Bogotá D.C, miércoles 31 de diciembre de 2025

PARA: MARÍA CLAUDIA PARIAS DURÁN
Directora General

DE: ELEANA MARCELA PAEZ URREGO
Asesora de Control Interno (E)

ASUNTO: Remisión informe final de la Auditoría al Modelo de Seguridad y Privacidad de la Información MSPI IDARTES 2025 y los Sistemas de Información de PANDORA-ORFEO

Cordial saludo,

De manera atenta anexo a esta comunicación el informe final de la auditoría al Modelo de Seguridad y Privacidad de la Información MSPI IDARTES 2025 y los Sistemas de Información de PANDORA-ORFEO, cuyo el objetivo correspondió a “Evaluar la conformidad y la eficacia del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) de IDARTES, incluyendo la gestión de riesgos de ciberseguridad y la protección de datos personales.”

Cabe detallar que el ejercicio de auditoría arrojó un total de nueve (9) observaciones. Una vez remitido el informe preliminar a la Oficina Asesora de Planeación y Tecnologías de la Información, se obtuvo la respuesta de aceptación correspondiente; asimismo, los resultados fueron socializados con los jefes de las unidades de gestión mencionadas en dichos hallazgos..

A continuación, se presentan las observaciones:

#	OBSERVACIÓN	DESCRIPCIÓN DETALLADA	POSIBLE RESPONSABLE
1	**Vacancia del Rol de Oficial de Seguridad (CISO)**	El cargo de "Profesional Universitario" creado para liderar el MSPI está vacante desde septiembre de 2025. Esta brecha en la gobernanza genera un riesgo crítico en la gestión estratégica y la transición normativa.	**Talento Humano / OAPTI**
2	**Manejo Inseguro de Información de Nómina**	Uso de archivos Excel con datos financieros y personales sensibles compartidos vía Gmail sin clasificación, cifrado, ni protección por contraseña, contraviniendo los controles de transferencia segura.	**Talento Humano (Nómina)**
3	**Deficiencia en Atributos del Inventario de Activos**	El sistema SAI (Sin Capital) opera bajo un enfoque netamente contable y administrativo. Carece de campos para la clasificación de seguridad (Confidencialidad, Integridad y Disponibilidad).	**OAPTI / Almacén**

#	OBSERVACIÓN	DESCRIPCIÓN DETALLADA	POSIBLE RESPONSABLE
4	**Falta de Metodología de Desarrollo Seguro**	El desarrollo de software (ej. SIF) utiliza Scrum para agilidad, pero no integra un ciclo de vida de desarrollo seguro (SDLC) ni metodologías técnicas como OWASP para prevenir vulnerabilidades desde el diseño.	**OAPTI (Gestión de Software)**
5	**Deficiencia en Detección y Respuesta a Incidentes**	Inexistencia de "Playbooks" técnicos documentados para escenarios de alto impacto. El reporte de "Cero Incidentes" sugiere una incapacidad técnica de detección profunda ante la falta de herramientas tipo SIEM o EDR.	**OAPTI (Seguridad Informática)**
6	**Desconexión en la Propiedad de los Riesgos**	Los líderes de procesos funcionales desconocen o niegan poseer riesgos de TI. La OAPTI gestiona la matriz de riesgos de forma técnica sin una notificación formal ni aceptación de riesgos residuales por parte de los dueños del negocio.	**Líderes de Proceso / OAPTI**
7	**Vacío en la Gobernanza de Protección de Datos**	Incertidumbre administrativa entre Jurídica y Planeación tras la salida del abogado encargado. Actualmente no hay un responsable (OPD) para la actualización de la política ni el reporte de novedades ante la SIC.	**Subdirección Jurídica / OAPTI**
8	**Debilidad en Estandarización de Roles (Orfeo)**	No existe una matriz de perfiles estandarizada para Orfeo. Las activaciones funcionales se realizan de forma manual y "ad-hoc" según criterio de cada jefe, incrementando el riesgo de acumulación de privilegios.	**Gestión Documental / OAPTI**
9	**Ausencia de Controles en Plataformas Externas**	Dependencia crítica de plataformas administradas por la Secretaría de Cultura (CultuRed) sin memorandos de entendimiento técnicos, protocolos de acceso o acuerdos de nivel de servicio (SLA) formalizados.	**OAPTI / Subdirección Jurídica**

Anexo a esta comunicación se envía:

- Informe Final de Auditoria al MSPI 2025.pdf

Cordialmente,
Documento 20251300894803 firmado electrónicamente por:

ELEANA MARCELA PAEZ URREGO, Jefe de Oficina Contol Interno, Área de Control Interno, Fecha firma: 31-12-2025 09:24:50

Revisó: ANGEL ANTONIO DIAZ VEGA - Área de Control Interno

Anexos: 1 folios

8a28f5e1a0819976d4cc40f21ee8cad7917d53e3accc24e4f6e878b1dae35e03
Codigo de Verificación CV: c65af Comprobar desde:

INFORME DE AUDITORÍA INTERNA DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SISTEMAS DE INFORMACIÓN DE PANDORA Y ORFEO

ÁREA DE CONTROL INTERNO

INSTITUTO DISTRITAL DE LAS ARTES

BOGOTÁ D.C.

Diciembre de 2025

CONTENIDO

INTRODUCCIÓN

El presente informe de auditoría interna se deriva de la evaluación sistemática realizada al Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) del Instituto Distrital de las Artes – IDARTES, enfocándose en los procesos y los sistemas de información PANDORA y ORFEO. En cumplimiento del Objetivo Estratégico N°11 de la entidad, orientado a fortalecer la infraestructura tecnológica y mejorar la prestación del servicio a la ciudadanía, este ejercicio se desarrolla en un contexto donde las entidades públicas enfrentan una exposición creciente a incidentes de seguridad digital que pueden afectar su funcionamiento operativo. La auditoría se fundamenta en la transición institucional hacia la norma internacional NTC-ISO/IEC 27001:2022 y la adopción de los nuevos lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), establecidos en las Resoluciones 500 de 2021 y 02277 de 2025. A través del análisis del ciclo PHVA (Planear, Hacer, Verificar y Actuar), se busca no solo verificar la conformidad técnica y legal, sino también identificar oportunidades estratégicas para mitigar riesgos de ciberseguridad, proteger datos personales y elevar el nivel de madurez de la seguridad digital en la entidad.

1. OBJETIVO

Evaluar la conformidad y la eficacia del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) de IDARTES, enfocándose en la gestión de riesgos y la protección de datos personales, en los procesos críticos y los Sistemas de Información Pandora y Orfeo, utilizando como criterios la norma NTC ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC.

Objetivos Específicos

Verificación de Sistemas Críticos: Auditar la implementación y operación de los controles de seguridad en los Sistemas de Información Pandora y Orfeo, con el fin de verificar su alineación con el Anexo A de la norma ISO/IEC 27001:2022 y los controles tecnológicos establecidos en el MSPI 2025.

Evaluación Integral y Madurez: Evaluar la eficacia del SGSPI bajo el ciclo PHVA e identificar brechas y no conformidades, en el proceso de Gestión de la Protección de Datos Personales, permitiendo determinar el nivel de madurez actual de la entidad frente a los riesgos de seguridad de la información.

2. ALCANCE

El alcance de la auditoría comprende la evaluación integral de las cinco fases operativas del Modelo de Seguridad y Privacidad de la Información (MSPI): Diagnóstico (Análisis GAP), Planificación, Operación, Evaluación de Desempeño y Mejoramiento Continuo. La verificación incluye la gestión estratégica de activos de información, el proceso sistemático de valoración y tratamiento de riesgos de seguridad digital. De igual manera, el alcance integra el examen detallado de los lineamientos transversales de seguridad de la información, el ciclo de vida de la gestión de incidentes, los controles de la seguridad en la relación con proveedores de TIC y los controles específicos para el uso de servicios en la nube, garantizando en todo momento la alineación con los estándares de la norma ISO/IEC 27001:2022 y el marco jurídico nacional proferido por el MinTIC.

3. METODOLOGÍA

La metodología aplicada, se fundamentó en las directrices de la normativa de auditoría, siguiendo un enfoque sistemático, independiente y basado en evidencias para garantizar la integridad y objetividad del proceso de evaluación. El ejercicio se desarrolló a través de la ejecución de entrevistas personales y virtuales, con los líderes y funcionarios de los procesos de la entidad; utilizando plataformas de conexión remota y encuentros presenciales para la recolección de testimonios técnicos y operativos. Se realizo complementariamente, un análisis documental exhaustivo de las evidencias, registros y manuales aportados por los auditados y almacenados en los sistemas de información PANDORA y ORFEO, verificando de manera rigurosa su conformidad frente a los requisitos obligatorios de la norma ISO/IEC 27001:2022 y los lineamientos del MSPI 2025.

4. CRITERIOS

Los criterios que sustentan el presente ejercicio de auditoría, se fundamentan principalmente en la Norma Técnica Colombiana NTC-ISO/IEC 27001:2022, la cual establece los requisitos para el Sistema de Gestión de Seguridad de la Información (SGSI). Asimismo, se integra el cumplimiento estricto de la Ley 1581 de 2012 y sus decretos reglamentarios, que rigen la protección de datos personales en el territorio nacional. En alineación con el marco desarrollado por MINTIC, se evaluó la observancia de la Política de Gobierno Digital y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) dictados por el MinTIC a través de las Resoluciones 500 de 2021 y 02277 de 2025. Finalmente, la auditoría contrastó las operaciones frente a las Políticas internas de Seguridad de la Información de IDARTES, incluyendo la Política de Seguridad (GTI-POL-02), la Política de

Privacidad, y los manuales de gestión de riesgos y contratación vigentes en la entidad.

5. RIESGOS DE AUDITORÍA

Ceguera Operativa: Riesgo de asumir que "no existen incidentes" debido a la falta de herramientas de detección proactiva, lo que podría ocultar compromisos de seguridad silenciosos.

Muestreo: La revisión de expedientes y equipos se realizó por muestreo, por lo que podrían existir desviaciones no detectadas en la totalidad del universo de datos.

6. RESULTADOS DE LA AUDITORÍA

6.1. FORTALEZAS

- **Infraestructura de Red Robusta:** Se evidencia una arquitectura de red (Ítem 20) bien segmentada por VLANs, con equipos perimetrales en Alta Disponibilidad, lo que garantiza la resiliencia operativa.

- **Alineación Estratégica e Interoperabilidad:** Existe una fuerte articulación con el Plan de Desarrollo Distrital y la Alta Consejería TIC. La entidad ha adoptado el uso de X-Road para interoperabilidad y ofrece servicios de datos, demostrando madurez en el Gobierno Digital.

- **Gestión de Backups y Activos:** Se cumple rigurosamente con la política de copias de seguridad (Ítem 15) y se mantiene un inventario de activos de información consolidado y publicado (Ítem 13), lo cual es la base para cualquier estrategia de defensa.

- **Cultura de Inventario:** Los procesos misionales (Teatros, Escenarios) tienen claridad sobre sus activos físicos y tecnológicos, facilitando la trazabilidad.

- **Alineación Estratégica y Gobernanza:** Se evidencia que el Modelo de Seguridad y Privacidad de la Información (MSPI), está plenamente alineado con el Plan Estratégico Institucional y el Plan de Desarrollo Distrital. La entidad utiliza el Plan Estratégico de Tecnologías de la Información (PETI), como una hoja de ruta dinámica que integra las recomendaciones de la Alta Consejería Distrital de las TIC, para fortalecer la transparencia y la seguridad digital.

- **Cultura Organizacional y Capacitación:** Existe un compromiso sólido con la formación del personal, integrando formalmente el MSPI dentro del Plan Institucional de Capacitaciones (PIC). Esto se complementa con estrategias de uso y apropiación alineadas a la arquitectura empresarial, que incluyen charlas específicas sobre la transición a la norma ISO 27001:2022 y evaluaciones de conocimiento antes y después de las capacitaciones.

- **Segregación de Funciones y Control de Acceso:** Los sistemas de información críticos, como SIF, SiCapital (módulo Perno) y Orfeo, cuentan con una estructura definida de roles y perfiles. El acceso a funciones sensibles (como la liquidación de nómina o radicación de procesos disciplinarios) está restringido a personal autorizado y es validado periódicamente por los jefes inmediatos a través de la mesa de servicio.

- **Gestión del Ciclo de Vida de los Activos:** La entidad dispone de procedimientos estandarizados para la identificación, placa y control de inventarios de bienes físicos (hardware) a través del módulo SAI/SiCapital. Al mismo tiempo, destaca el proceso de "Baja de Bienes", el cual exige un concepto técnico del área de tecnología para asegurar el resguardo o borrado de la información antes de la disposición final de los equipos.

- **Legalidad y Protección de Datos de Terceros:** Se identifican mecanismos robustos para garantizar la privacidad, tales como la inclusión de cláusulas de confidencialidad en los contratos de vigilancia, aseo, alianzas comerciales y para los jurados del banco de expertos. De igual forma, el proceso de formación artística (Nidos y Crea) aplica protocolos estrictos y formatos específicos para la autorización del uso de imagen y tratamiento de datos de niños, niñas y adolescentes.

- **Monitoreo y Resiliencia Tecnológica:** La entidad realiza un monitoreo proactivo mediante herramientas de análisis de vulnerabilidades (Nessus) y cuenta con un esquema de copias de seguridad diarias en la madrugada para plataformas críticas. Adicionalmente, IDARTES participa en pilotos de monitoreo de seguridad (SOC/CERT) 24/7 con la Alta Consejería Distrital para detectar amenazas en tiempo real sobre servicios transversales.

6.2. CUMPLIMIENTOS

- **Gestión Proactiva de Vulnerabilidades Técnicas**

La entidad demuestra un cumplimiento sólido del control A.8.8 (Gestión de vulnerabilidades técnicas,) mediante la ejecución sistemática de escaneos periódicos en ciclos definidos (julio y noviembre de 2025). Este ejercicio abarca el núcleo de la infraestructura digital, incluyendo aplicaciones críticas para la misionalidad como Orfeo y Pandora, así como el ecosistema de servicios web institucionales, utilizando herramientas especializadas como Nessus para garantizar un estado de "sanitización" técnica.

Este proceso trasciende la detección, pues se integra en un flujo de remediación documentado donde los hallazgos críticos y altos, son priorizados para su atención por las áreas de infraestructura y desarrollo. Al finalizar cada ciclo, se realizan pruebas de re-testeo, para validar la efectividad de las correcciones, lo que asegura que el riesgo residual se mantenga dentro de los niveles de aceptación institucional y se cumpla con la fase de Evaluación de Desempeño del MSPI.

- **Trazabilidad y Control del Ciclo de Vida de Identidades**

IDARTES asegura una correlación efectiva entre la gestión administrativa y la seguridad lógica conforme a los controles A.5.16 (Gestión de la identidad) y A.5.18 (Derechos de acceso). Se evidencia que toda creación, modificación o revocación de cuentas en el Directorio Activo, nace de una solicitud formal en la Mesa de Ayuda (GLPI), la cual requiere la autorización explícita del superior o jefe inmediato, garantizando que cada acceso cuente con un soporte administrativo y una justificación por necesidad del proceso.

Esta dinámica permite mantener una trazabilidad completa sobre el historial de accesos, facilitando procesos de auditoría y reduciendo la probabilidad de existencia de "cuentas huérfanas" o accesos no autorizados. Por lo demás, la segregación de funciones se fortalece al vincular las funcionalidades de los aplicativos (como en el módulo Perno o SIF) con roles específicos aprobados desde el ingreso del funcionario, cumpliendo rigurosamente con la política de mínimo privilegio.

- **Monitoreo Centralizado y Resiliencia de Terminales**

La entidad ha robustecido su capacidad de detección y respuesta mediante la implementación de un esquema de registros centralizado en la herramienta de ORION, alineado al control A.8.15 (Registros de eventos). Esta arquitectura permite la agregación de logs de diversos componentes de la infraestructura, facilitando la identificación proactiva de anomalías y el monitoreo constante de la salud de la red en tiempo real.

Se adiciona, la garantía de la protección del perímetro final con el monitoreo de antivirus en más de 900 estaciones de trabajo, asegurando que los dispositivos de los colaboradores, mantengan firmas actualizadas y controles de integridad. Esta estrategia de monitoreo se ve potenciada por la participación en pilotos de seguridad con la Alta Consejería Distrital de las TIC, lo que eleva la postura de ciberseguridad institucional hacia un modelo de vigilancia 24/7, fundamental para la fase de Operación del MSPI

- **Alineación del MSPI con la Estrategia Institucional**

La entidad demuestra una integración efectiva entre el Modelo de Seguridad y Privacidad de la Información (MSPI) y su planeación estratégica. Los objetivos de seguridad se encuentran alineados con el Plan Estratégico de Tecnologías de la Información (PETI), el cual a su vez responde a las metas del Plan de Desarrollo Distrital y las directrices de la Alta Consejería Distrital de las TIC.

Este cumplimiento se evidencia mediante el seguimiento cuatrimestral de las actividades de seguridad reportadas ante el Comité Institucional de Gestión y Desempeño. La aprobación formal de estos avances por la alta dirección asegura que la seguridad de la información no sea un esfuerzo aislado, sino un componente transversal de la gobernanza institucional.

- **Institucionalización de la Capacitación en Seguridad**

IDARTES ha logrado incluir la seguridad de la información, dentro del Plan Institucional de Capacitaciones (PIC). Se realizan charlas y jornadas de sensibilización, ejecutadas desde la oficina de planeación para toda la comunidad de colaboradores, abordando temas críticos como la transición a la norma ISO 27001:2022 y la gestión de datos personales.

Para garantizar la efectividad de estas acciones, la entidad utiliza formatos de asistencia y realiza evaluaciones de conocimiento antes y después de las sesiones. Este enfoque permite medir el nivel de apropiación de los conceptos de seguridad por parte del personal, cumpliendo con el requisito de toma de conciencia de la norma internacional.

- **Formalización y Control del Teletrabajo**

Existe una política de teletrabajo codificada y disponible para consulta en la Intranet institucional, la cual regula el acceso a esta modalidad, mediante convocatorias formales y la validación de un comité técnico. El proceso garantiza que el trabajo remoto se realice bajo condiciones controladas y aprobadas administrativamente.

Como control preventivo, la Oficina de Tecnologías de la Información (OPTI) realiza inspecciones técnicas obligatorias a los equipos y la conectividad de los teletrabajadores antes de su autorización. Adicionalmente, el personal recibe capacitación específica sobre el manejo seguro de la información fuera de las instalaciones físicas, asegurando la resiliencia del perímetro lógico.

- **Segregación de Funciones en Sistemas Críticos**

Se evidencia una robusta segregación de funciones en el manejo de aplicativos sensibles como SIF y SiCapital (módulo Perno). El acceso se basa en roles y perfiles diferenciados, donde las tareas de ingreso de información, revisión y aprobación final de procesos financieros están asignadas a funcionarios distintos.

Este control de acceso es gestionado formalmente a través de la mesa de servicio, requiriendo la autorización explícita del jefe inmediato o supervisor del contrato para la activación de funcionalidades. Esto minimiza el riesgo de errores no detectados o manipulaciones no autorizadas de la información institucional.

- **Protección Integral de Datos de Infancia y Adolescencia**

El proceso de Formación Artística (Nidos y Crea) cumple con protocolos estrictos para el tratamiento de datos de niños, niñas y adolescentes. Se utilizan formatos específicos de autorización para el uso de imagen y obras, los cuales son requisito indispensable para la participación en eventos o publicaciones en redes sociales.

La información recolectada se almacena en el sistema SIF, el cual cuenta con campos dedicados para cargar estas autorizaciones digitales y físicas. El acceso a estos datos sensibles, está restringido a un número limitado de roles dentro de la gerencia, garantizando la confidencialidad exigida por la Ley 1581 de 2012.

- **Gestión de Inventarios y Responsabilidad de Activos**

La entidad utiliza el aplicativo Sin Capital (módulo SAI) para la identificación y control de sus bienes físicos. Este sistema permite la trazabilidad completa del hardware, asignando cada activo a un funcionario o contratista responsable ("inventario a cargo") mediante un número de placa y registro oficial.

El proceso de asignación se encuentra articulado con el sistema de gestión documental Orfeo, donde se radican los comunicados de movimiento de inventario, para sustentar la responsabilidad del tenedor. Esta integración asegura que cada activo tecnológico tenga un doliente identificado dentro de la estructura organizacional.

- **Protocolo Seguro de Baja de Bienes Tecnológicos**

IDARTES cuenta con un procedimiento formal para la baja de bienes que contempla la seguridad de la información, como un paso crítico antes de la disposición final. Los equipos tecnológicos que ya no se utilizan, deben pasar por una revisión técnica especializada antes de ser retirados.

Para ejecutar la baja, se requiere obligatoriamente un concepto técnico emitido por el área de tecnología, el cual certifica que el equipo se encuentra en condiciones adecuadas para el egreso y que se han realizado los procesos de resguardo o borrado de información pertinente. Esto previene la fuga accidental de datos en medios de almacenamiento descartados.

- **Clasificación de Información en Gestión Documental**

El sistema de gestión documental Orfeo, ha sido parametrizado para permitir la clasificación de la información conforme a la Ley 1712 de 2014. Los funcionarios pueden etiquetar los radicados como públicos, clasificados o reservados según la naturaleza del trámite.

Se han identificado y capacitado específicamente a las unidades que manejan series documentales sensibles, como historias laborales, procesos disciplinarios y datos de primera infancia, para asegurar que la restricción de acceso, sea aplicada desde la radicación. Esto garantiza que solo el personal competente visualice la información restringida.

- **Trazabilidad y Verificación de Nómina**

El proceso de liquidación de nómina, cuenta con niveles de seguridad que garantizan la integridad de los pagos. El sistema SiCapital registra la "huella digital" de cada transacción, permitiendo identificar quién ingresó las novedades y quién dio el visto bueno final.

Al final de cada periodo, los informes generados incluyen las firmas electrónicas de los responsables, lo que proporciona una pista de auditoría sólida. Este mecanismo permite realizar conciliaciones precisas y asegura que no se realicen modificaciones salariales sin la debida cadena de revisión.

- **Compromisos de Confidencialidad con Terceros**

La entidad extiende sus políticas de seguridad a proveedores y aliados, mediante la inclusión de cláusulas de confidencialidad en los contratos de servicios transversales, como vigilancia y aseo. Los contratistas asumen la obligación legal de no divulgar información reservada conocida en ejercicio de sus funciones.

Para el caso del banco de expertos y jurados, es requisito obligatorio la firma de un acuerdo de confidencialidad para acceder a las propuestas artísticas. Estos acuerdos son revisados por la Subdirección Jurídica y quedan radicados en Orfeo como parte del acervo documental del proceso.

- **Esquema de Copias de Respaldo y Recuperación**

Se ha establecido un esquema de copias de seguridad automáticas para plataformas críticas como SIF, las cuales se ejecutan diariamente en horas de la madrugada. Este control asegura la disponibilidad de la información ante posibles fallos técnicos o ataques de integridad.

La responsabilidad de estos respaldos recae en la OPTI, que actúa como custodio técnico de la información almacenada en la infraestructura institucional. La ausencia

de solicitudes de restauración por pérdida de datos, en el último año sugiere una estabilidad operativa positiva del entorno tecnológico.

- **Gestión Documental del Ciclo de Vida de la Información**

IDARTES cumple con la normativa archivística nacional mediante la aplicación de Tablas de Retención Documental (TRD) vigentes. El proceso asegura que la documentación física y digital se conserve durante los tiempos de retención estipulados según su ciclo vital.

En cuanto a la eliminación, existe un protocolo que incluye la trituración por empresas certificadas, que garantizan que los documentos no puedan ser reconstruidos. El proceso exige dejar evidencia en video y actas firmadas, asegurando una disposición final segura que previene la recuperación no autorizada de datos.

- **Control de Acceso Físico y Monitoreo**

La entidad dispone de un sistema compartido de Circuito Cerrado de Televisión (CCTV), para el monitoreo de sus sedes y equipamientos culturales. Este sistema combina recursos propios y servicios del contrato de vigilancia para robustecer la seguridad física de los activos.

El acceso a las instalaciones, está regulado por el uso de carné institucional y registros en minutas de ingreso para visitantes y equipos personales. Áreas sensibles como las bodegas de almacenamiento, requieren una autorización firmada por el almacenista general y el supervisor de vigilancia, elevando el nivel de control sobre bienes críticos.

- **Proceso de Paz y Salvo para Desvinculación**

IDARTES cuenta con un procedimiento formal de desvinculación de personal, que incluye la entrega obligatoria de activos de información y cierre de credenciales. Se utiliza un formato de "paz y salvo" que requiere la firma de seis dependencias, incluyendo sistemas, almacén y gestión documental.

Para los contratistas, este proceso se gestiona digitalmente a través del sistema Pandora, donde se verifica el reintegro de equipos y la entrega de backups documentales, antes de autorizar el último pago. Si un funcionario incumple con esta entrega, el caso es remitido a Control Disciplinario, asegurando que la salida del personal no comprometa la integridad de los activos institucionales.

6.3. OBSERVACIONES

Como resultado del ejercicio de auditoría interna realizado al Sistema de Gestión de Seguridad y Privacidad de la Información (MSPI) de IDARTES, y bajo los lineamientos técnicos de la norma NTC-ISO-IEC 27001:2022, se detallan a continuación las observaciones y hallazgos identificados. Este análisis integral, producto de entrevistas directas con los líderes de proceso y una revisión exhaustiva de las evidencias documentales, tiene como fin evaluar el nivel de conformidad de los controles organizacionales, de personas y tecnológicos. Los puntos descritos a continuación, reflejan tanto las capacidades actuales de la entidad, como los riesgos críticos que requieren atención inmediata para fortalecer la resiliencia institucional y garantizar la protección de los activos de información.

OBS-01: Vacancia del Rol de Oficial Seguridad (CISO). (Control A.5.2)

Criterio: La norma ISO 27001:2022 exige la definición y asignación clara de roles y responsabilidades para la seguridad de la información dentro de la entidad.

Evidencia: Durante la entrevista con Talento Humano, se confirmó que el cargo de "Profesional Universitario" creado en la planta temporal para liderar el MSPI, se encuentra vacante. El proceso de contratación falló en septiembre de 2025 y se estima retomar la convocatoria solo hasta mayo de 2026.

Hallazgo: Existe una brecha en la gobernanza del sistema, ya que la entidad no cuenta actualmente con un líder o CISO formalmente vinculado para dirigir la transición hacia la nueva norma, lo que genera un riesgo de desatención en la gestión estratégica de la seguridad.

OBS-02: Manejo de Información Sensible sin Clasificación ni Cifrado (Controles A.5.12 y A.5.14)

Criterio: La información debe clasificarse según su sensibilidad y los medios de transferencia deben ser seguros para evitar divulgaciones no autorizadas.

Evidencia: El equipo de nómina utiliza archivos paralelos en Excel con datos financieros y personales sensibles, los cuales son compartidos vía correo electrónico estándar (Gmail), sin etiquetas de clasificación ni protección por contraseña. La funcionaria de nómina describe que no utilizan los niveles de clasificación disponibles en la herramienta.

Hallazgo: El tratamiento de la información no estructurada (hojas de trabajo), durante la liquidación de nómina incumple los requisitos de confidencialidad y transferencia segura, exponiendo datos personales masivos a riesgos de fuga por error humano.

OBS-03: Deficiencia en los Atributos de Seguridad del Inventario de Activos (Control A.5.9)

Criterio: El inventario de activos debe incluir, además de la identificación física, la clasificación de seguridad y la identificación del propietario de la información.

Evidencia: El sistema de inventario SAI (SiCapital), funciona exclusivamente como un listado contable y administrativo. Se confirmó que el sistema permite asignar un responsable físico, pero carece de campos para registrar la clasificación de la información (Confidencialidad, Integridad, Disponibilidad).

Hallazgo: El inventario actual no cumple con el estándar de seguridad de la información, al no permitir la identificación de la sensibilidad del activo, lo que dificulta la aplicación de controles proporcionales al riesgo.

OBS-04: Falta de Metodología Formal de Desarrollo de Software Seguro (Control A.8.25)

Criterio: Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas de información.

Evidencia: La Oficina de Tecnología (OPTI) y los líderes de desarrollo del SIF, manifestaron utilizar la metodología Scrum. Sin embargo, se evidencia que no cuentan con un ciclo de vida de desarrollo seguro (SDLC) formalizado, ni la aplicación metodología técnica de seguridad (como OWASP) integrada en sus procesos.

Hallazgo: El proceso de desarrollo de software se centra en la agilidad operativa, pero carece de un marco técnico de seguridad obligatorio, lo que incrementa el riesgo de introducir vulnerabilidades desde la fase de diseño.

OBS-05 Deficiencia en la Capacidad de Respuesta y Detección de Incidentes (Controles A.5.24 y A.5.26)

Criterio:

- NTC-ISO-IEC 27001:2022, Control A.5.24: Requiere que la organización planifique y prepare la gestión de incidentes mediante la definición y documentación de procesos de respuesta.
- NTC-ISO-IEC 27001:2022, Control A.5.26: Establece que se debe dar respuesta a los incidentes siguiendo procedimientos técnicos documentados.
- Lineamientos de Gestión de Incidentes MSPI 2025: Exige la implementación de planes de respuesta, que incluyan la detección rápida para minimizar el impacto y restaurar servicios críticos.

Evidencia:

- Durante la entrevista con el equipo de la OAPTI, se manifestó que no se cuenta con "Playbooks" o guías técnicas documentadas, para enfrentar escenarios críticos específicos como Ransomware o Fuga de Información.
- La entidad reportó oficialmente "Cero Incidentes" de seguridad materializados durante el último año en procesos misionales y administrativos.
- Se constató que, aunque se cuenta con monitoreo básico y centralización de logs (ORION Kiwi Syslog), no se evidencia el uso de herramientas de detección avanzada (tipo SIEM o EDR), que permitan identificar amenazas sofisticadas o comportamientos anómalos de forma proactiva en las más de 900 estaciones de trabajo.

Hallazgo

- Existe un incumplimiento en la fase de "Preparación" del ciclo de vida de incidentes definido en el MSPI. La carencia de guías estandarizadas (Playbooks), genera una alta dependencia de la idoneidad del personal y vulnera la capacidad de respuesta oportuna ante ataques de propagación rápida.
- El reporte de "Cero Incidentes" no es consistente con la infraestructura actual de la entidad, lo que sugiere una incapacidad técnica de detección profunda más que una ausencia real de amenazas. Esta brecha de visibilidad técnica,

impide la mejora continua y contraviene los principios de resiliencia digital exigidos por la norma y el modelo nacional de seguridad.

OBS – 06 Desconexión en la Propiedad y Aceptación de Riesgos de Seguridad de la Información (Requisitos 6.1.2, 6.1.3 (e) y 7.3.3)

Criterio:

- NTC-ISO-IEC 27001:2022, Cláusula 6.1.2: La organización debe identificar a los dueños de los riesgos de seguridad de la información.
- NTC-ISO-IEC 27001:2022, Cláusula 6.1.3 (e): Se requiere obtener la aprobación de los dueños de los riesgos sobre el plan de tratamiento y la aceptación de los riesgos residuales.
- Modelo Maestro MSPI 2025, Numeral 7.3.3: Establece que los dueños de los riesgos deben ser los líderes de los procesos afectados y realizar la aprobación formal del plan de tratamiento.

Evidencia:

- Durante las entrevistas con las áreas misionales y de apoyo (Talento Humano, Gestión de Circulación, Fomento), los líderes de proceso manifestaron de manera recurrente, que "no poseen riesgos de tecnología de la información" asociados a sus actividades.
- Se evidenció que la Oficina Asesora de Planeación y Tecnologías de la Información (OAPTI), mantiene una matriz técnica de riesgos de seguridad ("documento vivo") en la que se evalúan vulnerabilidades y amenazas sobre activos críticos como bases de datos y sistemas de información.
- Sin embargo, el equipo de la OAPTI, confirmó en entrevista que no se ha formalizado la notificación ni la aceptación del riesgo por parte de los líderes de los procesos (dueños de la información), admitiendo la falta de este mecanismo de aprobación en el ciclo actual de gestión.

Hallazgo:

- Se identifica un incumplimiento en la asignación de la responsabilidad sobre los riesgos. La entidad gestiona los riesgos de seguridad como una "bolsa" netamente técnica bajo la custodia de la OAPTI, omitiendo la formalidad del rol del Dueño del Riesgo (Risk Owner) en las áreas funcionales.

- La carencia de una notificación formal y una respuesta de aceptación por parte del negocio genera un vacío de control, donde el líder del proceso desconoce el nivel de riesgo residual, que asume al operar sus activos de información (ej. SIF, Orfeo, Pandora). Esta situación contraviene la metodología institucional y los requisitos de gobernanza de la norma ISO 27001, impidiendo que la Alta Dirección tome decisiones informadas sobre la asignación de recursos para el tratamiento de riesgos críticos.

OBS-07 Vacío en la Gobernanza y Gestión de la Protección de Datos Personales (Controles A.5.2 y A.5.34)

Criterio:

- ISO/IEC 27001:2022, Control A.5.2 (Roles y responsabilidades de seguridad de la información): Los roles y responsabilidades de seguridad de la información deben asignarse y comunicarse dentro de la organización.

- ISO/IEC 27001:2022, Control A.5.34 (Privacidad y protección de la PII): La organización debe identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la información de identificación personal (PII) de acuerdo con las leyes y reglamentos aplicables.

- Documento Maestro MSPI 2025 (Numeral 6.1): Define el rol del Oficial de Protección de Datos Personales (OPD) como el encargado de velar por la implementación efectiva de las políticas y procedimientos para cumplir el Régimen de Protección de Datos Personales de Colombia.

- Ley 1581 de 2012: Marco legal nacional para la protección de datos personales.

Evidencia:

- En entrevista con la Subdirección Jurídica, se manifestó que actualmente existe un "vacío" en la aplicación de la política de protección de datos

personales y que el rol del oficial está en proceso de análisis para determinar su perfil e idoneidad.

- El equipo de la Oficina Asesora de Planeación y Tecnologías de la Información (OAPTI) confirmó que las actividades de protección de datos quedaron en el "limbo" tras la desvinculación de un abogado contratado anteriormente por Jurídica para este fin.

- Se evidenció incertidumbre administrativa entre los procesos de Planeación y Jurídica, respecto a la responsabilidad directa sobre la actualización y liderazgo de la Política de Protección de Datos Personales.

- A pesar de contar con aproximadamente 400 bases de datos registradas ante la Superintendencia de Industria y Comercio (SIC), no hay un funcionario o equipo asignado para realizar el reporte de novedades o la gestión de incidentes específicos de datos personales.

Hallazgo :

- Existe un incumplimiento en la estructura de gobernanza del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), debido a la ausencia de un Oficial de Protección de Datos Personales (OPD) o responsable designado. Esta carencia ha provocado la suspensión de actividades críticas, como la actualización de la Política de Protección de Datos y el monitoreo de bases de datos ante la SIC.

- La falta de claridad en la asignación del rol entre las áreas Jurídica y Planeación, vulnera la capacidad de la entidad para garantizar la privacidad de los datos de ciudadanos y artistas, contraviniendo el control A.5.34 de la norma ISO 27001:2022 y los lineamientos obligatorios del MSPI 2025 para entidades del Estado.

- Riesgo Asociado: Probabilidad de sanciones legales por parte de la autoridad de control (SIC), inadecuado tratamiento de datos sensibles de niños, niñas y adolescentes en programas misionales (Nidos y Crea), e incapacidad de respuesta efectiva ante incidentes de fuga de información personal.

OBS-08 Debilidad en la Estandarización de Roles y Perfiles en el Sistema Orfeo (Controles A.5.15 y A.5.18)

Criterio:

- NTC-ISO-IEC 27001:2022, Control A.5.15 (Control de acceso): Se debe establecer, documentar y revisar una política de control de acceso, con base en los requisitos del negocio y de seguridad de la información.

- NTC-ISO-IEC 27001:2022, Control A.5.18 (Derechos de acceso): Se debe restringir y controlar la asignación y uso de derechos de acceso.

- Documento Maestro MSPI 2025 (Lineamientos de Roles y Responsabilidades): La definición de roles es fundamental para establecer tareas precisas, minimizar ambigüedades y reducir el riesgo de imprecisiones en la ejecución de funciones.

Evidencia:

- Durante la entrevista con el equipo de Gestión Documental, el administrador del sistema Orfeo indica claramente: "no existe una estandarización de roles y perfiles, sino que lo que se tiene es activaciones funcionales, de acuerdo a las necesidades de cada persona en su actividad por proceso".

- Se constató que la asignación de permisos se basa en la solicitud del jefe inmediato de cada área, quien decide “qué” funcionalidades requiere cada persona bajo su cargo en un momento determinado.

- El proceso de creación de usuarios e implementación de funcionalidades, se ejecuta de forma manual a través de la mesa de servicio, tras la validación administrativa del supervisor del contrato o jefe.

- Información entregada por la Oficina de Tecnologías de la Información (OPTI) de roles y perfiles de las aplicaciones de Pandora y Orfeo

Hallazgo:

- Se identifica una debilidad en la gobernanza de accesos para la aplicación crítica Orfeo. La ausencia de una matriz de perfiles estandarizada, impide que las reglas de acceso se basen en requisitos técnicos y de seguridad predefinidos por la entidad, derivando en un modelo de gestión "ad-hoc".

- Al no existir perfiles definidos por cargo o función, la asignación de derechos queda sujeta al criterio individual del jefe de área, lo que incrementa el riesgo de acumulación de privilegios (privilege creep) y dificulta la realización de auditorías de cumplimiento efectivas sobre quién tiene acceso a qué información y por qué motivo de negocio.

- Esta práctica contraviene el principio de mínimo privilegio y la exigencia de la norma de contar con reglas de control de acceso documentadas y basadas en el riesgo institucional.

OBS-09 Ausencia de Controles Formales y Protocolos de Seguridad en Plataformas Sectoriales Externas (Controles A.5.19 y A.5.23)

Criterio:

- NTC-ISO-IEC 27001:2022, Control A.5.19 (Seguridad de la información en las relaciones con los proveedores): Los requisitos de seguridad para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar y documentar.
- NTC-ISO-IEC 27001:2022, Control A.5.23 (Seguridad de la información para el uso de servicios en la nube): Los procesos de adquisición, uso y gestión de servicios externos, deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.
- Modelo de Seguridad y Privacidad de la Información (MSPI) 2025: Establece que la gestión de seguridad con proveedores debe abordarse de forma integral, incluyendo requisitos contractuales, evaluación de riesgos y medidas técnicas específicas.

Evidencia:

- Durante las entrevistas con los procesos de Circulación y Fomento, se evidenció una dependencia crítica de la plataforma CultuRed y sus módulos asociados, los cuales son administrados y autorizados externamente por la Secretaría de Cultura.
- Se confirmó que IDARTES no ejerce control directo sobre la administración, creación o revocación de usuarios en estas plataformas, ni posee visibilidad sobre los controles de integridad aplicados a los datos institucionales allí alojados.
- Los auditados manifestaron que la Secretaría de Cultura se encuentra aún en proceso de definición de los protocolos formales para la solicitud de usuarios, lo que implica que el intercambio de información y el acceso a datos

sensibles como insumos al proceso que se realiza actualmente sin un marco operativo estandarizado.

- **Hallazgo** :

- En esta observación se identifica un riesgo de cumplimiento normativo y operativo debido a la falta de acuerdos de nivel de servicio (SLA) técnicos y protocolos de seguridad formalizados con la Secretaría de Cultura para el uso de plataformas compartidas.
- La entidad opera bajo un modelo de confianza ciega hacia el tercero administrador, vulnerando el principio de responsabilidad compartida definido en el MSPI, donde la entidad debe verificar que los controles aplicados por terceros, estén alineados con su propio plan de tratamiento de riesgos.
- La ausencia de la socialización del entendimiento técnicos o protocolos documentados para la gestión de incidentes y el control de accesos en estas plataformas externas, impide garantizar la integridad de estos insumos gestionados por IDARTES.

7. CONCLUSIONES

Madurez Documental vs. Vacío de Liderazgo Operativo: IDARTES demuestra un avance significativo en la alineación de su Plan Estratégico de TI (PETI) con los objetivos de seguridad y la actualización de sus políticas internas. No obstante, la vacancia actual del rol de Oficial de Seguridad (CISO) representa una debilidad crítica en la gestión, ya que la ausencia de un líder formalmente vinculado dificulta la transición efectiva hacia la norma 27001:2022 y delega la responsabilidad estratégica en un equipo técnico que actúa bajo un esquema de "arte y parte".

Capacidad de Detección y Falso Sentido de Seguridad: La gestión técnica ha logrado centralizar logs y realizar escaneos de vulnerabilidades periódicos ; sin embargo, el reporte de "Cero Incidentes" en el último año, ante la falta de herramientas de detección profunda (tipo SIEM o EDR), sugiere una incapacidad técnica de visibilidad más que una ausencia real de amenazas. La gestión debe migrar de un monitoreo de disponibilidad a uno de detección de comportamientos anómalos para garantizar la verdadera resiliencia del sistema.

La ausencia de un Oficial de Seguridad (CISO) y un Oficial de Protección de Datos (DPO) formales, ha derivado en una gestión de riesgos administrativa (cumplir el

papel) en lugar de técnica (anticipar el ataque). La sensación de falsa seguridad ("no tenemos incidentes") es el mayor riesgo latente, pues la entidad no está preparada procedimentalmente para responder cuando un incidente inevitablemente ocurra.

Fortalecimiento del Ciclo de Vida de Desarrollo y Dependencias Externas: Se propone integrar formalmente una Metodología de Desarrollo Seguro (S-SDLC) que obligue a realizar pruebas de seguridad desde el diseño y no solo antes del despliegue. Complementariamente, es imperativo formalizar Memorandos de Entendimiento Técnicos con la Secretaría de Cultura para las plataformas externas (CultuRed), asegurando que IDARTES establezca protocolos de interacción sobre la administración de accesos y la integridad de los datos de los artistas y ciudadanos.

8. RECOMENDACIONES

Retomar y concluir el proceso de vinculación de oficial de seguridad: Es prioritario completar la contratación de la persona encargada de dirigir la seguridad de la información, ya que actualmente el puesto está vacío. Sin este líder, la entidad no tiene una cabeza estratégica que tome las decisiones necesarias para protegernos contra riesgos digitales, lo que podría retrasar la actualización de nuestras defensas según las nuevas normas nacionales.

Asegurar el manejo de la nómina y datos sensibles: Debemos cambiar de inmediato la forma en que se comparten los archivos de Excel con información de sueldos y datos personales a través del correo electrónico. Se recomienda dejar de enviar estos archivos como adjuntos simples y empezar a usar carpetas digitales seguras con llaves de acceso o ponerles contraseñas obligatorias, evitando así que un error humano al escribir una dirección de correo exponga la vida privada de los trabajadores.

Saber qué información es la más valiosa en el inventario: El listado actual de computadores y programas debe incluir una marca que diga qué tan secreta o importante es la información que contienen. Hoy solo sabemos a quién le entregamos cada equipo para temas de contabilidad, pero no sabemos cuáles guardan los datos más delicados, lo que nos impide darles una protección especial a los que más lo necesitan.

Construir programas informáticos más resistentes: Al crear o mejorar las aplicaciones de la entidad, debemos incluir pruebas de seguridad desde el primer día de diseño y no solo al final. No es suficiente con que el sistema funcione rápido; hay que asegurar que esté construido con "cerrojos digitales" internos para que sea difícil de atacar, siguiendo guías internacionales que eviten fallas que luego sean costosas de arreglar.

Crear manuales para actuar ante ataques digitales: Necesitamos guías escritas que digan paso a paso qué debe hacer el equipo técnico si sufrimos un ataque grave, como el secuestro de información o la pérdida de datos. No podemos depender solo de la memoria del personal; estos manuales de emergencia son como los de un simulacro de incendio, pero para nuestra red, y nos permitirán reaccionar rápido para que el servicio no se detenga por mucho tiempo.

Formalizar el uso de aplicaciones de otras entidades: Es necesario firmar acuerdos oficiales con la Secretaría de Cultura para definir cómo se cuidan los datos en plataformas compartidas como CultuRed. Actualmente dependemos de ellos, pero IDARTES no tiene control sobre quién entra o cómo se protegen esos datos; estos acuerdos deben dejar claro quién responde si algo falla y asegurar que la información de nuestros artistas siempre esté segura.

Definir un único responsable para la privacidad de datos: La dirección debe formalizar qué oficina (Jurídica o Planeación) es la encargada de liderar la protección de datos personales de los ciudadanos. Actualmente hay una confusión sobre quién tiene el mando, y este vacío de poder puede causar que incumplamos leyes nacionales o que no reportemos a tiempo nuestras bases de datos ante las autoridades de control.

Controlar cada cambio en los sistemas de cómputo: Debemos hacer obligatorio que, antes de cualquier cambio importante en nuestras redes o servidores, se registre y se evalúe si ese ajuste puede abrir un hueco de seguridad, ya que actualmente este procedimiento no se está aplicando formalmente. Es urgente corregir los fallos reportados en el sistema Pandora, específicamente la duplicidad de registros y los errores en las consultas que dejan a la vista el código interno de la herramienta, lo cual compromete seriamente la privacidad de la tecnología institucional. A veces, por arreglar algo con rapidez, se pueden debilitar las defensas de la entidad sin que lo notemos; por tanto, un control ordenado de estos cambios nos permitirá evitar caídas inesperadas y garantizar que las aplicaciones funcionen siempre de manera segura y confiable

ANEXO N°.1: DETALLE OBSERVACIONES

#	OBSERVACIÓN	DESCRIPCIÓN DETALLADA	POSIBLE RESPONSABLE
1	**Vacancia del Rol de Oficial de Seguridad (CISO)**	El cargo de "Profesional Universitario" creado para liderar el MSPI está vacante desde septiembre de 2025. Esta brecha en la gobernanza genera un riesgo crítico en la gestión estratégica y la transición normativa.	**Talento Humano / OAPTI**
2	**Manejo Inseguro de Información de Nómina**	Uso de archivos Excel con datos financieros y personales sensibles compartidos vía Gmail sin clasificación, cifrado, ni protección por contraseña, contraviniendo los controles de transferencia segura.	**Talento Humano (Nómina)**
3	**Deficiencia en Atributos del Inventario de Activos**	El sistema SAI (Sin Capital) opera bajo un enfoque netamente contable y administrativo. Carece de campos para la clasificación de seguridad (Confidencialidad, Integridad y Disponibilidad).	**OAPTI / Almacén**
4	**Falta de Metodología de Desarrollo Seguro**	El desarrollo de software (ej. SIF) utiliza Scrum para agilidad, pero no integra un ciclo de vida de desarrollo seguro (SDLC) ni metodologías técnicas como OWASP para prevenir vulnerabilidades desde el diseño.	**OAPTI (Gestión de Software)**
5	**Deficiencia en Detección y Respuesta a Incidentes**	Inexistencia de "Playbooks" técnicos documentados para escenarios de alto impacto. El reporte de "Cero Incidentes" sugiere una incapacidad técnica de detección profunda ante la falta de herramientas tipo SIEM o EDR.	**OAPTI (Seguridad Informática)**
6	**Desconexión en la Propiedad de los Riesgos**	Los líderes de procesos funcionales desconocen o niegan poseer riesgos de TI. La OAPTI gestiona la matriz de riesgos de forma técnica sin una notificación formal ni aceptación de riesgos residuales por parte de los dueños del negocio.	**Líderes de Proceso / OAPTI**

#	OBSERVACIÓN	DESCRIPCIÓN DETALLADA	POSIBLE RESPONSABLE
7	**Vacío en la Gobernanza de Protección de Datos**	Incertidumbre administrativa entre Jurídica y Planeación tras la salida del abogado encargado. Actualmente no hay un responsable (OPD) para la actualización de la política ni el reporte de novedades ante la SIC.	**Subdirección Jurídica / OAPTI**
8	**Debilidad en Estandarización de Roles (Orfeo)**	No existe una matriz de perfiles estandarizada para Orfeo. Las activaciones funcionales se realizan de forma manual y "ad-hoc" según criterio de cada jefe, incrementando el riesgo de acumulación de privilegios.	**Gestión Documental / OAPTI**
9	**Ausencia de Controles en Plataformas Externas**	Dependencia crítica de plataformas administradas por la Secretaría de Cultura (CultuRed) sin memorandos de entendimiento técnicos, protocolos de acceso o acuerdos de nivel de servicio (SLA) formalizados.	**OAPTI / Subdirección Jurídica**

Elaboró	**Aprobó**
Angel Antonio Diaz Vega	Eleana Marcela Páez Urrego
NOMBRE Y APELLIDO	**NOMBRE Y APELLIDO**
Cargo: /Contratista	Jefe de Oficina Control Interno