MSPI donde se contempla la actualización del PRD para la entidad."(…).*

**ANÁLISIS DE LA OFICINA DE CONTROL INTERNO FRENTE A LA RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

Aunque el proceso indica en su respuesta que: "*se contempla una iniciativa denominada Modelo de Ciberseguridad y MSPI donde se contempla la actualización del PRD para la entidad*", de acuerdo con el alcance de esta auditoría no evidenció la actualización documental requerida para dar cumplimiento a la normatividad señalada en la observación N° 05, ni avances sobre el particular.

De acuerdo con el análisis expuesto anteriormente, **se mantiene la observación** y su respectiva recomendación.

## 7.4 SEGUIMIENTO AL PLAN DE CONTINUIDAD DEL NEGOCIO (BCP) PARA GARANTIZAR LA RESILIENCIA OPERATIVA DEL IDRD EN SITUACIONES DE EMERGENCIA O INTERRUPCIONES PROLONGADAS.

En este capítulo se pudo evidenciar la necesidad de desarrollar e implementar un Plan de Continuidad del Negocio (BCP) para el Instituto Distrital de Recreación y Deporte (IDRD), a fin de asegurar su capacidad operativa frente a emergencias o interrupciones prolongadas. Actualmente, el IDRD carece de un BCP formalmente documentado, lo que representa un riesgo significativo para la continuidad de sus operaciones misionales.

La normativa vigente establece claras obligaciones para las entidades públicas respecto a la implementación de planes de continuidad. El Decreto 1078 de 2015 y la Ley 1712 de 2014 obligan a la gestión de la seguridad de la información y la transparencia, demandando medidas que aseguren la continuidad operativa. El Decreto 2573 de 2014 y el Manual del Modelo Integrado de Planeación y Gestión (MIPG) refuerzan la importancia de garantizar la continuidad de los servicios documentales y misionales. Así mismo, el Plan Distrital de Gestión del Riesgo y la Ley 1523 de 2012 destacan la gestión del riesgo de desastres como una prioridad esencial, mientras que la Circular 003 de 2015 del MinTIC proporciona lineamientos específicos para el desarrollo de estos planes bajo el modelo MSPI.

Para el IDRD, es esencial alinear el futuro BCP con los marcos MSPI y MIPG, asegurando su integración con los procesos de gestión de riesgos institucionales. La identificación de servicios críticos, como la operación de escenarios deportivos y sistemas de información, es clave en el análisis de impacto del negocio (BIA). Se recomienda planificar escenarios de interrupción específicos y realizar simulacros periódicos para validar la efectividad del BCP, además de incorporar los lineamientos del Plan Distrital de Gestión del Riesgo en sus operaciones.

### 7.4.1 Elementos Esenciales del BCP Enfocado en TIC.

- **Gobernanza y Marco de Referencia:** Establecer una política de continuidad del negocio clara, formar un comité responsable y asegurar el cumplimiento normativo.
- **Análisis de Impacto al Negocio (BIA):** Identificar procesos críticos de TIC, determinar tiempos objetivos de recuperación (RTO) y puntos de recuperación (RPO).
- **Gestión de Riesgos:** Evaluar y mitigar riesgos específicos que afecten los sistemas TIC.
- **Estrategias de Continuidad:** Diseñar estrategias de alta disponibilidad, respaldo de datos y redundancia en infraestructura.
- **Plan de Respuesta y Recuperación:** Desarrollar procedimientos de contingencia y recuperación con roles y responsabilidades asignados.
- **Gestión de Comunicaciones:** Definir protocolos de comunicación interna y externa durante contingencias.
- **Documentación del PCN TIC:** Mantener un manual detallado del PCN y anexos técnicos.
- **Capacitación y Concienciación:** Entrenar al personal regularmente y fomentar una cultura de continuidad del negocio.
- **Pruebas y Simulacros:** Realizar pruebas periódicas y ajustes basados en lecciones aprendidas.
- **Mantenimiento y Actualización:** Revisar el PCN regularmente y adaptarlo a cambios

significativos.

- **Integración con Otros Planes:** Asegurar que el PCN TIC esté coordinado con otros planes de continuidad, gestión de riesgos y seguridad de la información.

El Plan de Continuidad del Negocio no solo es una obligación normativa, sino también una herramienta crucial para asegurar la capacidad del IDRD de enfrentar eventos que puedan interrumpir sus actividades misionales. Aunque podría argumentarse que, al ser un proceso de apoyo y no estratégico, la elaboración de este plan podría estar fuera de su alcance, es altamente recomendable desarrollar un plan específico de continuidad del negocio centrado en las TIC, debido a su papel vital en el soporte y la operación de los procesos institucionales

Finalmente, es crucial monitorear tecnologías emergentes que puedan mejorar la continuidad de los servicios TIC y asegurar que los proveedores también cuenten con planes de continuidad adecuados. Implementar un Plan de Continuidad de Negocio TIC permitirá al IDRD minimizar interrupciones, proteger su reputación y garantizar la prestación continua de servicios a la comunidad.

**OBSERVACIÓN No. 06:** La ausencia de un Plan de Continuidad del Negocio (BCP) documentado y específico para el IDRD, particularmente en el ámbito de las Tecnologías de la Información y Comunicación (TIC), limita su capacidad para manejar y recuperarse de interrupciones significativas. Esto pone en riesgo la continuidad operativa de servicios críticos, lo cual podría tener consecuencias negativas en la prestación de servicios esenciales a la comunidad. Además, esta situación no cumple con normativas vigentes, como el Decreto 1078 de 2015 y el Plan Distrital de Gestión del Riesgo, que exigen planes de continuidad en entidades públicas. Actualmente, no existen mecanismos efectivos para evaluar y mitigar los riesgos asociados con la continuidad operativa de los servicios TIC del IDRD.

**RECOMENDACIÓN No. 12:** Desarrollar e implementar un Plan de Continuidad del Negocio (BCP) enfocado en las Tecnologías de la Información y Comunicación (TIC), alineado con el Decreto 1078 de 2015 y el Plan Distrital de Gestión del Riesgo. Este plan debe incluir un Análisis de Impacto al Negocio (BIA) que permita identificar procesos críticos y sus interdependencias, así como estrategias para mitigar riesgos asociados con la continuidad operativa. Asimismo, es necesario definir procedimientos claros para la respuesta y recuperación ante interrupciones, establecer roles y responsabilidades específicas, y diseñar un plan de comunicación que facilite la coordinación en situaciones de crisis. Adicionalmente, se sugiere implementar un cronograma de pruebas periódicas y un mecanismo para actualizar el plan de forma continua, asegurando su relevancia frente a cambios tecnológicos, organizacionales o normativos. Finalmente, la creación de un comité de continuidad encargado de gestionar, supervisar y promover la cultura de resiliencia garantizará la sostenibilidad operativa del IDRD frente a posibles interrupciones.

**RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

*"(…)En la formulación del nuevo PETI 2024 - 2027, se contempla una iniciativa denominada Modelo de Ciberseguridad y MSPI donde se contempla el DRP como un entregable del proyecto. "(…).*

**ANÁLISIS DE LA OFICINA DE CONTROL INTERNO FRENTE A LA RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

Aunque el proceso indica en su respuesta que "*se contempla una iniciativa denominada Modelo de Ciberseguridad y MSPI donde se contempla el DRP como un entregable del proyecto*", de acuerdo con el alcance de esta auditoría no evidenció avances sobre el particular, para dar cumplimiento a la normatividad señalada en la observación N° 06.

De acuerdo con el análisis expuesto anteriormente, **se mantiene la observación** y su respectiva recomendación.

## 7.5 VERIFICAR EL APROVISIONAMIENTO DE SERVICIOS (SISTEMAS DE INFORMACIÓN Y CAPACIDAD DE CÓMPUTO, LICENCIAMIENTO, ALMACENAMIENTO) DE LA ENTIDAD Y CONTROL DE TERCEROS.

En este capítulo, se verificó el aprovisionamiento de servicios dentro de la entidad, abarcando áreas críticas como los sistemas de información, la capacidad de cómputo, el licenciamiento y el almacenamiento. Además, se examinó el control y la gestión de los servicios proporcionados por terceros, asegurando que se alineen con los objetivos estratégicos de la institución. Este enfoque integral busca optimizar la eficiencia operativa y garantizar que los recursos tecnológicos estén adecuadamente gestionados, soportando de manera efectiva las necesidades actuales y futuras de la entidad.

A Continuación, se presenta un análisis detallado de los sistemas operativos utilizados en la muestra seleccionada, ilustrando la cantidad de implementaciones de cada sistema y proyectando la brecha de soporte en los próximos años. A través de esta representación, se busca identificar la distribución actual de los sistemas operativos dentro del IDRD, así como anticipar los desafíos de soporte que puedan surgir a medida que algunos de estos sistemas se acerquen al final de su vida útil. Esta información es crucial para planificar actualizaciones tecnológicas y asegurar la continuidad operativa en el futuro, permitiendo una gestión proactiva de los recursos tecnológicos de la entidad.

**Tabla 8. Modelo de Seguridad y Privacidad de la Información MSPI 2024.**

| Versión | Cantidad | Observación |
|---|---|---|
| CentOS 7 | 5 | Se acerca al final del soporte principal. |
| Ubuntu Server 20.04 LTS | 3 | Ha superado el fin del soporte principal. |
| Ubuntu Server 22.04 LTS | 1 | Soporte a largo plazo hasta Abril 2027 |
| Windows 10 Pro | 1 | Ha superado el fin del soporte principal. |
| Windows Server 2016 Datacenter | 4 | Ha superado el fin del soporte principal. |
| Windows server 2019 Data center | 1 | Posible error tipográfico, debería ser "Datacenter" |
| Windows Server 2019 Datacenter | 9 | Soporte a largo plazo hasta Enero 2029 |
| **Total general** | **24** | |

Fuente: Plan-Estrategico-de-Tecnologias-de-la-Informacion-IDRD-PETI-2024-2027v1.9

### 7.5.1 Evaluación de Sistemas Operativos

Esta evaluación de los sistemas operativos del IDRD se centró en identificar riesgos asociados al soporte de estos y en ofrecer recomendaciones estratégicas para mitigar vulnerabilidades potenciales. La gestión adecuada de estos sistemas es crucial para mantener la seguridad y eficiencia operativa en un entorno tecnológico en constante evolución. Al adoptar un enfoque proactivo, se busca garantizar que la infraestructura tecnológica sea robusta y adaptable, protegiendo los activos digitales y optimizando los recursos para mantener la competitividad y capacidad de innovación de la organización.

- **Evaluación Detallada:**

- **CentOS 7 (Soporte limitado):** CentOS 7 se está acercando al final de su soporte principal, lo que significa que Red Hat dejará de ofrecer actualizaciones de seguridad y soporte oficial. Para minimizar riesgos, se recomienda planificar la migración a alternativas como Rocky Linux, AlmaLinux o RHEL, especialmente si el entorno requiere soporte continuo. Es crucial validar las dependencias y la compatibilidad antes de proceder con la migración.
- **Ubuntu Server 20.04 LTS (Soporte extendido):** Aunque esta versión LTS sigue recibiendo actualizaciones críticas bajo el esquema ESM (Extended Security Maintenance), ha superado el fin de su soporte principal. Se recomienda migrar a Ubuntu Server 22.04 LTS para asegurar un soporte completo y acceso a nuevas características, revisando las dependencias de las aplicaciones antes de actualizar.
- **Ubuntu Server 22.04 LTS (Soporte vigente hasta 2027):** Esta versión ofrece soporte a largo plazo, lo que la convierte en una opción adecuada para entornos de producción. Se recomienda mantener actualizaciones regulares y monitorear continuamente su estado de soporte.
- **Windows 10 Pro (Sin soporte principal):** Debido al fin del soporte principal de Microsoft para Windows 10 Pro, este sistema operativo es más vulnerable a amenazas emergentes. Se recomienda migrar a Windows 11 o a una versión que cuente con soporte activo. En caso de que su uso sea indispensable, es crucial implementar controles de seguridad rigurosos y restringir su acceso a redes externas para minimizar riesgos.
- **Windows Server 2016 Datacenter (Sin soporte principal):** Sin el soporte principal, estas instancias son vulnerables, recibiendo solo parches críticos bajo soporte extendido. Se sugiere migrar a Windows Server 2019 o 2022, que ofrecen un soporte más prolongado, asegurándose de revisar la compatibilidad de las aplicaciones antes de la migración.
- **Windows Server 2019 Datacenter (Soporte vigente hasta 2029):** Esta versión está completamente respaldada, garantizando actualizaciones y parches hasta enero de 2029. Se recomienda priorizar esta versión para futuros despliegues y mantener un programa de actualizaciones regulares.

- **Acciones Prioritarias para la Gestión de Sistemas Operativos del IDRD.**

**Planificación de Migraciones:**

- **Sistemas Operativos Obsoletos:** Es esencial planificar la migración de Ubuntu 20.04 y CentOS 7 a versiones más recientes o a alternativas que ofrezcan soporte continuo. Del mismo

modo, se debe considerar la actualización de Windows 10 Pro y Windows Server 2016 a versiones activas que cuenten con soporte completo para asegurar la estabilidad y seguridad del entorno.

**Implementación de Medidas de Seguridad:**

- **Sistemas sin Soporte Completo:** Para aquellos sistemas que ya no reciben soporte completo, se recomienda restringir su conectividad a redes públicas y asegurar que sigan recibiendo actualizaciones críticas hasta que se completen las migraciones necesarias.

**Validación de Compatibilidad de Aplicaciones:**

- **Antes de Actualizar:** Antes de efectuar actualizaciones de sistemas operativos, es crucial evaluar la compatibilidad y las dependencias de las aplicaciones con los sistemas actuales para evitar interrupciones y asegurar la continuidad del negocio.

**Monitoreo del Soporte Continuo:**

- **Prevención de Obsolescencia:** Mantener un sistema de monitoreo que garantice que los sistemas no queden fuera del ciclo de actualizaciones futuras es fundamental para evitar vulnerabilidades y mantener la seguridad.

**Servidores Windows y Diversidad de Plataformas:**

- **Gestión Unificada:** La coexistencia de múltiples versiones de sistemas operativos Linux (Debian, Ubuntu, CentOS, SUSE, OracleLinux) y Windows Server puede complicar la gestión unificada de seguridad y actualizaciones. Es necesario simplificar y coordinar estos procesos para mejorar la eficacia.

**Versiones Desactualizadas y en Fin de Soporte:**

- **Riesgos Asociados:** Windows Server 2016 Datacenter y CentOS 7 están próximos o ya han alcanzado su fin de soporte, lo que implica un riesgo significativo debido a la falta de nuevas funcionalidades y vulnerabilidades no resueltas. Planificar una migración es crucial. SUSE Linux Enterprise 12 y Ubuntu 20.04 LTS también requieren evaluaciones para futuras actualizaciones a versiones con soporte completo.

**Uso de Versiones Recientes:**

- **Ventajas de Actualización:** La implementación de Windows Server 2019 Datacenter y Ubuntu Server 22.04.1 LTS proporciona sistemas actualizados que reducen los riesgos asociados a vulnerabilidades no corregidas.

**Falta de Información sobre Actualizaciones y Parches:**

- **Necesidad de Transparencia:** Sin detalles claros sobre el estado de actualización y parches de las versiones en uso, es difícil garantizar que las vulnerabilidades conocidas hayan sido

adecuadamente mitigadas. Es imperativo mantener registros precisos y actualizados de todas las acciones de mantenimiento y parches aplicados.

**7.5.2 Riesgos Identificados:**

**Riesgos Asociados a Versiones en Fin de Soporte:**

- **Vulnerabilidades No Parcheadas:** La presencia de sistemas como Windows Server 2016, SUSE Linux Enterprise 12 y CentOS 7, que se encuentran cerca del fin de su soporte o ya lo han alcanzado, introduce un riesgo significativo de vulnerabilidades no parcheadas. Estas plataformas son susceptibles a ataques dirigidos que explotan vulnerabilidades conocidas, lo que puede comprometer la seguridad de todo el entorno.

**Compatibilidad de Software:**

- **Desafíos de Coexistencia:** La coexistencia de múltiples distribuciones de Linux junto con diversas versiones de Windows Server puede dar lugar a problemas de compatibilidad, especialmente en aplicaciones que dependen de la integración entre estos sistemas operativos. Es fundamental evaluar y gestionar cuidadosamente estas interacciones para evitar interrupciones en el servicio.

**Gestión de Parches y Actualizaciones:**

- **Brechas en la Implementación:** La diversidad de sistemas operativos en uso puede conducir a inconsistencias en la implementación regular de parches y actualizaciones. Esto puede dejar ciertos sistemas expuestos a vulnerabilidades, subrayando la necesidad de un enfoque más coordinado y uniforme en la gestión de actualizaciones.

**Control de Accesos y Auditoría:**

- **Verificación de Mecanismos:** Asegurar que los mecanismos de autenticación y auditoría estén configurados de manera uniforme es esencial, especialmente en sistemas críticos para la misión. La falta de consistencia en estos controles puede aumentar el riesgo de accesos no autorizados y dificultar el seguimiento de incidentes de seguridad.

**Inexistencia de una Estrategia de Migración Unificada:**

- **Falta de Planificación Clara:** Actualmente, no parece existir una estrategia clara y unificada para el reemplazo o actualización de sistemas que se acercan al fin de su soporte. La ausencia de una planificación estructurada aumenta el riesgo de interrupciones operativas y deja a la infraestructura vulnerable a amenazas que podrían haberse mitigado con una migración oportuna.

**OBSERVACIÓN No. 07:** En el análisis de los riesgos asociados a los sistemas operativos cercanos al fin de su soporte, se evidencio que está comprometida la continuidad operativa de la infraestructura tecnológica al dificultar la respuesta ante vulnerabilidades emergentes. Esta situación aumenta los riesgos de seguridad y condiciona la capacidad de la entidad para mantener

servicios estables y confiables. Asimismo, la falta de una estrategia de migración clara y la complejidad añadida por la diversidad de plataformas limitan la implementación uniforme de actualizaciones y el control de accesos, poniendo en riesgo el cumplimiento de la conformidad con normativas como la Ley 1581 de 2012, que exige medidas técnicas y administrativas para proteger los datos personales de posibles incidentes. Como consecuencia, el IDRD podría enfrentar interrupciones en sus servicios críticos, una mayor exposición a ciberataques y sanciones legales por el incumplimiento de sus obligaciones normativas, afectando la confianza de la ciudadanía en la entidad.

**RECOMENDACIÓN No. 13:** Actualizar los sistemas operativos que están próximos a quedarse sin soporte es crucial para garantizar la seguridad y funcionalidad de las plataformas tecnológicas. Por ejemplo, Windows Server 2016 Datacenter debe ser actualizado a una versión más reciente, como Windows Server 2019 o 2022, lo que permitirá continuar recibiendo actualizaciones de seguridad y acceder a nuevas funcionalidades que mejoren el rendimiento y la protección del entorno. De manera similar, es necesario planificar la transición de sistemas como CentOS 7 para asegurar que estos sistemas sigan siendo seguros y eficientes.

En el caso de equipos de cómputo que aún operan con sistemas obsoletos como Windows 7, cuyo soporte finalizó en enero de 2020, es fundamental actualizarlos, ya que estos representan una grave vulnerabilidad en materia de seguridad de la información. La falta de actualizaciones expone a estos sistemas a riesgos significativos, como la pérdida de confidencialidad, integridad y disponibilidad de datos sensibles y personales.

Tomar estas medidas de actualización reducirá significativamente los riesgos de seguridad y garantizará un entorno tecnológico confiable y eficiente dando cumplimiento a la Ley 1581 de 2012.

**RECOMENDACIÓN No. 14:** Reducir la diversidad de distribuciones Linux en uso ayudará a simplificar la administración y el mantenimiento de los sistemas. Consolidar en distribuciones como Ubuntu LTS o alternativas Red Hat/CentOS, según las necesidades específicas de la organización, puede mejorar la eficacia operativa y facilitar la gestión de parches y actualizaciones.

**RECOMENDACIÓN No. 15:** Implementar una Política Robusta de Gestión de Parches: Automatizar las actualizaciones críticas en los sistemas soportados es fundamental para minimizar el riesgo de explotación de vulnerabilidades conocidas. Una política eficaz debe asegurar que todos los sistemas estén actualizados de manera oportuna, reduciendo así la exposición a amenazas de seguridad.

**RECOMENDACIÓN No. 16:** Es crucial verificar la configuración de cada sistema operativo para garantizar la seguridad. Esto incluye la implementación de contraseñas seguras y la autenticación multifactorial (MFA), así como la configuración adecuada de firewalls internos y externos. Además, desactivar servicios innecesarios puede reducir la superficie de ataque, contribuyendo a un entorno más seguro.

**RECOMENDACIÓN No. 17:** Utilizar herramientas como Zabbix para el monitoreo en tiempo real de los sistemas asegura la detección y respuesta rápida a incidentes. Es importante garantizar que todos los sistemas tengan backups frecuentes y probados, cubriendo bases de datos críticas

y sistemas clave, para asegurar la recuperación rápida ante fallos.

**RECOMENDACIÓN No. 18:** Para sistemas que no ofrecen soporte extendido, es esencial definir plazos claros para actualizar o reemplazar antes de que se conviertan en vulnerabilidades críticas. Este enfoque asegura la continuidad operativa y la seguridad del entorno tecnológico.

**RECOMENDACIÓN No. 19:** Migrar instancias de Ubuntu 20.04 LTS a 22.04 o superior antes del fin de soporte en abril de 2025 es crucial para mantener el soporte. También se debe considerar la consolidación de Debian y Ubuntu en una única distribución para simplificar la administración y optimizar recursos.

**RECOMENDACIÓN No. 20:** Implementar controles centralizados para monitorear actualizaciones de seguridad en todas las versiones activas de Ubuntu y Debian es necesario. Establecer una estrategia de seguridad unificada para todos los entornos Linux asegura consistencia en la protección y mejora la respuesta ante incidentes.

**RECOMENDACIÓN No. 21:** Consolidar sistemas de pruebas para reducir la duplicación de recursos y costos es una medida eficaz. Implementar medidas de seguridad específicas, como el aislamiento de red, garantizará un entorno de pruebas seguro y controlado.

**RECOMENDACIÓN No. 22:** Monitorear el vencimiento de la licencia de PanOS y planificar renovaciones con anticipación es crucial para evitar interrupciones de servicio. Además, asegurar el cumplimiento de términos en Oracle Linux evitará penalidades costosas.

**RECOMENDACIÓN No. 23:** Ampliar el esquema de backups más allá de Veeam Backup es vital para asegurar una cobertura completa para bases de datos críticas y sistemas esenciales como Orfeo BD y GitLab, garantizando así la recuperación rápida y efectiva ante cualquier fallo.

**RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

*"(…)Se informa que el área de tecnología ha avanzado de forma proactiva en el desarrollo de un proceso que se está contratando a través de Colombia Compra Eficiente, el cual permite a la entidad superar el rezago en la actualización de los sistemas operativos pendientes.*

*Es importante destacar que, para el IDRD, el parque de servidores se encuentra completamente actualizado y el centro de datos ha sido fortalecido, dotándolo de una infraestructura de alta capacidad y robustos mecanismos de gestión de seguridad. Estas mejoras permiten a la entidad contar con tecnología de punta para respaldar sus gestiones administrativas y misionales, garantizando mayor eficiencia, seguridad y disponibilidad operativa. "(…).*

**ANÁLISIS DE LA OFICINA DE CONTROL INTERNO FRENTE A LA RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

Frente a la respuesta allegada por el proceso esta auditoria informa que la documentación tomada

para la evaluación fue la entregada por el proceso donde claramente se evidenció la no actualización de sistemas operativos, esta evidencia reposa en el mismo PETI 2024-2027 donde se puede observar:

**Tabla 9. Modelo de Seguridad y Privacidad de la Información MSPI 2024.**

*Tabla 17. Sistemas operativos. Fuente: Recopilación propia.*

| Versión | Cantidad | Observación |
|---|---|---|
| CentOS 7 | 5 | Se acerca al final del soporte principal. |
| Ubuntu Server 20.04 LTS | 3 | Ha superado el fin del soporte principal. |
| Ubuntu Server 22.04 LTS | 1 | Soporte a largo plazo hasta Abril 2027 |
| Windows 10 Pro | 1 | Ha superado el fin del soporte principal. |
| Windows Server 2016 Datacenter | 4 | Ha superado el fin del soporte principal. |
| Windows server 2019 Data center | 1 | Posible error tipográfico, debería ser "Datacenter" |
| Windows Server 2019 Datacenter | 9 | Soporte a largo plazo hasta Enero 2029 |
| **Total general** | **24** | |

Fuente: Plan-Estrategico-de-Tecnologias-de-la-Informacion-IDRD-PETI-2024-2027v1.9

De acuerdo con el análisis expuesto anteriormente, **se mantiene la observación** y su respectiva recomendación.

## 7.6 EVALUAR LA GESTIÓN DE RIESGOS FRENTE A UN INCIDENTE DE DATOS PERSONALES DEL IDRD Y EL CUMPLIMIENTO DE CONTROLES EN SUS MAPAS DE RIESGOS DE GESTIÓN Y CORRUPCIÓN.

Durante el proceso de auditoría realizado en el Instituto Distrital de Recreación y Deporte (IDRD), se evidenció la importancia crítica de evaluar la gestión de riesgos relacionados con incidentes de datos personales. El análisis reveló que, mientras se han implementado ciertos controles en los mapas de riesgos de gestión y corrupción, existen áreas que requieren fortalecimiento para asegurar un cumplimiento más robusto y eficaz. Este capítulo del informe detalla las observaciones clave y proporciona un marco para entender cómo los controles actuales pueden ser optimizados para mitigar riesgos, proteger la información sensible y asegurar la integridad de los procesos administrativos en el IDRD.

El IDRD cuenta con la Política de Tratamiento de Datos Personales, implementada en 2018, que establece el marco normativo y operativo para la protección de datos personales en la entidad.

En términos de cumplimiento legal, la política hace referencia a las leyes aplicables, incluyendo la Ley 1581 de 2012, el Decreto 1377 de 2013 y el Decreto Único 1074 de 2015, además de reconocer el derecho al hábeas data conforme al artículo 15 de la Constitución Política de Colombia. No obstante, es crucial garantizar que esta política esté actualizada respecto a cualquier cambio legislativo o normativo reciente para asegurar su vigencia y efectividad.

En cuanto al Registro Nacional de Bases de Datos, la política subraya la obligación de registrar las bases de datos ante la Superintendencia de Industria y Comercio (SIC), tal como lo exige la Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales. Este aspecto debe revisarse constantemente para asegurar su actualización y conformidad con las circulares y directrices recientes emitidas por la SIC.

La política también aborda las categorías especiales de datos, incluyendo los datos sensibles y de menores, conforme a la normativa vigente. Sin embargo, sería beneficioso incluir ejemplos prácticos específicos al contexto del IDRD, como el uso de datos biométricos en actividades recreativas, para ilustrar mejor su aplicación.

Respecto al Oficial de Protección de Datos, la política designa a una persona responsable, pero no detalla si ésta cuenta con el respaldo de un programa integral de cumplimiento y formación que fortalezca la gestión de datos dentro de la entidad. Un enfoque más estructurado en este ámbito podría mejorar la eficacia y el cumplimiento de las normativas.

Finalmente, se describen los derechos de los titulares de datos y los procedimientos para atender consultas y reclamos. Aunque estos procedimientos están bien articulados, sería pertinente incluir más información sobre los mecanismos digitales disponibles para facilitar el acceso, especialmente para aquellas poblaciones con acceso limitado a medios físicos.

En el marco de la auditoría realizada, se ha desarrollado un cuadro de evaluación que identifica áreas clave para el fortalecimiento de la gestión de riesgos en el manejo de datos personales en el IDRD. Este cuadro se organiza en varias categorías, cada una con elementos específicos a evaluar, una descripción de estos y recomendaciones para mejorar la gestión de riesgos.

**Tabla 9. Evaluación de Riesgos de Datos Personales.**

| CATEGORÍA | ELEMENTO PARA EVALUAR | DESCRIPCIÓN | RECOMENDACIONES |
|---|---|---|---|
| **Identificación del riesgo** | Naturaleza del incidente | Tipo de incidente (acceso no autorizado, pérdida, alteración, etc.) | Implementar una matriz de clasificación de incidentes según su criticidad y afectación a los titulares de los datos. |
| | Datos comprometidos | Tipo de datos afectados (sensibles, financieros, personales básicos) | Catalogar y priorizar datos sensibles según la Ley 1581 de 2012. |
| **Prevención** | Política de tratamiento de datos | Existencia y cumplimiento de la política de tratamiento de datos personales | Revisar y actualizar la política con alineación a la normatividad vigente. |

| CATEGORÍA | ELEMENTO PARA EVALUAR | DESCRIPCIÓN | RECOMENDACIONES |
|---|---|---|---|
| | Capacitación del personal | Nivel de formación del personal en manejo y protección de datos personales | Realizar talleres y simulacros sobre incidentes de seguridad y buenas prácticas en protección de datos. |
| | Clasificación de activos de información | Identificación de sistemas y bases de datos que contienen información sensible | Realizar un inventario actualizado de bases de datos según Decreto 1377 de 2013. |
| **Detección** | Herramientas de monitoreo | Sistemas para detectar accesos no autorizados o alteraciones | Implementar y optimizar herramientas como SIEM y monitoreo continuo para detección temprana de incidentes. |
| | Procesos de auditoría | Auditorías internas o externas sobre el manejo de datos | Realizar auditorías periódicas basadas en estándares como ISO 27001 e ISO 27701. |
| **Respuesta** | Plan de respuesta a incidentes | Existencia de un procedimiento claro para responder a incidentes | Diseñar un plan de respuesta a incidentes con roles, responsabilidades, y tiempos de respuesta establecidos. |
| | Notificación de incidentes | Proceso para informar a la SIC y a los titulares sobre el incidente | Crear un protocolo de notificación conforme al Artículo 17 de la Ley 1581 de 2012. |
| | Documentación del incidente | Registro detallado del incidente, acciones tomadas y lecciones aprendidas | Implementar un sistema para registrar y analizar incidentes de forma centralizada. |
| **Mitigación** | Revisión y eliminación de vulnerabilidades | Análisis de la causa raíz y resolución | Realizar análisis post-incidente y planes de mejora. |
| | Restablecimiento de sistemas | Tiempo para restaurar la información comprometida | Diseñar un DRP (Plan de Recuperación ante Desastres) que contemple incidentes relacionados con datos personales. |
| **Cumplimiento normativo** | Registro Nacional de Bases de Datos | Inscripción y actualización de bases de datos ante la SIC | Verificar que todas las bases de datos del IDRD estén inscritas y actualizadas en el RNBD. |
| | Consentimiento de los titulares | Existencia de mecanismos para la obtención y registro del consentimiento | Validar que el consentimiento sea explícito y verificable según lo dispuesto en el Decreto 1377 de 2013. |
| | Evaluación de impacto en privacidad | Análisis de los efectos sobre los titulares de los datos | Implementar evaluaciones de impacto en privacidad (PIA) para identificar riesgos potenciales antes de implementar nuevos proyectos o tecnologías. |

Fuente: Elaboración Propia Equipo OCI.

**OBSERVACIÓN No. 08:** Se ha identificado que la falta de actualización y alineación de las políticas de protección de datos con la normativa vigente está comprometiendo la seguridad de los datos personales, en especial los de menores de edad, lo que constituye un incumplimiento de la Ley 1581 de 2012, que exige garantizar medidas técnicas, humanas y administrativas para la protección de esta información. Además, el uso de sistemas operativos desactualizados expone

estos datos a riesgos significativos de seguridad, incrementando la probabilidad de brechas de datos y accesos no autorizados. Esta situación pone en riesgo tanto la integridad de la información gestionada por el IDRD como el cumplimiento de sus obligaciones legales, afectando la confianza de la ciudadanía. Es fundamental implementar de inmediato una matriz para la clasificación de incidentes y optimizar las herramientas de monitoreo para mitigar estos riesgos.

**RECOMENDACIÓN No. 24:** Verificar y actualizar la política de protección de datos del IDRD, garantizando su alineación con las directrices más recientes de la Superintendencia de Industria y Comercio (SIC) y cualquier cambio legislativo o jurisprudencial posterior a 2018, aplicable a Bogotá. Esta actualización debe incluir medidas específicas para la protección de datos de menores de edad y la integración de sistemas tecnológicos seguros. Además, se sugiere realizar un diagnóstico de los sistemas operativos y avanzar en un plan de actualización tecnológica para garantizar la seguridad de la información y el cumplimiento de las normativas vigentes, minimizando riesgos legales y operativos.

**RECOMENDACIÓN No. 25:** Se recomienda Implementar un proceso continuo para evaluar los riesgos asociados al tratamiento de datos personales, especialmente en proyectos que involucran tecnologías emergentes o nuevas actividades del IDRD. Esto es crucial para mitigar los riesgos identificados en la observación sobre la seguridad de los datos personales de menores.

**RECOMENDACIÓN No. 26:** Se recomienda asegurar la comprensión y el cumplimiento de las políticas de tratamiento de datos por parte de todos los empleados y contratistas a través de sesiones regulares de capacitación. Esto fortalecerá la cultura de protección de datos dentro del IDRD.

**RECOMENDACIÓN No. 27:** Se recomienda desarrollar protocolos detallados para la recolección, uso y almacenamiento de datos sensibles y de menores, con un enfoque particular en actividades específicas del IDRD, como deportes o eventos culturales. Esto abordará directamente la preocupación sobre la seguridad de los datos de menores.

**RECOMENDACIÓN No. 28:** Se recomienda integrar herramientas digitales avanzadas para facilitar la gestión de derechos de los titulares, como formularios electrónicos fácilmente accesibles desde la página web oficial del IDRD. Esto mejorará la accesibilidad y la gestión eficiente de los derechos de los ciudadanos.

**RECOMENDACIÓN No. 29:** Se recomienda reforzar los avisos de privacidad, asegurando que estén redactados en un lenguaje claro y comprensible para los ciudadanos, especialmente en actividades públicas organizadas por el IDRD. Esto fomentará la confianza y la transparencia en el manejo de datos personales.

**RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

*"(…) En la formulación del nuevo PETI 2024 - 2027, se contempla una iniciativa denominada Modelo de Ciberseguridad y MSPI donde se contempla las mejoras al tratamiento de datos e información de los ciudadanos"(…).*

**ANÁLISIS DE LA OFICINA DE CONTROL INTERNO FRENTE A LA RESPUESTA DEL PROCESO GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN:**

Si bien el proceso allega en su respuesta, que "*se contempla una iniciativa denominada Modelo de Ciberseguridad y MSPI" donde se contempla las mejoras al tratamiento de datos e información de los ciudadanos",* de acuerdo con el alcance de esta auditoria no evidenció avances sobre el particular, para cumplir con la normatividad descrita en la observación N° 08.

De acuerdo con el análisis expuesto anteriormente, **se mantiene la observación** y su respectiva recomendación.

## 8. CONCLUSIÓN

Considerando el objetivo general y alcance de la presente evaluación, de acuerdo con los resultados obtenidos en el presente informe, se reitera la observación emitida en el Informe de auditoría vigencia 2023 respecto de: "*Se sugiere que, desde la Alta Dirección, se analice la importancia de implementar los lineamientos para el fortalecimiento institucional en materia de TIC, a través del posicionamiento de los Líderes de Áreas TI, la estructuración de un área propia de Tecnologías y Sistemas de Información, y una gestión estratégica que facilite la gobernabilidad y gestión de las Tecnologías de la Información en la entidad…";* para lo cual se concluye que la gestión de Tecnologías de la Información y Comunicaciones (TIC) pueda ser reconocida como un proceso estratégico e independiente dentro del IDRD, con un presupuesto planificado que priorice el impacto positivo en la seguridad de la información. Esta transformación puede fortalecer la protección de datos personales sensibles, especialmente aquellos de menores de edad. La falta de actualización en sistemas y políticas actuales representa un riesgo significativo que necesita la atención inmediata de la alta dirección para mitigar posibles vulnerabilidades.

Además, no fue posible determinar un porcentaje de avance y cumplimiento real del PETI debido a la falta de alineación entre los proyectos y las iniciativas del plan, lo que se debe a la incoherencia entre las estrategias de gestión de información y los proyectos del portafolio TI. Así mismo, la ausencia de documentación formalizada en el sistema de gestión ISOLUCIÓN, junto con inconsistencias en la medición de indicadores y retrasos en los cronogramas, dificulta el cumplimiento de la Ley 1712 de 2014 sobre transparencia de la información pública, lo que genera riesgos de incumplimiento normativo y sanciones por parte de los entes de control.

La falta de actualización del Manual de Políticas de Seguridad Digital, cuyo último cambio data de 2019, ha generado una desalineación con las normativas actuales, como el Decreto 1083 de 2015. Esta falta de revisión periódica compromete la efectividad de las políticas implementadas y aumenta el riesgo de incumplir las directrices normativas del sector público. Aunque el IDRD cuenta con una política de seguridad, presenta brechas debido a la falta de actualización y

protocolos para tareas críticas, lo que pone en riesgo la confidencialidad, integridad y disponibilidad de la información.

Además, el Plan de Recuperación de Desastres (PRD) no está alineado con los estándares técnicos necesarios, comprometiendo la continuidad operativa de los servicios críticos. La ausencia de un Plan de Continuidad del Negocio (BCP) específico para TIC limita la capacidad de gestionar operaciones críticas en caso de interrupciones. La falta de actualización en las políticas de protección de datos personales, especialmente en lo que respecta a menores de edad, compromete la seguridad de la información y el cumplimiento de la Ley 1581 de 2012. Así mismo, el uso de sistemas operativos desactualizados aumenta las brechas de seguridad y la probabilidad de accesos no autorizados, afectando la confianza de la ciudadanía.

Finalmente, es necesario que el IDRD fortalezca su infraestructura digital mediante la integración de herramientas que faciliten la gestión de derechos de los titulares y el monitoreo de seguridad. Establecer auditorías regulares garantizará el cumplimiento de los estándares legales y permitirá identificar áreas de mejora continua, asegurando la integridad y seguridad de la información gestionada.

No obstante, con el fin de mejorar y proteger el valor institucional, en el cuerpo del informe se identifican observaciones, oportunidades de mejora y recomendaciones para su consideración y establecimiento de acciones de mejora.

Cordialmente,

**LUZ ANGELA FONSECA RUIZ**
Jefe Oficina de Control Interno (E)

Elaboró: Jorge Luis Zambrano Murcia - Contratista OCI.
Khaanko Norberto Ruiz Rodriguez - Contratista OCI.