RESUMEN EJECUTIVO AUDITORÍA INTERNA DE GESTIÓN

INFORMACIÓN DE LA AUDITORÍA	
Título de la Auditoría	Auditoría Interna del Modelo de Seguridad y Privacidad de La Información - MSPI
Aspecto Evaluable (Unidad Auditable, Proceso, Dependencia):	Proceso Direccionamiento Estratégico (DES); Comunicaciones (COM); Producción Estadística (PES); Gestión jurídica (GJU); Proceso de Gestión Contractual (GCO); Gestión de Bienes y Servicios (GBS); Gestión Financiera (GFI); Gestión del Talento Humano (GTH), Gestión tecnológica (GTE); Gestión de Información y Documental (GID); Gestión de Proveedores de datos (GPD).
Líder de Proceso / Jefe(s) Dependencia(s):	Direccionamiento estratégico (DES) y Oficial de seguridad de la información: Claudia Díaz Hernández - Jefe Oficina Asesora de Planeación Comunicación: Gladys Adriana Quintero Hernández - Directora técnica DICE (E) Gestión Jurídica: Federico Alfonso Núñez García: - Jefe Oficina Asesora Jurídica Proceso Producción Estadística (PES): Leonardo Trujillo Oyola Subdirector Proceso de Gestión Contractual (GCO): María Fernanda De la Ossa Archila - Diana Milena Pinzón Pulido Gestión de Bienes y Servicios (GBS): María Fernanda De la Ossa Archila – Jaqueline Soto Quiroz Gestión del Talento Humano (GTH): María Fernanda De la Ossa Archila – Laura Evelyn Arroyo España. Gestión Financiera (GFI): María Fernanda De la Ossa Archila – Leonard Páez Ramírez Gestión Tecnológica (GTE): Luis Martin Barrera Pino Gestión de Información y Documental (GID): María Fernanda De la Ossa Archila y Luis Martin Barrera Pino Gestión de Proveedores de Datos (GPD): Julieth Alejandra Solano Villa - Directora técnica DIRPEN Secretaría General (SG) y Oficial de protección de datos personales: María Fernanda De la Ossa Archila Secretaría General
Objetivos de la Auditoría: (General y específicos)	General: Evaluar el nivel de implementación del Modelo de Seguridad y Privacidad de la Información en el DANE – FONDANE Específicos: 1) Evaluar la identificación de contexto y sus partes interesadas con sus necesidades y expectativas en términos de seguridad y privacidad de la información. 2) Revisar los límites de aplicabilidad del MSPI

INFORMACIÓN DE LA AUDITORÍA	
	3) Revisar el liderazgo y compromiso de la alta dirección con el MSPI y la política de seguridad de la información 4) Revisión de activos de información y metodología de gestión de riesgos de seguridad de la información y protección de datos personales y sus planes de tratamiento 5) Declaración de aplicabilidad 6) Revisión de competencias, toma de conciencia y comunicaciones 7) Verificar la implementación de los controles declarados en la declaración de aplicabilidad (Anexo A ISO 27001:2013) 8) Revisar planes de mejoramiento de auditorías anteriores relacionadas con seguridad
Alcance de la Auditoría:	Se auditarán las actividades que se desarrollan para cumplir con los requisitos del Modelo de Seguridad y Privacidad de la Información en el DANE central. Para el periodo comprendido entre el 1 de enero 2019 a 30 de Septiembre del 2022. Se auditarán los riesgos de seguridad de la información de todos los procesos participantes en la auditoría. La Auditoria será Presencial y Virtual en DANE CAN.
Criterios de la Auditoría:	GENERALES • Constitución Política de Colombia. Artículos 15, 209 y 269. • Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. • Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado. • Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. • Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos. • Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. • Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. • Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26. • Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. • Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

INFORMACIÓN DE LA AUDITORÍA	
	• Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital". • CONPES 3854 de 2016. Política Nacional de Seguridad digital. • Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos. • Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. • Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones. • Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital RESOLUCIÓN NUMERO 746 DE 2022 por la cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales establecidos en la Resolución 500 de 2020. PROCESO DIRECCIONAMIENTO ESTRATÉGICO (DES): MSPI / ISO 27001:2013 5.2, 6.1, 6.2, 7.5, 8.1, 8.2, 8.3, 9.1, 10.2, Anexo A.5 SECRETARÍA GENERAL Requisitos Ley 1581 de 2012 y decretos reglamentarios. PROCESO GESTIÓN DE TECNOLOGIA (GTE): MSPI / ISO 27001:2013 Declaración de Aplicabilidad: Anexo A.5 Políticas de Seguridad de la Información / A.6.1.5 Dispositivos móviles /A.10 Criptografía / A.11 Seguridad física y del entorno / A13 Seguridad en las comunicaciones / A.8 Gestión de Activos / A.9 Control de acceso lógico / A.11.2 Seguridad en los equipos / A12 Seguridad en las operaciones / A.14 Adquisición, desarrollo y mantenimiento de sistemas / A.15 Seguridad con proveedores/ A.16 Gestión de incidentes /A.17 Continuidad del negocio PROCESO GESTIÓN JURÍDICA (OAJ):

INFORMACIÓN DE LA AUDITORÍA	
	Declaración de Aplicabilidad: A.18 Cumplimiento GESTIÓN DE PROVEEDORES DE DATOS (GPD): MSPI / ISO 27001:2013 Declaración de Aplicabilidad: A.8 Gestión de Activos / A.15 Relaciones con Proveedores Ley 1581 de 2012: Autorizaciones, Gestión de Encargados de Tratamiento de Datos Personales COMUNICACIONES (COM): MSPI/ ISO 27001:2013 7.4 Comunicaciones Requisitos Ley 1581 de 2012 PRODUCCIÓN ESTADÍSTICA (PES) MSPI/ISO 27001:2013 6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES MSPI /ISO 27001:2013 Declaración de aplicabilidad: A.18 CUMPLIMIENTO PROCESO GESTIÓN CONTRACTUAL (GCO): MSPI / ISO 27001:2013Declaración de Aplicabilidad: A.15 Seguridad con proveedores Requisitos Ley 1581 de 2012: Autorizaciones PROCESO GESTIÓN DE BIENES Y SERVICIOS (GBS): MSPI / ISO 27001:2013 Declaración de Aplicabilidad: Anexo A.11 Seguridad Física Requisitos de la Ley 1581 de 2012 PROCESO GESTIÓN DEL TALENTO HUMANO (GTH): MSPI / ISO 27001:2013 5.3 Roles y responsabilidades de seguridad, 7.2 Competencias, 7.3 Toma de conciencia, 7.4 Comunicación, Declaración de Aplicabilidad: A.6 Organización de la Seguridad de la Información, A.7 Seguridad en el Talento Humano Requisitos de la Ley 1581 de 2012 Gestión de Información y Documental (GID): MSPI / ISO 27001:2013 - A8 Gestión de Activos de Información, A11 Seguridad Física y del entorno Los demás relacionados con las unidades auditables
Jefe Oficina Control Interno:	Duvy Johanna Plazas Socha
Auditor líder:	Jorge Luis Vargas Buitrago
Equipo auditor:	Diana Carolina Orjuela Moreno Javier Alberto Rubiano Quiroga

Reunión de apertura			**Ejecución de la auditoria**						**Reunión de cierre**		
			Desde			**Hasta**					
DD	**MM**	**AAAA**	**DD**	**MM**	**AAAA**	**DD**	**MM**	**AAAA**	**DD**	**MM**	**AAAA**
01	11	2022	02	11	2022	09	12	2022	28	12	2022

1. FORTALEZAS

- Se evidenció una eficaz gestión de los dispositivos móviles de la Entidad. Están inventariados, se tiene registro de dispositivos entregados, devueltos y dados de baja e implementan medidas de seguridad adecuadas (Criterio: MSPI (AD.2.2.1) - ISO 27001 (A.6.2.1): Se deberían adoptar medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.)

- Se evidenció que el área de comunicaciones implementa lineamientos y procedimientos adecuados para apoyar las a las necesidades internas y externas pertinentes al Modelo de Seguridad y Privacidad de la Información, que incluyen: el contenido de las comunicaciones, cuándo, a quién y quién debe comunicar; y los procesos para llevar a cabo la comunicación. ***(criterio: MSPI - ISO 27001 (7.2)*** *La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información.)*

- Se evidenció la implementación de la solución FortiDDoS (contra ataques de denegación de servicio), que permite tener visibilidad granular del tráfico de red en tiempo real y protección automática frente a los ataques DDoS dirigidos hacia la Entidad y así evitar pérdidas de disponibilidad en los servicios y sistemas de información**. (criterio: MSPI - ISO 27001 (A.13.1.1**) *Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.)*

- Se evidenció la existencia de un procedimiento de control de cambios a sistemas de información e infraestructura tecnológica que busca para analizar, aprobar o rechazar los cambios de los diferentes componentes de la infraestructura del Centro de Computo del DANE. Esto garantiza que los cambios que se hagan sean controlados y no haya problemas de disponibilidad en la plataforma tecnológica. Este procedimiento está soportado en el documento GTE-040-PDT-005 PROCEDIMIENTO PARA LA GESTIÓN DE CAMBIOS DE TI, VERSIÓN, FECHA: 28/Jun/2022

2. RESUMEN DE LOS HALLAZGOS (solo el título de la novedad encontrada)

No.	Descripción de la Situación	*criterio*
H1	Se evidenció que en el documento Contexto Institucional aportado por el proceso de direccionamiento estratégico, el análisis de contexto no tiene en cuenta los aspectos relacionados con seguridad y privacidad de la información. Por lo tanto, no se identifican las amenazas, oportunidades, fortalezas y debilidades que estén	***MSPI – ISO 27001 (4.1)*** *La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la*

No.	Descripción de la Situación	*criterio*
	alineadas con el MSPI. ***Respuesta Auditor***: Una vez revisada la respuesta por parte de la Oficina de Planeación, se hizo la revisión de los aspectos de seguridad y privacidad de ambos contextos, se debe complementar el contexto externo, ya que no tiene en cuenta los aspectos legales, políticos, sociales y ambientales que puedan tener un impacto en la seguridad de la información. Por lo anterior el Hallazgo No. 1 se mantiene.	*información.*
H2	Se evidenció que en el documento Contexto Institucional aportado por el proceso de direccionamiento estratégico, no se identifican las necesidades y expectativas de las partes interesadas externas e internas en perspectiva de seguridad y privacidad de la información.	***MSPI – ISO 27001(4.2)*** *La organización debe determinar:* *a) las partes interesadas que son pertinentes al sistema de gestión de la seguridad de la información; y* *b) los requisitos de estas partes interesadas pertinentes a seguridad de la información.*
H3	De acuerdo por las evidencias aportadas, se observó que el Modelo de Seguridad y Privacidad de la Información no tiene un alcance establecido que determine los límites de la implementación.	***MSPI – ISO 27001(4.3)*** *La organización debe determinar los límites y la aplicabilidad del Modelo de seguridad y privacidad de la información para establecer su alcance.*
H4	Revisando el documento de la Declaración de Aplicabilidad, se observó que no está formalizada, aprobada y publicada en Isolución. Esta Declaración de Aplicabilidad debe contener los controles necesarios para la gestión de riesgos de seguridad y privacidad de la información.	***MSPI – ISO 27001(6.1.3)*** *La Entidad debe producir una declaración de aplicabilidad que contenga los controles necesarios y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del MSPI.*
H6	Revisando la información aportada por el Área de Gestión de Talento Humano se pudo observar que no están establecidas las competencias necesarias para el rol del Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales y perfiles asociados a actividades de seguridad de la información. Sin embargo, en el contrato aportado por la OSIS de la colaboradora que apoya los temas de seguridad de la información si se evidenció la exigencia de las competencias para cumplir con sus funciones.	***MSPI – ISO 27001(7.2)*** *La organización debe:* *a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información, y* *b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;* *c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones*

No.	Descripción de la Situación	*criterio*
		tomadas; y *d) conservar la información documentada apropiada, como evidencia de la competencia.*
H7	A partir de la muestra tomada en la mesa de trabajo con la Oficina de planeación, se evidenció la implementación de una metodología de gestión de riesgos alineada con la guía de administración de riesgos del DAFP versión 4.0. Sin embargo, al momento de solicitar la evaluación de riesgos posterior a la implementación de controles, no se pudo evidenciar la valoración periódica de los riesgos de seguridad de la información ni los planes de tratamiento de riesgo.	***MSPI – ISO 27001(8.2 y 8.3) – Política de Administración de Riesgos numeral 3.4.2 Primera línea de defensa:*** *La organización debe llevar a cabo valoraciones de riesgos de la seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en el numeral 6.1.2* *a). Formular, ejecutar, hacer seguimiento y determinar la efectividad de los planes de tratamiento de los riesgos, conforme con los niveles de aceptación del riesgo.* *b) La organización debe conservar información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información.*
H8	Revisando la documentación aportada por la oficina de planeación y la oficina de sistemas, se evidenció que la Entidad no cuenta con indicadores para medir el cumplimiento de los objetivos del MSPI. Tampoco se define quien debe llevar a cabo el seguimiento y la medición de los resultados de la implementación de los controles.	***MSPI – ISO 27001(9.1)*** *La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.*
H9	Revisando el documento aportado por la Oficina de Sistemas llamado manual *de políticas de seguridad y privacidad de la información, se evidenció* que el documento no está terminado, aprobado, formalizado, socializado y publicado en la plataforma Isolución.	***MSPI(AD.2.2.1) – ISO 27001(A.5.1.1)*** *Desde el más bajo nivel, la política de la seguridad de la información debería estar apoyada en políticas específicas por temas, que además exigen la implementación de controles de seguridad de la información y están típicamente estructuradas para tener en cuenta las necesidades de algunos grupos objetivo dentro de una organización, o para tener en cuenta temas determinados*
H10	Revisando el formato aportado por la Secretaría General llamado *GTH-060-PDT-001-f-014 Autorización para el tratamiento de datos personales*, se evidenció que, si bien está publicado en Isolución, este no ha sido	***LEY 1581 de 2012 – Decreto 1377 de 2013.*** *Artículo 5. Autorización. El Responsable del Tratamiento deberá adoptar*

No.	Descripción de la Situación	*criterio*
	implementado. Esto se pudo observar al momento de solicitar las pruebas de las autorizaciones recolectadas las cuales no fueron aportadas. Lo anterior demuestra que la Entidad no cuenta con la autorización requerida para el tratamiento de los datos personales de colaboradores, proveedores, visitantes, entre otros.	*procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados, así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento.*
H12	Según la documentación aportada por la Oficina de Sistemas, se evidenció que la Entidad no cuenta con una política de uso aceptable de los activos de información aprobada, publicada que incluya los roles, responsabilidades y reglas en el uso seguro de activos de información.	***MSPI (AD.4.1.3) – ISO 27001 (A.8.1.3)*** *Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.*
H13	Al momento de solicitar el etiquetado de los activos de información según su clasificación a la oficina de planeación, se evidenció que no existe un esquema de etiquetado de activos de información que permita identificar la clasificación de estos, según los criterios establecidos en la metodología de levantamiento de activos de información de la Entidad y la Ley 1712 de 2014.	***MSPI (AD.4.2.2) – ISO 27001 (A.8.2.2)*** *Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de* *Información adoptada por la organización.*
H14	Revisando la documentación aportada por la oficina de planeación, se evidenció que no existe un documento formalizado, publicado y socializado, que contenga los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación (etiquetado)	***MSPI (AD.4.2.3) – ISO 27001 (A.8.2.3)*** *Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.*
H15	Según la documentación aportada por la oficina de Sistemas y la oficina de planeación, se evidenció que la Entidad no cuenta con una política de control de acceso formalizada donde se especifiquen las reglas para el acceso a máquinas, aplicativos, bases de datos, servicios y redes según la necesidad de acceso según roles y responsabilidades de los usuarios.	***MSPI (T.1.1.1) – ISO 27001 (A.9.1.1)*** *Se debería establecer, documentar y revisar una política de control de acceso con base en los* *requisitos del negocio y de seguridad de la información*
H16	Dentro del Formato Acuerdo de Confidencialidad con código GTH-060-PDT-001-f-009 aportado por el área de Gestión Humana, no se pudo identificar las exigencias	***MSPI (T.1.4.2) – ISO 27001 (A.9.4.2)*** *Se debería exigir a los usuarios que*

No.	Descripción de la Situación	*criterio*
	para guardar la reserva de la información de autenticación a los recursos de la plataforma tecnológica (usuarios y contraseñas, tokens)	*cumplan las prácticas de la organización para el uso de información secreta para la autenticación.*
H17	Pese a que se implementan controles de cifrado a nivel de almacenamiento y transmisión de información, al revisar el documento aportado por la Oficina de Sistemas llamado *manual de políticas de seguridad y privacidad de la información*, no se evidenció la existencia de una política de controles criptográficos que contenga lineamientos sobre los niveles de protección requerida, algoritmos de cifrado que se deben utilizar, como gestionar las llaves de cifrado y cuáles son los deberes del responsable de esta implementación.	***MSPI (T.2.1.1 - T.2.1.2) – ISO 27001 (A.10.1.1 - 10.1.2)*** • *La organización debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.* • *Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.*
H18	Revisando el documento aportado por la Oficina de Sistemas llamado *Política de Desarrollo Seguro De Software*, se observó que contiene lineamientos para implementar principios de construcción de sistemas seguros. Sin embargo, dicho documento no está aprobado, publicado ni socializado.	***MSPI (T.6.2.1 - T.6.2.5) – ISO 27001 (A.14.2.1 - A.14.2.5)*** ***Se debe establecer y aplicar*** *reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.*
H19	A partir de la muestra tomada en las mesas de trabajo con la oficina de sistemas, se evidenció que en el ambiente de desarrollo no se verifican los mínimos de seguridad de los equipos de cómputo personales de los desarrolladores. El equipo de la muestra no contaba con herramienta antimalware a lo cual el ingeniero desarrollador manifestó que no era necesaria porque el equipo era un MAC. Con lo anterior, se concluye que no se está controlando adecuadamente los entornos de desarrollo de software.	***MSPI (T.6.2.6) – ISO 27001 (A.14.2.6)*** *Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.*
H20	De acuerdo con la entrevista realizada en mesa de trabajo a la Oficina de Sistemas respecto a los procedimientos de desarrollo, pruebas y puesta en producción de aplicativos, se evidenció que los sistemas de información no son sometidos a pruebas de seguridad antes de salir a producción. Es importante poder detectar las brechas de seguridad a nivel de código, plataformas de operación y sistemas operativos para remediarlas antes de salir a producción.	***MSPI (T.6.2.8) – ISO 27001 (A.14.2.8)*** *En el caso que se realicen desarrollos nuevos o actualizaciones en las aplicaciones productivas, se debe llevar a cabo pruebas de seguridad de la información antes de salir al ambiente productivo.*

No.	Descripción de la Situación	*criterio*
H21	De acuerdo con la documentación aportada por la oficina de planeación y la oficina de sistemas respecto a las relaciones con proveedores, no se evidenció la existencia de una política de seguridad en la relación con proveedores aprobada, formalizada y publicada, que contenga las reglas y los lineamientos de seguridad en el uso seguro de recursos tecnológicos y activos de información de la entidad y donde se les obligue cumplir con las políticas de seguridad del DANE. Es importante que la exigencia del cumplimiento de esta política quede dentro de los términos del contrato con terceros que tengan acceso a los activos de información.	***MSPI (AD.7.1) – ISO 27001 (A.15.1- A.15.1.1- A.15.1.2)*** *La organización debe asegurar la protección de los activos de información que sean accesibles para los proveedores. Adicionalmente, se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda acceder, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización*
H23	Si bien la oficina de sistemas ha hecho un esfuerzo por levantar la información necesaria para construir el Análisis de Impacto del Negocio (BIA) para poder identificar los activos críticos que necesitan continuidad en su operación, se pudo evidenciar la construcción de un documento del BIA, sin embargo, no está aprobado, formalizado y publicado para su implementación. Lo anterior da como resultado la no existencia de un plan de continuidad del negocio que contenga la estructura organizacional de gestión adecuada, el personal vital para la continuidad de la operación, lineamientos para la ejecución de pruebas de respuesta y recuperación y los controles de seguridad en contingencia.	***MSPI (AD.5.1.1- AD.5.1.2 -AD.5.1.3) – ISO 27001 (A.17.1.1 A.17.1.2 - A.17.1.3)*** *La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.*
H24	En mesa de trabajo con la Oficina de sistemas, se evidenció que la Entidad no cuenta con arquitecturas redundantes de sus sistemas críticos alojados en el centro de cómputo principal en otro centro alterno. Existen algunas redundancias dentro del mismo centro de cómputo principal y otros servicios que están en nube, sin embargo, no está alineado con los criterios del MSPI y no garantiza disponibilidad de los sistemas críticos en caso de un incidente.	***MSPI (AD.5.2.1) – ISO 27001 (A.17.2.1)*** *Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.*
H26	En lo relacionado con el Programa de Protección de Datos Personales se evidenció lo siguiente: - No cuentan con autorizaciones de tratamiento de datos personales - El aviso de privacidad de videovigilancia no cumple con los requerimientos de la Ley 1581 de 2012 y el Decreto 1317 de 2013	***MSPI (AD.6.1.4) – ISO 27001*** *(A.18.1.4)* *Ley 1581 de 2012* *Decreto 1377 de 2013* *Decreto único reglamentario 1074 de 2015* *Resolución 500 de 2021, MINTIC* *Resolución 746 de 2022, MINTIC*

No.	Descripción de la Situación	*criterio*
	- No se identifican encargados de tratamiento ni se hacen contratos de transmisión de datos personales. - No se identifican riesgos asociados al tratamiento de datos personales - No se evidenció la existencia de una manual interno de políticas y procedimientos para el tratamiento de datos personales - No se tiene claridad si la Entidad realiza transferencias internacionales de datos y en caso de que se hiciera, no se tienen los mecanismos para hacerlas dentro de los términos de la ley - No se evidenció el reporte del incidente de seguridad a la Superintendencia de Industria y Comercio	

3. CONCLUCIONES

- La implementación del Modelo de Seguridad y Privacidad está en un nivel de madurez Medio – Alto. Es claro el esfuerzo que han hecho las distintas áreas involucradas en la implementación del modelo, a mediano plazo pueden llegar a un nivel de madurez Alto.
- La entidad realiza la planificación, liderazgo, implementación y control de las estrategias de gestión, uso y apropiación de las tecnologías de la información y comunicaciones, a través de la implementación, facilitando la gestión del sistema de gestión, enmarcados en la rigurosidad de los requisitos del Modelo de Seguridad y Privacidad de la Información - MSPI.
- Se evidencia el liderazgo y compromiso de la alta dirección con el Modelo de Seguridad y Privacidad de la Información - MSPI desde el establecimiento e implementación de la política y objetivos del modelo, con el uso del enfoque por procesos y con la asignación de los recursos necesarios para la implementación.
- La Entidad evidencia cumplimiento de los requerimientos para la administración de los recursos de infraestructura y físicos, que garanticen la operación del DANE, con el cumplimiento de los programas de mantenimiento preventivo y la optimización en la distribución de las áreas con el control de seguridad de la información.
- La Entidad tuvo en cuenta las lecciones aprendidas del incidente de seguridad para mejorar sustancialmente sus controles de ciberseguridad.

4. RECOMENDACIÓNES (dirigidos a atacar la causa encontrada por el auditor)

- Se debe finalizar la construcción del Manual de Políticas de Seguridad, formalizarlo, publicarlo y socializarlo con el fin de que los colaboradores conozcan los deberes, prohibiciones y derechos en cuanto al manejo de los activos de información.

- Construir un documento que permita tener a la mano los datos de contacto dentro de las autoridades relacionadas con los temas de seguridad de la información y los grupos de interés especial
- Propender por recolectar la autorización del tratamiento de datos personales desde el momento que inicia el proceso precontractual con los aspirantes al talento humano, con el fin de cumplir los requisitos de la Ley 1581 de 2012.
- Se deben determinar claramente las competencias de aquellos perfiles que vayan a tener un rol de seguridad de la información al interior de la Entidad.
- Establecer controles de seguridad por defecto en los proyectos, independientemente de su naturaleza, con el fin de mitigar riesgos, garantizar un correcto manejo de los activos de información y cumplir con las políticas de seguridad de la información.
- Establecer una política de teletrabajo que pueda complementar los controles para las conexiones remotas que se aplican actualmente cuando los colaboradores lo solicitan.
- Incluir dentro de las cláusulas de confidencialidad la obligación de guardar reserva de la información de autenticación (usuarios y contraseñas).
- Establecer causales de incumplimiento de políticas de seguridad y privacidad que serán motivo de apertura de procesos disciplinarios para los funcionarios o incumplimientos contractuales para los contratistas.
- Es conveniente realizar evaluaciones de conocimiento de las capacitaciones dictadas en Seguridad de la Información para poder tomar acciones para reforzar el tema en las personas que así lo requiera.
- Definir una política de uso aceptable de los activos de información donde se indiquen las reglas para el uso seguro de los recursos tecnológicos e información documentada a la que tienen acceso los colaboradores. Esta política debe ser socializada a toda la Entidad.
- Realizar el etiquetado de los activos de información según la clasificación obtenida en el inventario y crear un procedimiento del manejo de los activos según su criticidad.
- Crear procedimientos de disposición segura de medios de almacenamiento con el fin de hacer borrado seguro de la información en medios removibles o equipos de cómputo.
- Establecer, aprobar y publicar una política de control de acceso lógico que determine las reglas de acceso a los activos de información según las necesidades del negocio.
- Realizar periódicamente depuración de usuarios en el Directorio Activo y las aplicaciones con el fin de evitar accesos no autorizados después de la terminación del contrato laboral o de prestación de servicios.
- Establecer una política de controles criptográficos donde se definan los criterios que se deben tener en cuenta para toma de la decisión de cifrar información, los algoritmos que se deben usar y los roles y responsabilidades de este proceso.
- Se debe hacer una reorganización al cableado estructurado eléctrico y de datos con el fin de evitar interceptaciones, interferencias o daños en el cableado.
- Es considerable detallar el tiempo de resolución de vulnerabilidades de acuerdo con el CVSS (Score de la vulnerabilidad) para un mejor seguimiento y solución.

- Garantizar los mínimos de seguridad que deben tener los computadores personales (sistema operativo licenciado y actualizado, herramienta antimalware actualizada, software legal instalado en la máquina, entre otros) al momento de autorizar su conexión a la red interna de la Entidad.
- Definir una política de seguridad en la relación con proveedores con el fin de establecer mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso, conocimiento o relación con los servicios o productos en el marco del contrato cumpla con las políticas, normas y procedimientos de seguridad de la Información.
- Se deben establecer procedimientos de análisis de seguridad en las aplicaciones antes de salir a producción con el fin de evitar la materialización de amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información gestionada dentro de la plataforma tecnológica de la Entidad.
- Seguir trabajando en el levantamiento del BIA con el fin de hacer una buena planeación de la continuidad del negocio y conocer los recursos financieros necesarios para tener replicación de las infraestructuras críticas.
- Continuar con la implementación del programa de protección de datos personales para evitar sanciones por incumplimiento de la Ley 1581 de 2012.

Nombre Completo	**Responsabilidad** (cargo)	**Firma**
Duvy Johanna Plazas Socha	Jefe Oficina de Control Interno	**(FIRMADO ELECTRONICAMENTE)** DUVY JOHANNA PLAZAS SOCHA 52.834.634
Jorge Luis Vargas Buitrago	Auditor	**(FIRMADO ELECTRONICAMENTE)** JORGE LUIS VARGAS BUITRAGO 13.861.633
Javier Alberto Rubiano Quiroga	Auditor	**(FIRMADO ELECTRONICAMENTE)** JAVIER ALBERTO RUBIANO QUIROGA 79.180.836

1. SOPORTES Y PAPELES DE TRABAJO

No	N°. Del Hallazgo u Observación	Nombre del Documento	Ubicación Física o Magnético	Área Responsable	Responsable
1	H1	Documento CONTEXTO INSTITUCIONAL DE MAYO DE 2021	EVIDENCIAS	OPLAN (Oficina de Planeación)	OPLAN (Oficina de Planeación)
2	H2	Documento CONTEXTO INSTITUCIONAL DE MAYO DE 2021		OPLAN	OPLAN
3	H3	Documentos Política General De Seguridad Y Privacidad De La Información Versión 2 y el Manual de Políticas de Seguridad y Privacidad de la Información (en construcción).		OPLAN	OPLAN

1. SOPORTES Y PAPELES DE TRABAJO

No	N°. Del Hallazgo u Observación	Nombre del Documento	Ubicación Física o Magnético	Área Responsable	Responsable
4	H4	Documento13. 30-11-2020-Declaración de aplicabilidad-DANE-FONDANE		OPLAN	OPLAN
5	H5	El Oficial de Seguridad de la Información en la mesa de trabajo con el proceso direccionamiento estratégico, el 4 de noviembre del 2022.		OPLAN	OPLAN
6	H6	Manual de funciones (descargarla), Contrato Andrea	EVIDENCIAS	GTH (Gestión de Talento Humano- Secretaría General)	GTH (Gestión de Talento Humano- Secretaría General)
7	H7	Documento politica-administracion-riesgos-DANE-FONDANE-nov20		OPLAN	OPLAN
8	H8	El Oficial de Seguridad de la Información en la mesa de trabajo con el proceso direccionamiento estratégico, el 4 de noviembre del 2022.		OPLAN	OPLAN
9	H9	Manual de Políticas de Seguridad y Privacidad de la Información (en construcción).		OSIS (Oficina de Sistemas)	OSIS (Oficina de Sistemas)
10	H10	Formato Autorización de Recolección y Tratamiento de Datos Personales para funcionarios del DANE Código: GTH-060-PDT-001-f-014 Versión: 01		GTH	GTH
11	H11	El Oficial de Seguridad de la Información en la mesa de trabajo con el proceso direccionamiento estratégico, el 9 de noviembre del 2022.		OPLAN	OPLAN
12	H12	Manual de Políticas de Seguridad y Privacidad de la Información (en construcción).		OSIS	OSIS
13	H13	El Oficial de Seguridad de la Información en la mesa de trabajo con el proceso direccionamiento estratégico, el 4 de noviembre del 2022		OPLAN	OPLAN
14	H14	El Oficial de Seguridad de la Información en la mesa de trabajo con el proceso direccionamiento estratégico, el 4 de noviembre del 2022		OPLAN	OPLAN
15	H15	El Oficial de Seguridad de la Información y la Oficina de Sistemas en la mesa de trabajo con el proceso direccionamiento estratégico, el 4 de noviembre y el 11 de noviembre del 2022 respectivamente.		OPLAN	OPLAN
16	H16	Formato Acuerdo de Confidencialidad y No Divulgación para Servidores Públicos Código: GTH-060-PDT-001-f-009 Versión: 02		GTH	GTH
17	H17	Manual de Políticas de Seguridad y Privacidad de la Información (en construcción).	EVIDENCIAS	OSIS	OSIS
18	H18	Documento POLÍTICA DE DESARROLLO SEGURODE SOFTWARE noviembre de 2019		OSIS	OSIS
19	H19	La Oficina de Sistemas en la mesa de trabajo del 23 de noviembre del 2022.		OSIS	OSIS
20	H20	La Oficina de Sistemas en la mesa de trabajo del 23 de noviembre del 2022.		OSIS	OSIS

1. SOPORTES Y PAPELES DE TRABAJO

No	N°. Del Hallazgo u Observación	Nombre del Documento	Ubicación Física o Magnético	Área Responsable	Responsable
21	H21	Manual de Políticas de Seguridad y Privacidad de la Información (en construcción).		OPLAN OSIS	OPLAN OSIS
22	H22	La Oficina de Sistemas en la mesa de trabajo del 09 de diciembre del 2022		OPLAN OSIS	OPLAN OSIS
23	H23	Documento ANÁLISIS DE IMPACTO AL NEGOCIO BIA 2022 (Análisis BIA DANE Sep_2022.docx) Ficha BIA_ Dirección de Recolección y Acopio - GIT Encuestas a personas e instituciones		OPLAN OSIS	OPLAN OSIS
24	H24	La Oficina de Sistemas en la mesa de trabajo del 09 de diciembre del 2022		OSIS	OSIS
25	H25	Mesa de trabajo del 09 de diciembre del 2022		OPLAN	OPLAN
26	H26	La Secretaría General en la mesa de trabajo del 02 de noviembre del 2022		SECRETARIA GENERAL	SECRETARIA GENERAL
NOTA: Los soportes y papeles de trabajo son las evidencias que se obtienen dentro del proceso auditor con el fin de Fundamentar Razonablemente los hallazgos, observaciones y recomendaciones. Estos reposan en la Oficina de Control Internos (OCI) o en la dependencia objeto de auditoría, evaluación o seguimiento. Las evidencias se anexan al Informe si se considera necesario. Los papeles de trabajo y soportes son documentos públicos.					