INFORME EJECUTIVO

AUDITORÍA INTERNA DE GESTIÓN AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) DEL DANE-FONDANE

Objetivo General	Evaluar la implementación y efectividad del Modelo de Seguridad y Privacidad de la Información (MSPI) en el DANE, con el fin de verificar su cumplimiento frente a los lineamientos, fases y requisitos establecidos por el MinTIC, así como determinar, mediante muestreo, si los controles de seguridad definidos son adecuados y operan de manera efectiva para mitigar los riesgos relevantes y garantizar la confidencialidad, integridad y disponibilidad de la información institucional.
Objetivos Específicos	**1.** Verificar que el Modelo de Seguridad y Privacidad de la Información del DANE se encuentre implementado conforme a las fases, lineamientos y requisitos establecidos por el MinTIC. **2.** Evaluar el proceso de identificación, valoración y tratamiento de los riesgos de seguridad de la información, verificando su coherencia con el Plan de Seguridad y Privacidad de la Información y con los riesgos relevantes de la Entidad. **3.** Verificar, a través de una muestra de controles asociados a los riesgos de seguridad de la información, si son adecuados y operan de manera efectiva para mitigar los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información, conforme a la declaración de aplicabilidad.
Alcance	La auditoría comprenderá la verificación de la implementación y operación del Modelo de Seguridad y Privacidad de la Información (MSPI) del DANE durante la vigencia 2025, conforme a lo establecido en la Resolución MinTIC 2277 de 2025, Anexo 1 – MSPI Versión 5, en el marco de los objetivos específicos planteados. La OCI no realizará pruebas técnicas especializadas de ciberseguridad ni evaluará el cumplimiento integral de los 93 controles del Anexo 1 a través de la herramienta de Diagnóstico de la OSIS y OPLAN.

1. RESULTADOS

Como resultado de las pruebas de auditoría aplicadas durante el proceso auditor, se identificaron dieciocho (18) fortalezas que evidencian el cumplimiento de la normativa aplicable a los temas evaluados, cinco (5) situaciones evidenciadas y un (1) hallazgo, a estos seis últimos se les formularon recomendaciones orientadas a fortalecer la gestión del asunto específico.

Si se requiere ampliación o detalle de las Situaciones evidenciadas, del hallazgo o de las fortalezas identificadas, lo invitamos a consultar la versión detallada del informe, que puede ser solicitada a la Oficina de Control Interno en cualquier momento.

TIPO DE OBSERVACIÓN	RESUMEN	RECOMENDACIÓN
 **H. No. 1** **Control A.7.5 Protección contra amenazas físicas y ambientales**	En verificación de la efectividad de la ejecución del control A.7.5 Protección contra amenazas físicas y ambientales, se identificó que, para el mes de septiembre se reportó: *"Sede Ibagué – 16 y 17 de septiembre – Contingencia Incendio se validó las condiciones de la infraestructura eléctrica de la sede después del incendio presentado en el cuarto técnico de sistemas."*. En este sentido la OCI evidenció que, aunque la Entidad realiza seguimiento al mantenimiento de infraestructura, existen debilidades en el diseño y en la aplicación del control, en la medida en que: el control no establece de manera expresa la realización de verificaciones técnicas integrales sobre las condiciones de protección física y ambiental y su ejecución se orienta principalmente al seguimiento documental de contratos, sin evidenciar de manera sistemática la validación técnica de componentes (red contra incendios, extintores, sistemas eléctricos, aire acondicionado, entre otros) Es importante precisar que el proceso auditado informó que el evento ocurrido en la sede de Ibagué no generó pérdida de información. No obstante, desde el enfoque de gestión de riesgos, este tipo de eventos puede derivar en impactos reputacionales y operativos para la entidad, asociados a la afectación de la disponibilidad de la información, la pérdida de infraestructura tecnológica crítica y la interrupción de la continuidad de los servicios institucionales.	• Revisar y ajustar el mecanismo de seguimiento definido en la matriz de riesgos, así como fortalecer los registros asociados a este control, de manera que se identifique de forma específica la verificación realizada a los contratos relacionados con sistemas contra incendios y extintores, incluyendo aspectos como fechas de seguimiento, responsables de la actividad y resultados de la revisión técnica. • Incorporar lecciones aprendidas del incidente a través del análisis de causa raíz del evento ocurrido en la sede Ibagué, con el fin de que se puedan detectar necesidades de ajuste de controles, planes (BCP/DRP) u otras herramientas. • Fortalecer la gestión de riesgos asegurando la formulación de planes de mejoramiento, encaminados a prevenir la recurrencia de situaciones similares.
 **S.E. No.1**	Se evidenció que la Entidad cuenta con el Plan Estratégico Institucional 2023–2026 debidamente documentado y alineado con el Plan Nacional de Desarrollo, así como con el documento de Contexto Institucional y la Política General de Seguridad de la	Formalizar e implementar un mecanismo periódico de revisión y actualización de las fuentes de información que soportan la planificación del MSPI, con una

TIPO DE OBSERVACIÓN	RESUMEN	RECOMENDACIÓN
Debilidades en la actualización de fuentes de información para la planificación del MSPI.	Información, existen oportunidades de mejora relacionadas con la actualización y trazabilidad de las fuentes de información clave (análisis de contexto, matriz de partes interesadas y declaración de aplicabilidad), que requieren revisiones periódicas, desactualización de algunos instrumentos y ausencia de control de versiones. Esta situación podría generar desalineación del modelo frente al contexto institucional, las necesidades, expectativas de las partes interesadas y los requisitos aplicables, afectando la identificación oportuna de riesgos y la adecuada definición de controles de seguridad de la información.	frecuencia definida y criterios de actualización basados en cambios del entorno interno y externo. Este mecanismo podría incluir: • La actualización del análisis de contexto institucional, incorporando factores internos y externos que puedan afectar la seguridad de la información. • La revisión y actualización de la matriz de partes interesadas, incluyendo de manera explícita sus necesidades y expectativas en materia de seguridad y privacidad de la información. • La gestión y control de versiones de la Declaración de Aplicabilidad (SoA), asegurando su trazabilidad y alineación con los riesgos identificados y los controles implementados.
S.E. No. 2 **Inconsistencias presentadas en el inventario de activos de información**	Se evidenció que la entidad cuenta con un procedimiento formal y una guía actualizada para la gestión de activos de información SIO-040-PDT-008 Procedimiento gestión de activos de información y SIO-040-GUI-011 Guía Gestión de Activos de Información, así como con un inventario consolidado de activos de información. Al evaluar la información registrada en el inventario de activos de información y la declaración de aplicabilidad, se identificaron oportunidades de mejora relacionadas con la inclusión, exclusión y correspondencia de activos	• Implementar un mecanismo formal de revisión, conciliación y actualización periódica entre el inventario de activos de información y la Declaración de Aplicabilidad (SoA), que contemple una validación cruzada, la actualización oportuna frente a cambios en los procesos o lineamientos y el control de versiones y

TIPO DE OBSERVACIÓN	RESUMEN	RECOMENDACIÓN
	requeridos para la implementación de controles de seguridad de la información, debido a diferencias en la inclusión, exclusión y forma de registro de algunos activos. Esta situación podría generar debilidades en la identificación de riesgos y en la definición de controles de seguridad, afectando la alineación entre la gestión de riesgos y la operación real de la Entidad.	trazabilidad de los ajustes realizados. • Definir lineamientos que permitan orientar de manera adecuada el diligenciamiento de los instrumentos definidos para realizar el levantamiento del Inventario de Activos de Información e incluir los documentos de referencia pertinentes en la Declaración de aplicabilidad.
S.E. No. 3 **Control 5.17 Información de autenticación**	Durante la revisión del control A.5.17 Información de autenticación, a cargo de Gestión de Transformación Digital (GTD), se identificó que la asignación y gestión de accesos a los repositorios de evidencias de los proyectos del Plan Estratégico de Tecnologías de Información (PETI) presenta desalineaciones entre el modelo formal de gobierno de proyectos y la operación efectiva de los permisos. En particular para el proyecto PRY-15, se identificó que once (11) personas contaban con permisos de acceso, mientras que el documento de gobierno del proyecto registraba cuatro (4) personas autorizadas. Adicionalmente, se observó que, en la práctica, los modelos de gobierno de los proyectos utilizan tres roles principales (patrocinador, responsable y enlace de seguimiento), mientras que el documento GTD-010-MAN-001 Manual para la Gestión de Proyectos con Componentes TIC, establece cinco (5) roles, lo que evidencia una diferencia entre el diseño formal	• Revisar y evaluar la pertinencia de ajustar los lineamientos institucionales asociados a la gestión de cambios y asignación de permisos en los proyectos del PETI, con el fin de asegurar la coherencia entre los roles definidos en el documento GTD-010-MAN-001 Manual para la Gestión de Proyectos con Componentes TIC, los roles efectivamente utilizados en los gobiernos de proyecto y los permisos otorgados técnicamente sobre los repositorios de evidencias. • Evaluar la frecuencia de revisión de accesos a los repositorios de evidencias de los proyectos, con el propósito de determinar si la periodicidad anual resulta

TIPO DE OBSERVACIÓN	RESUMEN	RECOMENDACIÓN
	del modelo de gobierno de proyectos y su aplicación operativa. Esta situación refleja debilidades en la gestión y control de permisos, lo que podría generar riesgos de accesos no autorizados y afectar la confidencialidad, integridad y disponibilidad de la información, impactando la efectividad del control de autenticación y la gobernanza de la seguridad de la información.	suficiente frente al riesgo de manipulación o alteración no autorizada de la información y así realizar depuraciones periódicas oportunas sobre los permisos otorgados. • Considerar la actualización del Manual indicado para incorporar las mejores prácticas operativas consideradas para la gestión de proyectos, de manera que se mantenga la alineación entre la documentación institucional, la operación efectiva y los controles establecidos en el MSPI para salvaguardar los activos de información.
S.E. No. 4 **Control A.7.6 – Trabajar en áreas seguras**	Durante la revisión del control A.7.6 Trabajar en áreas seguras, se evidenció que la entidad cuenta con lineamientos institucionales y formatos definidos para la recopilación de información de inmuebles y el registro de solicitudes de reparaciones locativas, como apoyo al seguimiento de las condiciones de infraestructura de las sedes institucionales. Así mismo, se evidenció que el GIT Gestión de Bienes y servicios realiza actividades de seguimiento a las condiciones de infraestructura, mediante visitas técnicas a sedes y comunicaciones con las direcciones territoriales para atender requerimientos relacionados con reparaciones locativas y mantenimiento de instalaciones.	• Revisar y ajustar la definición del control asociado al seguimiento de las condiciones de infraestructura de las sedes institucionales, con el fin de asegurar la coherencia entre la descripción del control establecida en la matriz de riesgos, las actividades definidas en el plan de tratamiento del riesgo y las prácticas operativas realizadas por el proceso. • Así mismo, se recomienda fortalecer el registro de las actividades de verificación y seguimiento a las condiciones de

TIPO DE OBSERVACIÓN	RESUMEN	RECOMENDACIÓN
	No obstante, existen oportunidades de mejora en la trazabilidad y estandarización de los registros del control, debido a que no se utilizan los formatos institucionales definidos en todas las aplicaciones del control y se presentan inconsistencias entre los instrumentos que orientan su ejecución. Esta situación podría dificultar la verificación del control y afectar la identificación oportuna de riesgos asociados a la seguridad física, impactando la disponibilidad y protección de los activos de información.	infraestructura, promoviendo el uso de los formatos institucionales definidos para la recopilación de información de inmuebles y el registro de solicitudes de reparaciones locativas, de manera que se garantice la trazabilidad y evidencia de la ejecución del control dentro del marco del Modelo de Seguridad y Privacidad de la Información (MSPI), que soporta la protección de la confidencialidad, integridad y disponibilidad de los activos de información institucionales.
S.E. No. 5 **Gobernanza del Comité Institucional de Gestión y Desempeño en el marco de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI)**	Con el fin de verificar la ejecución de las funciones asignadas al Comité Institucional de Gestión y Desempeño, y considerando lo indicado en el numeral 3, del artículo 2 de la Resolución 0447 de 2019, la OCI revisó las actas del Comité Institucional de Gestión y Desempeño de la vigencia 2025, no obstante, no se evidenció presentación, análisis ni toma de decisiones relacionadas con la implementación, seguimiento y mejora del Modelo de Seguridad y Privacidad de la Información (MSPI). Con base en las actas del mencionado Comité no fue posible identificar el cumplimiento de las responsabilidades asignadas al Representante de la Alta Dirección para las políticas de Gobierno Digital y Seguridad Digital, en lo relacionado con la presentación de información estratégica al Comité	Incluir sistemática y periódicamente en la agenda del Comité Institucional de Gestión y Desempeño, los temas estratégicos relacionados con la implementación, seguimiento y mejora del modelo, considerando los roles y responsabilidades que corresponden a cada comité, para asegurar: • La presentación de informes por parte del Representante de la Alta Dirección sobre el estado de la seguridad de la información. • El seguimiento a la implementación del MSPI,

TIPO DE OBSERVACIÓN	RESUMEN	RECOMENDACIÓN
	para la toma de decisiones, ni la incorporación de temas asociados a seguridad de la información dentro de la agenda de dicha instancia. Si bien la entidad cuenta con el Comité de Seguridad de la Información como instancia técnica, no se evidenció articulación efectiva para la presentación de sus resultados, análisis o recomendaciones hacia el Comité Institucional de Gestión y Desempeño, como instancia de direccionamiento estratégico en el marco del MIPG. Esta situación podría generar desalineación del modelo con los objetivos institucionales, debilidades en la toma de decisiones y riesgos de incumplimiento normativo, afectando la implementación integral del MSPI.	incluyendo riesgos, incidentes, oportunidades y acciones de mejora, • La articulación formal de los resultados del Comité de Seguridad de la Información con la instancia estratégica, y • La toma de decisiones informadas que permitan alinear el MSPI con la planeación institucional.

2. CONCLUSIÓN GENERAL

De acuerdo con el trabajo de auditoría desarrollado por la Oficina de Control Interno (OCI), se evidencia que el Departamento Administrativo Nacional de Estadística (DANE) cuenta con un Modelo de Seguridad y Privacidad de la Información (MSPI) implementado en su estructura normativa, metodológica y operativa, alineado con los lineamientos definidos por el MinTIC y que se encuentra en un proceso de transición a la implementación de la Resolución 2277 de 2025, MSPI versión 5.

La Entidad dispone de instrumentos institucionales que soportan el modelo, tales como la Política de Seguridad y Privacidad de la Información, el Plan de Seguridad y Privacidad de la Información, metodología para la gestión de riesgos, inventario de activos, declaración de aplicabilidad y documentación procedimental, así como la asignación formal de roles y responsabilidades en materia de seguridad de la información. Así mismo, se evidenció la existencia de controles tecnológicos, organizacionales y procedimentales implementados, y en la muestra de controles evaluados estos se

encuentran operando de manera efectiva, contribuyendo a la mitigación de riesgos asociados a la confidencialidad, integridad y disponibilidad de la información institucional.

No obstante, se identificaron aspectos que representan oportunidades de mejora para fortalecer la madurez del modelo, particularmente en aspectos relacionados con: la actualización de las fuentes de información utilizadas para la planificación del MSPI, tales como el análisis de contexto institucional, la matriz de partes interesadas y la declaración de aplicabilidad, consistencia y actualización del inventario de activos de información frente a los controles definidos en la declaración de aplicabilidad, gestión y revisión de accesos a repositorios de información en proyectos TIC, trazabilidad documental de algunos controles asociados a la seguridad física e infraestructura, alineación entre la documentación institucional y las prácticas operativas en la ejecución de controles y gobernanza estratégica del MSPI a través del Comité Institucional de Gestión y Desempeño.

En este contexto, se concluye que el MSPI del DANE presenta un nivel de implementación significativo, evidenciado en el cumplimiento del 75% de los requisitos evaluados, así como en la existencia de controles que operan en la práctica, por lo que la Oficina de Control Interno (OCI) recomienda formular acciones de mejora sobre el 25% de requisitos adicionales verificados que conlleven al fortalecimiento del modelo.

Cordialmente,

YULY DAYAN QUICENO RUSSI

Firmado digitalmente por YULY DAYAN QUICENO RUSSI
Fecha: 2026.04.10 11:47:21 -05'00'

YULY DAYAN QUICENO RUSSI
Jefe Oficina de Control Interno de Gestión
Proyectó: JCPS –Auditor Líder
CGAM – Auditor Apoyo
Aprobó: YDQR – Jefe OCI