

INFORME DEFINITIVO AUDITORÍA INTERNA DE GESTIÓN

INFORMACIÓN DE LA AUDITORÍA	
Título de la Auditoría	Auditoría Interna al Modelo de Seguridad y Privacidad de la Información - MSPI en el DANE - FONDANE
Aspecto Evaluable Unidad Auditable:	Proceso de Gestión Contractual (GCO); Gestión del Talento Humano (GTH); Gestión Tecnológica (GTE); Secretaría General; Oficina Asesora de Planeación
Líder de Proceso / Jefe(s) Dependencia(s):	Proceso Gestión Contractual (GCO): Diana Milena Pinzón Pulido - Edna Patricia Rangel Barragán Gestión Talento Humano (GTH): Ana María Cardona Gonzalez – Edna Patricia Rangel Barragán Gestión Tecnológica (GTE): Luis Martin Barrera Pino Secretaría General (SG): Oficial de protección de datos personales - Edna Patricia Rangel Barragan Oficina Asesora de Planeación: Oficial de Seguridad de la Información - Claudia Díaz Hernández
Objetivos de la Auditoría: (General y específicos)	General: Evaluar la identificación y estado de avance de los planes de mejoramiento de la auditoría al Modelo de Seguridad y Privacidad de la Información en el DANE - FONDANE realizada en el año 2022. 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. 3) Revisión de la Declaración de aplicabilidad. 4) Revisión de competencias del SGSI. 5) Revisión de competencias, tomade conciencia y comunicaciones 6) Revisión del plan de tratamiento de riesgos 7) Revisión de medición de indicadores del SGSI 8) Verificación de aprobación del Manual de Políticas de Seguridad de la Información 9) Revisión de estrategia de recolección de autorizaciones de datos personales 10) Estrategia de etiquetado y manejo de activos de información 11) Clausulado en términos de los contratos 12) Principios de construcción segura de sistemas de información 13) Política de seguridad en la relación con proveedores 14) Avances en la estrategia de continuidad del negocio 15) Revisión de requisitos legales vinculantes a la entidad 16) Avances en el programa de protección de datos personales. 17) Revisión de otros controles técnicos y administrativos asociados al MSPI de DANE - FONDANE.
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 15 de mayo al 30 de Octubre del 2023. De manera virtual y presencial. Se auditarán los riesgos de seguridad de la información de todos los procesos participantes en la auditoría.
Criterios de la Auditoría:	GENERALES • Constitución Política de Colombia. Artículos 15, 209 y 269.

INFORMACIÓN DE LA AUDITORÍA

- 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.
- 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.

INFORMACIÓN DE LA AUDITORÍA

- PROCESO GESTIÓN DE TECNOLOGÍA (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 CONTRACTUAL (GCO): MSPI / ISO 27001:2013 Declaración de Aplicabilidad: A.15 Seguridad con proveedores / Requisitos Ley 1581 de 2012: Autorizaciones.
- 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.
- Los demás relacionados con las unidades auditables

Jefe Oficina Control Interno: Duvy Johanna Plazas Socha**Auditor líder:** Jorge Luis Vargas Buitrago**Equipo auditor:** Jorge Luis Vargas Buitrago

Reunión de apertura			Ejecución de la auditoria						Reunión de cierre		
			Desde			Hasta					
DD	MM	AAAA	DD	MM	AAAA	DD	MM	AAAA	DD	MM	AAAA
20	11	2023	20	11	2023	11	12	2023	28	12	2023

1. ARTICULACIÓN CON MIPG

De acuerdo al alcance propuesto para esta auditoría, se identifica la articulación con la dimensión del Modelo Integrado de Planeación y Gestión: 3ª. Dimensión "Gestión con valores para resultados", en la medida en que se pone en marcha los cursos de acción o trayectorias de implementación definidas en la dimensión de Direccionamiento Estratégico y Planeación y contando con el talento humano disponible en la entidad. Su propósito es permitirle a la entidad realizar las actividades que la conduzcan a lograr los resultados propuestos y a materializar las decisiones plasmadas en su planeación institucional, en el marco de los valores del servicio público. Esta Dimensión aborda los aspectos más importantes que debe atender una organización para cumplir con las funciones y competencias que le han sido asignadas. Para ello, se tendrán en cuenta los lineamientos que se establecen en la Política que fortalece la gestión Institucional y el buen manejo de los recursos públicos, la cual dentro de ella se encuentra la "Seguridad Digital". 4ª. Dimensión "Evaluación de Resultados" en la medida en que la entidad debe conocer de manera permanente los avances en su gestión y los logros de los resultados y metas propuestas, en los tiempos y recursos previstos y si general los efectos deseados para la sociedad; permitiéndole introducir mejoras oportunas en su gestión, lo anterior en relación con su marco estratégico. 7ª. Dimensión: Control Interno, en la cual define la necesidad de establecer acciones, métodos y procedimientos de control y de gestión del riesgo, así como mecanismos para la prevención y evaluación de éste, buscando que a través del Control Interno se asegure el cumplimiento del propósito de las demás dimensiones de MIPG.

2. DESARROLLO DE LA AUDITORIA**2.1 Resultados de auditoría del MSPI**

A continuación, se relacionan los resultados de la auditoría correspondiente al seguimiento de los planes de mejoramiento de la auditoría al MSPI del año 2022.

2.1.1 Hallazgos 1 y 2 – Actividad 0140.1

Una vez revisado el documento del contexto institucional publicado en el mes de septiembre de 2023, se pudo evidenciar que en el análisis DOFA realizado para el contexto interno y externo, fueron incluidas las fortalezas, oportunidades, amenazas y debilidades asociadas a seguridad y privacidad de la información. Con esta acción se cierran los hallazgo 1 y 2 de la auditoría al MSPI vigencia 2022. Adicionalmente fueron identificadas las partes interesadas internas y externas con sus respectivas necesidades y expectativas:

<https://danegovco.sharepoint.com/sites/SistemaIntegradodeGestion-DANE/SiteAssets/Forms/AllItems.aspx?id=%2Fsites%2FSistemaIntegradodeGestion%2DDANE%2FSiteAssets%2FSitePages%2FContexto%2DEstrat%C3%A9gico%2FContexto%2DInstitucional%2D2023%2Epdf&parent=%2Fsites%2FSistemaIntegradodeGestion%2DDANE%2FSiteAssets%2FSitePages%2FContexto%2DEstrat%C3%A9gico>

Tabla 4. Componentes del análisis DOFA

Contexto Externo	Oportunidades	Son aspectos que podrían beneficiar o ser aprovechados por la entidad.
	Amenazas	Son aspectos que pueden poner en riesgo la ejecución de las actividades de la entidad y por lo tanto hay que evitar o contrarrestar para disminuir su impacto negativo.
Contexto Interno	Fortalezas	Son los aspectos positivos de la entidad que están bajo su control e influencia, tales como los conocimientos, activos, tecnología, capital financiero y humano, procesos y experiencia. Las fortalezas se alcanzan, se mantienen y se mejoran.
	Debilidades	Son aspectos en los que la entidad tiene dificultades o de los que carece y constituyen oportunidades de mejora. Son los factores negativos que en algún momento la pueden llevar a una crisis o a la materialización de riesgos; pueden surgir desde la creación de la entidad o aparecer en las diferentes etapas del desarrollo de sus actividades.

Tabla 8. Lista de Debilidades

FACTOR	DESCRIPCIÓN DE LA SITUACIÓN
Activos de seguridad de la información	Falta de estrategias para la Gestión del Conocimiento y la Información Institucional, lo que resulta en una pérdida de conocimiento y datos valiosos para la entidad
Activos de seguridad de la información	Falta de automatización contractual.
Comunicación	Dificultades en la comunicación interna y externa con los grupos de interés, usuarios y funcionarios de la entidad para informar sobre políticas, trámites, documentos, procesos y otros temas relevantes de la Entidad
Comunicación	Falta de articulación interna del DANE para realizar y enviar comunicaciones a las entidades del SEN, requerimientos internacionales y en general, tanto dentro como fuera de la entidad
Comunicación	Falta de aprovechamiento de medios digitales para la difusión de resultados y promoción de las herramientas del DANE
Comunicación	Ausencia de un lenguaje claro y sencillo al difundir los resultados de las operaciones estadísticas, dificulta su uso y comprensión

Tabla 5. Lista de Amenazas

FACTOR	DESCRIPCIÓN DE LA SITUACIÓN
Ambientales	Incumplimiento de la regulación ambiental de las entidades en nuestro entorno frente a la disposición y almacenamiento de componentes tecnológicos y/o químicos
Ambientales	Catástrofes naturales que afecten la seguridad y salud de los colaboradores de la entidad, así como, la infraestructura física y tecnológica de la misma.
Económicos y financieros	Recortes en el Presupuesto General de la Nación que afecte el funcionamiento de la misionalidad de la entidad.
Económicos y financieros	Falta de interés en las entidades y organizaciones internacionales para la generación de convenios que permitan generar capacidades en el fortalecimiento de la producción estadística de la entidad.
Económicos y financieros	Variabilidad de los precios del mercado de los productos de Tecnologías de la Información (TI) indexados a monedas extranjeras (USD)

Dado lo anterior, los hallazgos quedan cerrados.

Departamento Administrativo Nacional de Estadística

Carrera 59 No. 26 - 70, Interior CAN, Edificio DANE

Bogotá D.C. Colombia / Código postal 111321

Teléfono (601) 5978300

www.dane.gov.co / contacto@ dane.gov.co

2.1.2 Hallazgo 3 – Actividad 0140.2

Revisando las evidencias aportadas, se pudo observar que dentro del documento “Manual de Políticas complementarias de seguridad de la información” en el numeral 4 Alcance, se definen los límites de aplicabilidad del Modelo de Seguridad y Privacidad de la Información. Adicionalmente, el documento fue socializado al interior de la Entidad

MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN

4. ALCANCE

En el marco del Sistema Integrado de Gestión, el Modelo de Seguridad y Privacidad de la Información del DANE – FONDANE es aplicable para todos los procesos, servidores públicos, proveedores, contratistas, terceros, partes interesadas y quienes, en cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, transfieran, intercambien o consulten información, así como, a los entes de control o entidades que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación, buscando el cumplimiento de los requisitos pertinentes a este.

Por lo anterior, el hallazgo se da como cerrado.

2.1.3 Hallazgo 4 – Actividad 0140.3

Revisando Systema 20 no se encuentran evidencias sobre el avance de esta actividad. En el instrumento del plan de mejoramiento se registra que la actividad tiene fecha de finalización 15/12/2023, pero la declaración de aplicabilidad continúa siendo un borrador. El hallazgo se mantiene.

2.1.4 Hallazgo 6 – Actividad 0128.1

1.Una vez revisado el sitio de Tratamiento de Datos Personales de la página web de la Entidad, se pudo evidenciar que mediante Resolución 1248 del 17 de agosto de 2023 se establecen las competencias del Oficial de Protección de Datos Personales del DANE, dando cierre al hallazgo asociado a las competencias de la auditoría al MSPI del año 2022.

<https://www.dane.gov.co/files/acerca/Normatividad/resoluciones/2023/Res-GTH-1248-de-2023.pdf>

RESUELVE:		
Artículo 1º. Requisitos de formación académica y experiencia del Oficial de Protección de Datos Personales y del personal de apoyo. El Oficial de Protección de Datos Personales y el personal de apoyo que se designe para el efecto deberá cumplir con lo siguiente: Formación Académica Profesional: Título profesional de alguno de los siguientes núcleos básicos del conocimiento (NBC): - Derecho y afines - Economía. - Ingeniería Industrial y afines.		
RESOLUCIÓN 1248 DE 17 AGO 2023 Hoja No. 2		
Continuación de la Resolución "Por medio de la cual se relacionan los requisitos, competencias y experiencia para el desarrollo de las funciones del Oficial de Protección de Datos Personales y el personal designado como apoyo del Departamento Administrativo Nacional de Estadística-DANE y del Fondo Rotatorio del Departamento Administrativo Nacional de Estadística-FONDANE" - Título profesional en las disciplinas de Administración Pública o Administración de Empresas del (NBC) de Administración. - Ingeniería de Sistemas, Telemática y Afines. - Ingeniería Electrónica, Telecomunicaciones y Afines. - Comunicación Social, Periodismo y Afines. - Ciencia Política y Relaciones Internacionales. - Contaduría Pública. - Matemáticas, Estadística y Afines.		

Revisando las evidencias del plan de mejoramiento 0129, se evidencia que mediante Resolución 1452 de 2023 se establecen las competencias que debe cumplir el oficial de seguridad de la información nivel de formación académica, tiempo de experiencia y experiencia en seguridad de la información.

RESUELVE:		
Artículo 1º. Requisitos de formación académica y experiencia del Oficial de Seguridad de la información y del personal de apoyo. El Oficial de Seguridad de la información y el personal de apoyo que se designe para el efecto deberá acreditar los siguientes requisitos, según el nivel del empleo que ostente: Formación Nivel Directivo: Título profesional de alguno de los siguientes núcleos básicos del conocimiento (NBC): Administración; Arquitectura; Otros programas asociados a Bellas Artes; Biología, Microbiología y afines; Comunicación Social, Periodismo y afines; Derecho y afines; Contaduría Pública; Economía; Ingeniería de Sistemas, Telemática y afines; Matemáticas, Estadística y afines; Ingeniería Industrial y afines; Educación; Publicidad y afines; Psicología; Terapias; Antropología y Artes Liberales; Diseño; Sociología, Trabajo Social y afines; Geografía, Historia; Ciencia Política, Relaciones Internacionales; Ingeniería Electrónica, Telecomunicaciones y afines; Ingeniería Civil y afines; Ingeniería Eléctrica y afines; Artes Plásticas, Visuales y afines; Ingeniería Agrícola, Forestal y afines; Ingeniería Agroindustrial, Alimentos y afines; Otras ingenierías;		
RESOLUCIÓN 1452 DE 08 SEP 2023 Hoja No. 2		
Continuación de la Resolución "Por medio de la cual se establecen los requisitos, competencias y experiencia para el desarrollo de las funciones del Oficial de Seguridad de la información y del personal designado como apoyo del Departamento Administrativo Nacional de Estadística - DANE y del Fondo Rotatorio del Departamento Administrativo Nacional de Estadística - FONDANE" Ingeniería Agronómica, Pecuaria y afines; Ingeniería de Minas, Metalurgia y afines; Bacteriología; Medicina Veterinaria; Zootecnia; Salud Pública; Ingeniería Ambiental, Sanitaria y afines; Ingeniería Química y afines. Tiempo de Experiencia: El tiempo de experiencia requerida para el Oficial de Seguridad de la información y el personal de apoyo es la establecida en el Manual Específico de Funciones y Competencias Laborales del DANE, de acuerdo con el nivel del empleo que ostente el designado. Experiencia: Experiencia relacionada con las funciones del artículo segundo de la Resolución No. 644 de 2022, ítem "Oficial o Responsable de Seguridad de la Información", y las establecidas en el Manual Específico de Funciones y Competencias Laborales del servidor designado. Formación Niveles Asesor, Profesional y Contratistas que apoyen el ejercicio y ejecución de funciones inmersas en el rol de Oficial de Seguridad de la Información: Título profesional de alguno de los siguientes núcleos básicos del conocimiento (NBC): Título profesional en las disciplinas de Administración Pública;		

Por lo anterior, el hallazgo 6 queda cerrado.

2.1.5 Hallazgo 7 – Actividad 0140.4 – 0140.5 – 0140.6

Se evidencia la actualización de la documentación asociada a la administración de riesgos de la entidad. La política de administración de riesgos fue actualizada y publicada en Isolución en el mes de octubre de 2023. En este mismo sentido. Se actualizó el documento SIO-040-GUI-002 Guía de administración de riesgos y oportunidades.



- Revisando el sistema 20 no se encuentran los soportes de avance de la actividad, así mismo, al revisar el micrositio de seguridad y privacidad en el SharePoint de la entidad se evidencia que los mapas de riesgos son de la vigencia 2022.
- No se evidencia el cargue de los soportes de los planes de tratamiento de tratamiento de riesgos en el sistema 20.
- Según las evidencias revisadas, el hallazgo se mantiene.

2.1.6 Hallazgo 8 – Actividad 0140.7

No se reportan avances de las actividades del diseño e implementación de indicadores de seguridad y privacidad. Sin embargo, la fecha de finalización planteada en el plan de mejoramiento es 29/03/2024. Por lo anterior, el hallazgo se mantiene parcialmente.

2.1.7 Hallazgo 9 – Actividad 0140.8

El manual de políticas de seguridad GTE-040-MAN-002 Manual de Políticas Complementarias de Seguridad Digital ya se encuentra formalizado dentro del sistema integrado de gestión en Isolución:

<https://dane.isolucion.co/Administracion/frmFrameSet.aspx?Ruta=Li4vRnJhbWVWTZXRBCnRpY3Vsby5hc3A/UGFnaW5hPUJhbmNvQ29ub2NpbWlbnRvRGFuZS80LzQ3ODczYjJjOWFhNjRhZjg4NzFhMjk2ZjQ2NzMzMzMDQzLzQ3ODczYjJjOWFhNjRhZjg4NzFhMjk2ZjQ2NzMzMzMDQzLmFzcCZJREFSVEIDVUxPPTlwMTc4>



Esto da cierre al hallazgo relacionado con el manual de políticas.

2.1.8 Hallazgo 12 – Actividad 0140.9

Dentro de los soportes aportados, se evidencia que la política de uso aceptable de los activos de información fue incluida en el documento SIO-040-GUI-011 Guía para la identificación, clasificación, valoración y etiquetado de activos de información.

 DANE DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA	GUÍA PARA LA IDENTIFICACIÓN, CLASIFICACIÓN, VALORACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN DANE - FONDANE	CÓDIGO: SIO-040- GUI-011 VERSIÓN: 1 FECHA: 20/Nov/2023

4.6. USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN Y ETIQUETADO

- Se debe limitar el acceso a la información valorada como reservada o clasificada, solo tendrán acceso los colaboradores en el ejercicio de sus funciones, obligaciones o responsabilidades institucionales.
- La información electrónica y digital es custodiada por la Oficina de Sistemas siempre y cuando repose en servidores de la entidad, se debe dar cumplimiento a lo establecido en las políticas complementarias y procedimientos de control de acceso. La información física⁴⁵
- Se debe procurar articular la gestión documental con los activos de tipo información identificando los documentos que no están registrados en la Tabla de Retención Documental- TRD. Esta articulación se realiza para mantener actualizadas las TRD y especificar los tiempos de conservación de los activos de información en el archivo de gestión y en el archivo central, y así definir el tiempo para su eliminación y determinar el archivo histórico. Cabe precisar que los activos electrónicos y digitales deben contar con TRD.

Con esta acción se cierra el hallazgo reportado.

2.1.9 Hallazgo 13 – Actividad 0140.10

Al momento de revisar el documento SIO-040-GUI-011 Guía para la identificación, clasificación, valoración y etiquetado de activos de información, no se evidencian lineamientos sobre un esquema de etiquetado que permite identificar el tipo de información que trata o almacenan los activos de información.

Por lo anterior el hallazgo se mantiene.

2.1.10 Hallazgo 14 – Actividad 0140.11

Al momento de revisar el documento SIO-040-GUI-011 Guía para la identificación, clasificación, valoración y etiquetado de activos de información, no se evidencian lineamientos sobre el manejo de los activos de información de conformidad con su clasificación.

Sobre esta actividad se reportan soportes de una capacitación sobre activos de información para que los colaboradores entiendan el manejo de la herramienta de levantamiento de activos y los conceptos necesarios para hacer el levantamiento. Sin embargo, sobre el etiquetado de activos no se presentan avances. La fecha de finalización propuesta para la actividad es el 29/03/2023.

El hallazgo se mantiene parcialmente.

2.1.11 Hallazgo 15 – Actividad 0140.12

Revisando el documento GTE-040-MAN-002 Manual de Políticas Complementarias de Seguridad Digital se pudo evidenciar que en el numeral 4.1 se encuentra documentada la política de control de acceso lógico de la entidad.

4.1.1. Control de acceso lógico

- Los datos de acceso a los sistemas de información deberán estar compuestos por un ID o nombre de usuario y contraseña que deben ser únicos por cada usuario.
- En todos los sistemas de información de la Entidad se deben implementar controles de acceso, de tal forma que haya segregación de funciones entre los tipos de usuarios que puedan acceder a dichos sistemas, así como entre quien otorga el privilegio y quien lo utiliza.
- La Oficina de Sistemas asigna a los usuarios los permisos de acceso a la información con base en los roles y perfiles del usuario aprobados por los responsables de cada grupo o proceso. Esta política aplica para aquellos sistemas que estén sincronizados con el Directorio Activo, sin embargo, los que se encuentran exceptos deben contemplar los controles de seguridad de roles y responsabilidades en el sistema y políticas de nivel de seguridad en las contraseñas.

Con esta actividad cumplida el hallazgo se cierra.

2.1.12 Hallazgo 16 – Actividad 0131.1

Una vez realizada la verificación en el sistema Isolución, se evidenció que el formato GTH-060-PDT-001-f-009 fue actualizado con la inclusión de las responsabilidades a nivel de confidencialidad de la información de autenticación a los diferentes sistemas de información.

6	Cumplir con los siguientes compromisos de confidencialidad y seguridad de la información: 1. Identificar y reportar cualquier incumplimiento de las normas y/o procedimientos de seguridad de la información establecidos. 2. Cumplir las normas de acceso y uso de la información, a través de su software, hardware, redes, medios físicos y facilidades asociadas. 3. Utilizar los recursos informáticos con criterios de racionalidad y únicamente para las actividades propias del rol respectivo, y en beneficio de la entidad. 4. Conocer, cumplir y adoptar las políticas y procedimientos definidos en el marco normativo del Sistema Integrado de Gestión. 5. Conservar con total confidencialidad las contraseñas, tokens, credenciales de acceso a sistemas de información y cualquier recurso de la plataforma tecnológica institucional, incluyendo firmas digitales certificadas y mecanismos de control de acceso a las instalaciones del DANE, teniendo en cuenta que son de uso personal e intransferible. 6. Hacer buen uso del correo electrónico evitando promover o enviar: cadenas de mensajes de cualquier índole, donativos, obras de caridad, envío de virus, envío de software malicioso, avisos clasificados, boletines de cualquier índole, envío de información masiva o cualquier tipo de información no relacionada con la actividad. 7. Utilizar solamente software formalmente autorizado por el DANE a través de la Oficina de Sistemas. 8. Proteger la información en todos los medios (físico, informático, magnético, óptico, electrónico telemático y todo soporte de información que pueda surgir en el futuro, entre otros). 9. No retirar información confidencial,
---	--

⁴ **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

⁵ **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

⁶ **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Con esta actividad realizada se cierra el hallazgo.

2.1.13 Hallazgo 17 – Actividad 0140.13

Revisando el documento GTE-040-MAN-002 Manual de Políticas Complementarias de Seguridad Digita se pudo evidenciar que en el numeral 4.2 se encuentra documentada la política de controles criptográficos de la entidad.

4.2. CRIPTOGRAFÍA
El DANE implementará herramientas de cifrado, con el fin de proteger la confidencialidad e integridad de la información. Así mismo, el GIT de Plataformas Tecnológicas de la Oficina de Sistemas determina los equipos a los cuales se les deberán instalar controles criptográficos adicionales cuando así se requiera. - En el intercambio de información entre entidades públicas, se debe asegurar el uso del sistema de interoperabilidad Xroad establecido por MINTIC, dado que usa una capa de intercambio de datos distribuidos que proporciona una forma estandarizada segura de producir y consumir servicios. - En el intercambio de información con entidades que no usen el sistema de interoperabilidad expuesto por MINTIC, se debe realizar el intercambio de información vía SFTP. - La página web del DANE debe contar con los protocolos de SSL (por sus siglas en inglés Secure Sockets Layer), que actúa como una capa de comunicación y túnel que protege la información enviada y recibida. - Cuando los usuarios requieran acceder a sistemas o redes institucionales en el cumplimiento de sus funciones desde redes remotas, deberán tener habilitado un acceso VPN con token lo cual permite contar con un canal cifrado que garantiza la confidencialidad e integridad de las comunicaciones. - Se debe verificar que todo sistema de información que requiera realizar transmisión de información clasificada o reservada cuente con mecanismos de cifrado de datos.

Con esta actividad cumplida el hallazgo se cierra.

2.1.14 Hallazgo 18 – Actividad 0140.14

Revisando el documento GTE-040-MAN-002 Manual de Políticas Complementarias de Seguridad Digita se pudo evidenciar que en el numeral 4.5.2 se encuentra documentada la política de desarrollo seguro de software.

4.5.2. Seguridad en los procesos de desarrollo seguro de software y soporte

- La responsabilidad de aprobar el desarrollo de aplicaciones estará a cargo de la oficina de sistemas, al igual que la definición del acceso a los recursos para el desarrollo, el licenciamiento en los aplicativos y herramientas utilizadas.
- Se estandarizará el ciclo de vida, los criterios de seguridad y de calidad en el desarrollo de software, siguiendo los lineamientos de la Oficina de Sistemas.
- Se aplicarán los siguientes lineamientos de política para la documentación del software:
 - En los proyectos de desarrollo se describirán los requerimientos de seguridad que deben ser cubiertos por el nuevo sistema.

Con esta actividad cumplida el hallazgo se cierra.

2.1.15 Hallazgo 19 – Actividades 0136.0 - 0136.1 - 0136.2 - 0136.3

1. Dentro de la información aportada por la OSIS se evidencia la asignación de máquinas virtuales a los ingenieros que deben acceder a los diferentes ambientes de la infraestructura tecnológica de la Entidad.

PLATAFORMAS TECNOLÓGICAS

3.2 Usuarios Administradores

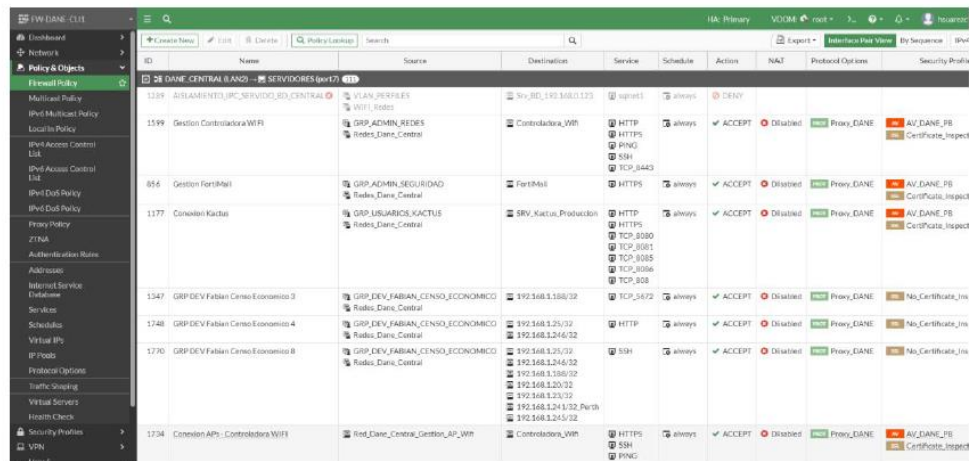
La herramienta de virtualización cuenta con un total de 4 usuarios administradores en Vmware 7.0

Tabla 3. Usuarios Administradores Habilitados.

usuario	Nombre	Correo Electrónico	Rol
nem1024	Ninroth Espinosa	nepinosam@dane.gov.co	administrador
<u>fjquinterob</u>	Francisco Javier Quintero	fjquinterob@dane.gov.co	administrador
<u>awcolmenaresb</u>	Alan Wilmer Colmenares Briones	awcolmenaresb@dane.gov.co	administrador
<u>jecastiblanco</u>	Julian Ernesto Castiblanco Romero	jecastiblanco@dane.gov.co	administrador

2. Dentro de la información aportada se evidencia la existencia de tres informes de depuración de políticas en el foritgate de la Entidad.

Al iniciar el proceso se tenían configuradas 111 políticas de seguridad en esta zona.



ID	Name	Source	Destination	Service	Schedule	Action	NAT	Protocol Options	Security Profile
1359	ANEXAMENED_IPC_SERVIDO_CENTRAL	VLAN_SERVILES	Srv_RD_192.168.0.1/32	igmpv1	always	DENY			
1599	Gestion Controladora WFI	GRP_ADMIN_REDES	Controladora_WFI	HTTP	always	ACCEPT	Disabled	Proxy_DANE	AV_DANE_PB Certificate_Inspect
654	Gestion FortiMail	GRP_ADMIN_SEGURIDAD	FortiMail	SMTP	always	ACCEPT	Disabled	Proxy_DANE	AV_DANE_PB Certificate_Inspect
1377	Conexion Kactus	GRP_USUARIOS_KACTUS	Srv_Kactus_Produccion	HTTP	always	ACCEPT	Disabled	Proxy_DANE	AV_DANE_PB Certificate_Inspect
1347	GRP DEV Fabian Censo Economico 3	GRP_DEV_FABIAN_CENSO_ECONOMICO	192.168.1.150/32	TCP	always	ACCEPT	Disabled	Proxy_DANE	No Certificate_Inspect
1748	GRP DEV Fabian Censo Economico 4	GRP_DEV_FABIAN_CENSO_ECONOMICO	192.168.1.25/32	HTTP	always	ACCEPT	Disabled	Proxy_DANE	No Certificate_Inspect
1730	GRP DEV Fabian Censo Economico 8	GRP_DEV_FABIAN_CENSO_ECONOMICO	192.168.1.25/32	SSH	always	ACCEPT	Disabled	Proxy_DANE	No Certificate_Inspect
1734	Conexion API - Controladora WFI	Red_Dane_Central_Gestion_API_WFI	Controladora_WFI	HTTPS	always	ACCEPT	Disabled	Proxy_DANE	AV_DANE_PB Certificate_Inspect

Durante este mes se depuraron 48 políticas de seguridad, quedando a la fecha configuradas 63 políticas de seguridad en esta zona.

3. Fueron aportados los soportes de la migración y asignación de usuarios al grupo VPN_SSL, así como la activación de doble factor de autenticación y asignación de tokens.

20241400000523

contestar por favor cite estos datos:

Radicado No.: *20241400000523*

Fecha: *Miércoles 17 de Enero 2024*

Página 14 de 26

PLATAFORMAS TECNOLÓGICAS

Migración Usuarios VPNSSL

Durante este mes se continua con el proceso de migración de usuarios con asignación VPNSSL creados en los servidores controladores de dominio a los firewalls perimetrales FG3700D.

En la ejecución de estas actividades, los usuarios son creados en los firewalls perimetrales validando las credenciales de red o dominio ya asignadas, luego de esto los usuarios son asignados a un único grupo creado en los firewalls perimetrales, donde se permite únicamente la conexión por escritorio a los equipos de cómputo asignados en la entidad. De igual manera se realiza la eliminación de todos los grupos a los cuales se encontraban asignados los usuarios y las políticas de seguridad asociadas a estos grupos en los firewalls perimetrales.

Durante este mes se logra realizar la migración de 159 usuarios, a continuación, la relación de usuarios migrados.

GRUPO 15				
S.N o	Objetos seleccionados	Recuento de objetos	Usuario	Token
70	SSL_Sistemas_Git_ProdEstaditicaSIA_AgroEconomicas	7	AOCubillosA	No
70	SSL_Sistemas_Git_ProdEstaditicaSIA_AgroEconomicas	7	DMBarreraM	No
70	SSL_Sistemas_Git_ProdEstaditicaSIA_AgroEconomicas	7	GAMuñozP	No
70	SSL_Sistemas_Git_ProdEstaditicaSIA_AgroEconomicas	7	JSSuarezR	No
70	SSL_Sistemas_Git_ProdEstaditicaSIA_AgroEconomicas	7	LCRamirezC	No
70	SSL_Sistemas_Git_ProdEstaditicaSIA_AgroEconomicas	7	MLPereaM	No
70	SSL_Sistemas_Git_ProdEstaditicaSIA_AgroEconomicas	7	VCorredorE	No
76	SSL_DirRecoleccionAcopio_Git_PreciosCostos	7	ALBlancoM	No
76	SSL_DirRecoleccionAcopio_Git_PreciosCostos	7	DSEspinosaQ	No
76	SSL_DirRecoleccionAcopio_Git_PreciosCostos	7	DAAvilaM	No

4. Se aporta el listado de asistencia de la socialización de las tareas realizadas.

Temas varios de soporte informático con sedes territoriales						
Participantes que asistieron	15					
Hora de inicio	8/18/23, 8:44:00 AM					
Hora de finalización	8/18/23, 11:23:31 AM					
Duración de la reunión	2 h 39 min 30s					
Tiempo medio de asistencia	1 h 15 min 22s					
2. Participantes						
Nombre	Primera entrada	Última salida	Duración de la reunión	Correo electrónico	Id. de participante (UPN)	Rol
Omar Yovanny Barahona Alvarado	8/18/23, 9:00:44 AM	8/18/23, 10:48:07 AM	1 h 47 min 23s	oybarahona@dane.gov.co	OYBarahona@DANE.GOV.CO	Organizador
Carlos Javier Vargas Bayona	8/18/23, 8:44:05 AM	8/18/23, 10:09:48 AM	1 h 25 min 42s	cjvargasb@dane.gov.co	CJVargasB@DANE.GOV.CO	Moderador
Yurid Milena Pérez Cañizares	8/18/23, 8:55:40 AM	8/18/23, 10:24:41 AM	1 h 27 min 46s	ymperez@dane.gov.co	YMPerezC@DANE.GOV.CO	Moderador
Edward Sandoval Mejia	8/18/23, 8:57:32 AM	8/18/23, 10:24:37 AM	1 h 27 min 4s	easandovalm@dane.gov.co	easandovalm@DANE.GOV.CO	Moderador
Sandra Milena Ramírez Ramírez	8/18/23, 8:59:52 AM	8/18/23, 10:00:17 AM	1 h 25s	SMRamirezR@dane.gov.co	SMRamirezR@DANE.GOV.CO	Moderador
Roberto Cesar Fonseca Barcos	8/18/23, 8:59:54 AM	8/18/23, 10:24:36 AM	1 h 24 min 42s	rcfonsecab@dane.gov.co	RCFonsecaB@DANE.GOV.CO	Moderador
Luz Dary Aponte García	8/18/23, 9:00:51 AM	8/18/23, 10:48:13 AM	1 h 47 min 22s	luzdary@dane.gov.co	LDAponteG@DANE.GOV.CO	Moderador
Oscar Eduardo Otálvaro Cruz	8/18/23, 9:01:15 AM	8/18/23, 10:24:36 AM	1 h 23 min 20s	oeotalvaroc@dane.gov.co	OEotalvaroc@DANE.GOV.CO	Moderador
Francisco Javier Zambrano Jimenez	8/18/23, 9:01:41 AM	8/18/23, 10:48:00 AM	1 h 46 min 19s	fjzambranoj@dane.gov.co	FJZambranoJ@DANE.GOV.CO	Moderador
Angel Yesid Ducuara Cruz	8/18/23, 9:04:32 AM	8/18/23, 9:48:37 AM	44 min 4s	ayducuarac@dane.gov.co	ayducuarac@DANE.GOV.CO	Moderador
Juan David Socha Muñoz	8/18/23, 9:07:12 AM	8/18/23, 10:24:46 AM	1 h 17 min 33s	jdsocham@dane.gov.co	jdsocham@DANE.GOV.CO	Moderador
Hendrix Suarez Cardenas	8/18/23, 9:10:06 AM	8/18/23, 10:09:07 AM	59 min	hsuarez@dane.gov.co	HSuarezC@DANE.GOV.CO	Moderador
Carlos Andres Sanchez Ruiz	8/18/23, 9:15:20 AM	8/18/23, 9:30:37 AM	15 min 17s	casanchezr@dane.gov.co	CASanchezR@DANE.GOV.CO	Moderador
Gloria Yazmin Herrera Linares	8/18/23, 9:19:23 AM	8/18/23, 11:23:31 AM	2 h 4 min 7s	gyherreral@dane.gov.co	GYHerreral@DANE.GOV.CO	Moderador
Harold Leandro Abril Triana	8/18/23, 10:36:14 AM	8/18/23, 10:36:33 AM	19s	hlabrilt@dane.gov.co	HLAbrilT@DANE.GOV.CO	Moderador

Con el cumplimiento de estas actividades se da por cerrado el hallazgo.

Departamento Administrativo Nacional de Estadística

Carrera 59 No. 26 - 70, Interior CAN, Edificio DANE

Bogotá D.C. Colombia / Código postal 111321

Teléfono (601) 5978300

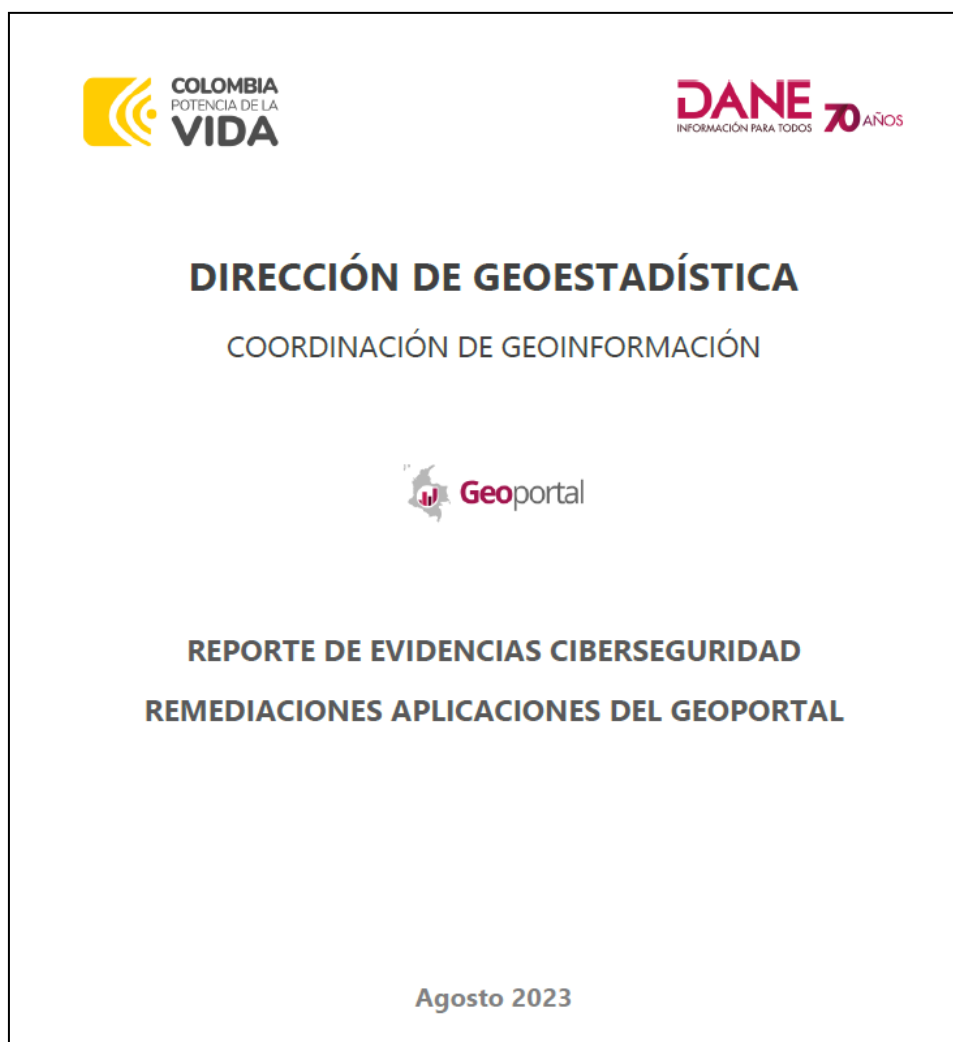
www.dane.gov.co / contacto@dane.gov.co

2.1.16 Hallazgo 20 – Actividades 0135.1 - 0135.2 - 0135.3 - 0135.4

1. Se evidencio que la GTE-020-GUI-002 Guía Metodológica de Sistemas de Información se encuentra aprobada y publicada en Isolución. Esta guía contiene los componentes necesarios para realizar pruebas no funcionales (de seguridad) a los sistemas de información dentro del ciclo de desarrollo de software con el fin de detectar brechas antes de la salida a producción de los aplicativos.

<https://dane.isolucion.co/Administracion/frmFrameSet.aspx?Ruta=Li4vRnJhbWVTZXRlc3R5Y3Vsby5hc3A/UGFnZW5hPUJhbmNvQ29ub2NpbWllbnRvRGFuZS9iL2lxZDg4OWEwMzNmYTQ1Nzg4MjExZmYwNDI4YzYzMzlyL2lxZDg4OWEwMzNmYTQ1Nzg4MjExZmYwNDI4YzYzMzlyLmFzcCZJREFSVEIDVUxPTE5NTly>

2. Se evidencia la gestión de las vulnerabilidades generadas del informe del BID. Esto se pudo observar en el documento 20230825_InformeGeoportalRemediaciónBID. Adicionalmente, se aporta evidencia de los planes de trabajo de gestión de estas vulnerabilidades.

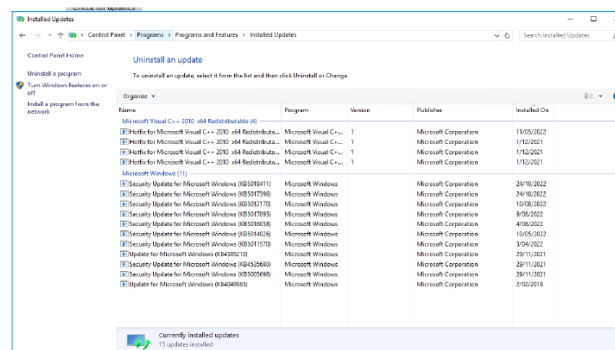


3. Se evidencia el aporte de los soportes de la remediación de vulnerabilidades en los servidores Windows y Linux asociados a la infraestructura analizada por el BID.



Instalación de actualizaciones críticas liberadas por Microsoft

Imagen 3 instalación de Actualizaciones durante el 2022



Original	Program	Version	Publisher	Installed On
Microsoft Visual C++ 2010 x64 Redistributable (x64)	Microsoft Visual C++	1	Microsoft Corporation	11/05/2022
[E] Update for Microsoft Visual C++ 2010 x64 Redistributable	Microsoft Visual C++	1	Microsoft Corporation	1/12/2021
[E] Update for Microsoft Visual C++ 2010 x64 Redistributable	Microsoft Visual C++	1	Microsoft Corporation	1/12/2021
[E] Update for Microsoft Visual C++ 2010 x64 Redistributable	Microsoft Visual C++	1	Microsoft Corporation	1/12/2021
Microsoft Windows (1)	Microsoft Windows		Microsoft Corporation	20/10/2022
[E] Security Update for Microsoft Windows (KB5014011)	Microsoft Windows		Microsoft Corporation	24/10/2022
[E] Security Update for Microsoft Windows (KB5014011)	Microsoft Windows		Microsoft Corporation	15/08/2022
[E] Security Update for Microsoft Windows (KB5014011)	Microsoft Windows		Microsoft Corporation	9/08/2022
[E] Security Update for Microsoft Windows (KB5014011)	Microsoft Windows		Microsoft Corporation	4/08/2022
[E] Security Update for Microsoft Windows (KB5014011)	Microsoft Windows		Microsoft Corporation	15/05/2022
[E] Security Update for Microsoft Windows (KB5014011)	Microsoft Windows		Microsoft Corporation	3/04/2022
[E] Update for Microsoft Windows (KB4035101)	Microsoft Windows		Microsoft Corporation	29/11/2021
[E] Security Update for Microsoft Windows (KB4035101)	Microsoft Windows		Microsoft Corporation	29/11/2021
[E] Security Update for Microsoft Windows (KB4035101)	Microsoft Windows		Microsoft Corporation	29/11/2021
[E] Update for Microsoft Windows (KB4035101)	Microsoft Windows		Microsoft Corporation	2/02/2019

20241400000523

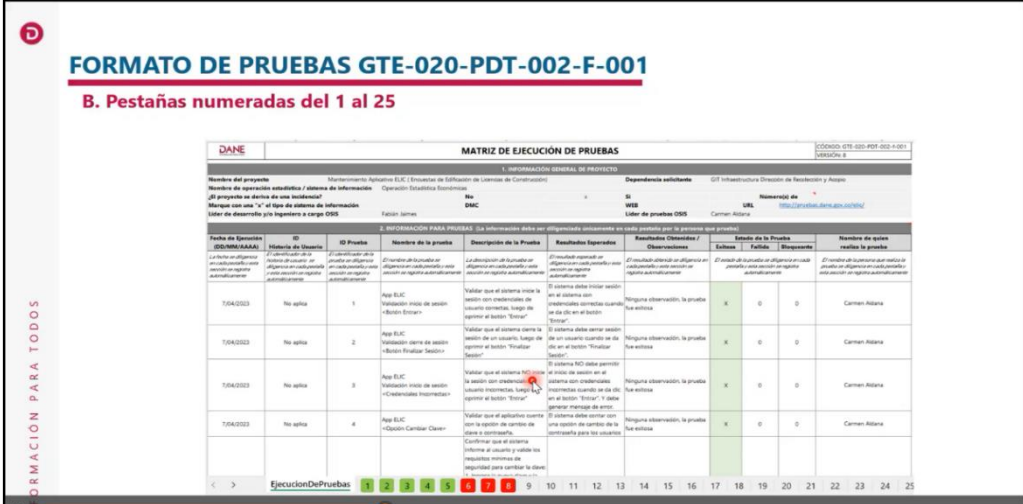
contestar por favor cite estos datos:

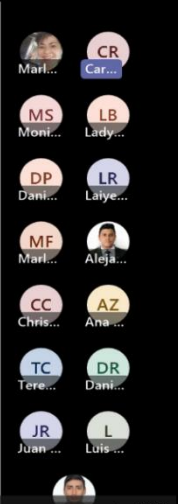
Radicado No.: *20241400000523*

Fecha: *Miércoles 17 de Enero 2024*

Página 17 de 26

4. Una vez revisada la información aportada se puede observar que se realizaron las socializaciones propuestas sobre el documento de arquitectura y la remediación de vulnerabilidades.





Con estas actividades cumplidas se da cierre al hallazgo

2.1.17 Hallazgo 21 – Actividades 0140.15 - 0140.16 - 0140.17

1. Revisando el documento GTE-040-MAN-002 Manual de Políticas Complementarias de Seguridad Digita se pudo evidenciar que en el numeral 4.6 se encuentra documentada los lineamientos de seguridad en la relación con proveedores.


**DEPARTAMENTO ADMINISTRATIVO
NACIONAL DE ESTADÍSTICA**

**MANUAL DE POLÍTICAS
COMPLEMENTARIAS DE SEGURIDAD
DIGITAL**

CÓDIGO: GTE-040-MAN-002
VERSION: 01
FECHA: octubre de 2023

PROCESO: GESTIÓN TECNOLÓGICA

SUBPROCESO: SEGURIDAD INFORMÁTICA

- Al menos una vez cada año, se debe realizar un escaneo de las aplicaciones más recientes puestas en producción, en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.

4.6. RELACIÓN CON LOS PROVEEDORES

- El DANE establecerá políticas y requisitos de seguridad digital para mitigar los riesgos asociados a cada proceso de contratación.
- Antes de iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad digital y de la información necesario durante y después del contrato
- Los supervisores de contratos deben asegurarse de comunicar las políticas y procedimientos de seguridad digital y de la información a los proveedores y/o contratistas.

4.6.1. Tratamiento de la Seguridad dentro de los Acuerdos con Proveedores

- Todos los contratistas, proveedores y/o terceros que presten sus servicios a la entidad, deberán aceptar los compromisos de confidencialidad definidos por el DANE, los cuales reflejan las directrices de protección y buen uso de la información contenidos en normas y políticas del SGSI.

20241400000523

contestar por favor cite estos datos:

Radicado No.: *20241400000523*

Fecha: *Miércoles 17 de Enero 2024*

Página 18 de 26

2. Se evidencia el desarrollo de jornadas de sensibilización en activos de información y gestión de riesgos.

A	B	C	D	E	F	G	H
1. Resumen							
Título de la reunión	Capacitación Activos de Información						
Participantes que asistieron	13						
Hora de inicio	11/24/23, 8:51:30 AM						
Hora de finalización	11/24/23, 11:04:53 AM						
Duración de la reunión	2 h 13 min 22 s						
Tiempo medio de asistencia	1 h 56 min 48 s						
2. Participantes							
Nombre	Primera entrada	Última salida	Duración de la	Correo electrónico	Id. de participi Rol		
Carolina Osorio Gomez	11/24/23, 8:51:38 AM	11/24/23, 11:02:13 min 14 s	2 h 13 min 14 s	cosorlog@dane.gov.co	COsorioG@D/ Organizador		
Lina Maria Cardenas Rojas	11/24/23, 8:56:17 AM	11/24/23, 11:02:08 min	2 h 8 min	lmcardenasr@dane.gov.co	LMCardenasR/ Moderador		
Viviana Jhaneth Naranjo Lopez	11/24/23, 8:56:25 AM	11/24/23, 11:02:08 min 8 s	2 h 8 min 8 s	vjnaranjol@dane.gov.co	VJNaranjol@I/ Moderador		
Hernando Mancipe Perez	11/24/23, 8:58:58 AM	11/24/23, 11:02:05 min 30 s	2 h 5 min 30 s	hmancipep@dane.gov.co	HMancipeP@/ Moderador		
Juan Nicolas Acevedo Pacheco	11/24/23, 9:00:29 AM	11/24/23, 11:02:04 min 7 s	2 h 4 min 7 s	jnacevedop@dane.gov.co	JNAcevedoP@/ Moderador		
Rodolfo Arturo Gonzalez Becerra	11/24/23, 9:00:41 AM	11/24/23, 11:02:03 min 37 s	2 h 3 min 37 s	ragonzalezb@dane.gov.co	RAGonzalezB@/ Moderador		
Anderson Eduardo Devia Vasquez	11/24/23, 9:01:08 AM	11/24/23, 11:02:03 min 25 s	2 h 3 min 25 s	aedevia@dane.gov.co	AEDeviaV@D/ Moderador		
Flor Marina Monroy Correa	11/24/23, 9:01:29 AM	11/24/23, 11:02:03 min 4 s	2 h 3 min 4 s	fmonroyc@dane.gov.co	FMMonroyC@/ Moderador		
Aseneth Sanchez Ariza	11/24/23, 9:03:45 AM	11/24/23, 11:02:03 s	2 h 37 s	asancheza@dane.gov.co	ASanchezaA@/ Moderador		
Legnny Yessenia Diaz Fierro	11/24/23, 9:04:39 AM	11/24/23, 11:01:59 min 41 s	1 h 59 min 41 s	lydiazf@dane.gov.co	LYDiazF@DAN/ Moderador		
Liliana Andrea Aguirre Lugo	11/24/23, 9:09:38 AM	11/24/23, 11:01:50 min 21 s	1 h 50 min 21 s	laaguirrel@dane.gov.co	LAAguirreL@/ Moderador		
Paola Fernanda Medina Tovar	11/24/23, 10:18:46 AM	11/24/23, 10:13:34 min 20 s	34 min 20 s	pfmedinat@dane.gov.co	PFMedinaT@/ Moderador		
Edwin Mauricio González Hernández líder 2023-4				edwin.gonzalez@eud.com.co	edwin.gonzalez/ Moderador		

3. Se presentan avances de la implementación del MSPI al comité de Seguridad y Privacidad de la Información.

 DANE INFORMACIÓN PARA TODOS	ACTA DE REUNIÓN / AYUDA DE MEMORIA	Código: SIO-020-GUI-001-f-002
		Versión: 06

1. Verificación del quórum

El secretario técnico del comité verifica si hay el quórum para desarrollar el Comité, determina que asistieron la mitad más uno de los miembros para tomar decisiones. Indica orden del día e inicia la agenda.

2. Presentación de los avances de los productos del plan de seguridad de la información (Oficina Asesora de Planeación)

La Oficina Asesora de Planeación presenta el seguimiento de las actividades y los avances del plan de seguridad de la información, en la herramienta de SharePoint que se dispuso para tal fin y está para consulta del comité en el siguiente enlace:

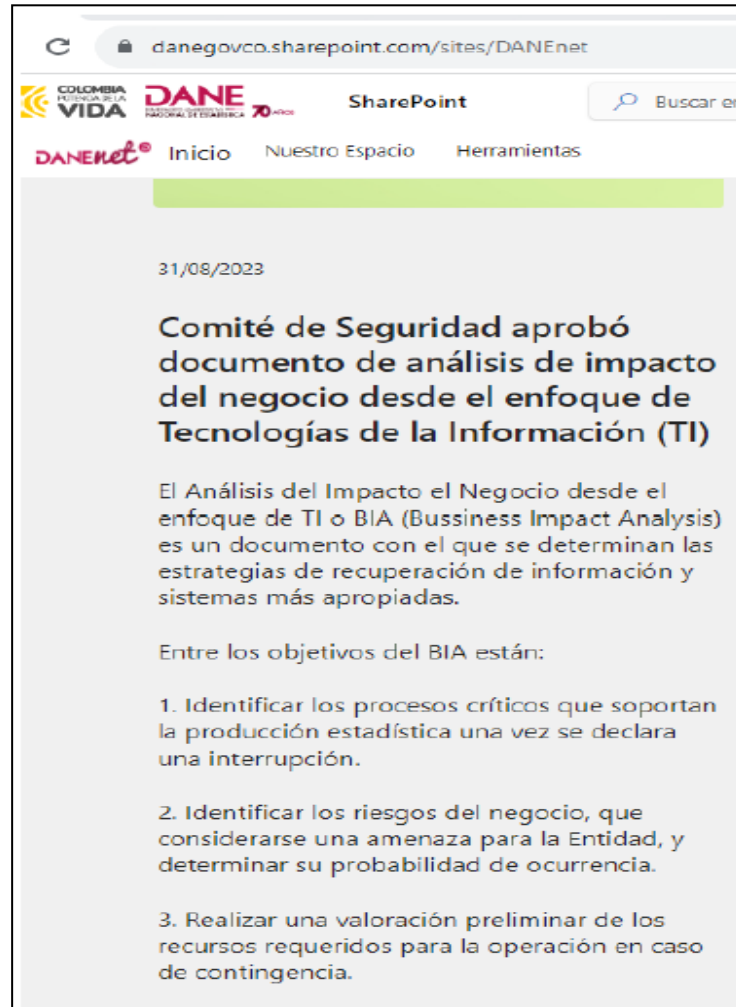
<https://danegovco.sharepoint.com/sites/osis/seguridad/Lists/Plan%20MSPI%202023/AllItems.aspx>

En resumen, de los 16 productos 8 se encuentran en ejecución y 8 no iniciados, a continuación, se relaciona el cuello de botella o alerta de los 3 productos no iniciados que deberían estar en estado de ejecución de acuerdo al cronograma:

- Definición de 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:

Cuello de botella: conocer si en el informe final de auditoría del MSPI, la Oficina de Control Interno mantiene este hallazgo.

Alerta: no se cuenta aún con el apoyo técnico para el responsable de seguridad de la información, debido a que la OPLAN tiene previsto proveer esta necesidad con un encargo, pero hubo una reclamación por parte uno de los posibles candidatos.



Con estas actividades cumplidas se cierra el hallazgo.

2.1.18 Hallazgo 23 – Actividades 0133.1 – 0133.2

Revisando las evidencias de la actividad, se evidenció que la OSIS hizo la solicitud de aprobación a las partes interesadas del documento 22092023 Análisis de Impacto del Negocio BIA2.dox. Se presenta como evidencia los correos de socialización y solicitud de aprobación del documento. Adicionalmente, la votación de aprobación se hizo de forma virtual y el documento fue aprobado.

Con estas actividades el hallazgo se cierra.

2.1.19 Hallazgo 24 – Actividades 0134.1 – 0134.2 - 0134.3

1. Se evidencia que en conjunto con el proveedor Oracle se hace una propuesta de solución DRP para la entidad. En esta propuesta se identifican causas de indisponibilidad y las consecuencias que esto trae

para la Entidad. Adicionalmente, se abordan conceptos claves para la recuperación en caso de catástrofes tecnológicas.

2. También se evidencia que se hizo una sesión presencial para realizar la presentación de la necesidad de la implementación de un DRP en la Entidad. Se aporta presentación y asistencia.

	ACTA DE REUNIÓN / AYUDA DE MEMORIA	Código: SIO-020-GUI-001-f-002 Versión: 06
---	---	--

Desarrollo:**1. Inicio de reunión**

La reunión se realiza como parte de la investigación de tecnologías para la implementación de un DRP y la determinación de opciones de acuerdo con lo que se requiere por parte de la Entidad.

Se envía el link de la reunión para las personas que no se encuentran de forma presencial. La reunión está enfocada en la solución que puede utilizarse para contar con soluciones DRP para bases de datos sin usar herramienta de terceros y para sitios web.

2. Alcance

- Estrategia de continuidad DRP para los portales WEB.
- Estrategia de continuidad DRP para bases de datos.

Los desafíos de la recuperación ante desastres incluyen:

- Reducir el tiempo de inactividad
- Infraestructura Adicional
- Gestión de la complejidad
- Asegurar el cumplimiento

3. Alternativas de solución

Para los portales en nube publica Oracle se puede implementar el Full Stack Disaster Recovery que es una solución que organiza la transición de recursos informáticos, bases de datos y aplicaciones entre regiones de la nube publica de Oracle, es decir que se tienen los recursos informáticos que componen una solución replicados en otra región de la nube ubicada en otra parte del mundo. La Entidad puede automatizar las acciones necesarias para recuperar uno o más sistemas de negocio sin rediseñar ni reorganizar la infraestructura, las bases de datos o las aplicaciones existentes.

3. Se hace solicitud de modificación de la actividad 134 debido ya que no se cuenta con el análisis ni el estudio técnico. Se propone entregar un informe técnico de la implementación de una solución DRP en el DANE, pero en el repositorio no se encuentran avances de dicho informe.

Nota aclaratoria: Teniendo en cuenta la respuesta al informe preliminar con radicado 20231300026433, se evidenció en el Systema 20 el cargue de las evidencias relacionadas con el análisis, el diseño de solución técnica y el estudio de mercado para la adquisición/implementación de la solución que contemple las

necesidades de continuidad del negocio que fueron identificadas en el BIA y los avances de la implementación de una solución de DRP y los elementos que lo componen de acuerdo con las soluciones que adquirió la entidad.

Con esta aclaración, se da por cerrado el hallazgo.

2.1.20 Hallazgo 26 – Actividades 0132.1 - 0132.2 - 0132.3 - 0132.4

Una vez realizada la verificación en el micrositio de protección de datos personales y en el sistema de información Isolución se pudo evidenciar los siguiente:

1. Autorizaciones de datos personales:

La Entidad adoptó los siguientes instrumentos para obtener las autorizaciones para el tratamiento de datos personales en los distintos medios de recolección:

Autorización de Recolección y Tratamiento de Datos Personales para Pasantes/Practicantes del DANE. GTH-070-PDT-010-f-005.

Autorización de Recolección y Tratamiento de Datos Personales para funcionarios. GTH-060-PDT-001-f-014

Autorización de Recolección y Tratamiento de Datos Personales de Postulantes de Contratación o Contratistas. GCO-050-PDT-001-f-010

Autorización de recolección y tratamiento de datos personales de oferentes. GCO-040-PDT-002-f-018

Autorización y registro de ingreso menores de edad en las instalaciones del DANE. GBS-030-PDT-001-f-009

Autorización consulta datos personales en registro de inhabilidades delitos sexuales. GCO-040-PDT-008-f-008

Formato registro de captura de huellas y/o imágenes faciales - personal interno. GBS-030-PDT-001-f-013.

Autorización de tratamiento de datos sensibles (datos biométricos) para el ingreso a las instalaciones del DANE.

Planilla control acceso - personal. GBS-030-PDT-003-f-001

Planilla control acceso áreas restringidas. GBS-030-PDT-003-f-002

Ingreso masivo para eventos internos DANE central GBS-030-PDT-001-f-011

Formato autorización ingreso sede fin de semana GBS-030-PDT-001-f-012

2. PROCEDIMIENTO PARA EL TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES A CARGO DEL DANE SIO-040-PDT-006.

Dentro de este procedimiento del mes de octubre de 2023, se hace identificación de los medios de recolección, validación de la obtención de la autorización, medios de almacenamiento, se identifica la necesidad de realizar transmisiones o transferencias de datos personales.

3. Manual de Políticas Internas para el Tratamiento y Protección de Datos Personales. SIO-020-MAN-003.

Este documento da cumplimiento a lo exigido por la ley de protección de datos con respecto a la existencia de un manual interno de políticas y procedimientos que define niveles de autoridad en el gobierno de dtos personales, las responsabilidades de las distintas líneas de defensa, la identificación de transmisiones (encargados) y transferencias, las actividades en todo el ciclo del tratamiento de datos personales, los

procedimientos de peticiones y reclamos por parte de titulares y lineamientos para la gestión de incidentes de datos personales.

4. Procedimiento Atención de solicitudes relacionadas con datos personales. COM-070-PDT-009.

Este procedimiento contiene las actividades necesarias para garantizar el derecho de habeas data a los titulares de datos. Además, contiene las políticas de operación y las responsabilidades del oficial de protección de datos personales.

Adicionalmente, el procedimiento tiene asociado el Formato complementario solicitud de datos personales. COM-070-PDT-009-f-001.

Con estas actividades realizadas el hallazgo se cierra.

3. FORTALEZAS

- La Oficina de Sistemas de Información logró tener infraestructura redundante para las copias de seguridad en un Data Center Alterno en la ciudad de Medellín, lo cual permite garantizar la protección de los Backups y un nivel alto de eficiencia en cuanto a restauraciones de información se refiere. Adicionalmente, adquirió licenciamiento de Oracle Cloud para tener una segunda contingencia para las copias de seguridad y ya inició su implementación.
- Se evidenció una gestión adecuada de las vulnerabilidades reportadas por el BID. En esta gestión de brechas de seguridad se evidenció que se acortó el tiempo de solución de las debilidades de seguridad y las actividades de remediación se hacen en ambientes controlados. Adicionalmente, se hacen pruebas a los sistemas de información antes de salir a producción.
- Se pudo observar que la documentación de la arquitectura de referencia para los sistemas de información es robusta y contiene todos los componentes necesarios para garantizar la seguridad de la información en todo el ciclo de desarrollo de los sistemas de información.
- La Secretaría General logró documentar e implementar los requisitos que establece la Ley 1581 de 2012 y su decreto reglamentario 1377 de 2013, a nivel de autorizaciones, manual interno de política de procedimientos, atención de PQR y procedimiento de gestión de datos personales con los lineamientos, actividades que se realizan durante todo el ciclo del dato y contratos de transmisión y transferencia de datos personales

4. RELACIÓN DE HALLAZGOS QUE NO FUERON CERRADOS

No.	Descripción de la Situación	<i>criterio</i>
H4	Revisando Systema 20 no se encuentran evidencias sobre el avance de esta actividad. En el instrumento del plan de mejoramiento se registra que la actividad tiene fecha de finalización 15/12/20023 pero la declaración de aplicabilidad continúa siendo un borrador	<i>MSPI – ISO 27001(6.1.3)</i> <i>La Entidad debe producir una declaración de aplicabilidad que contenga los controles necesarios y la justificación de las inclusiones, ya sea que se implementen</i>

No.	Descripción de la Situación	criterio
		<i>o no, y la justificación para las exclusiones de los controles del MSPI.</i>
H7	1. Se evidencia la actualización de la documentación asociada a la administración de riesgos de la entidad. La política de administración de riesgos fue actualizada y publicada en Isolución en el mes de octubre de 2023. En este mismo sentido. Se actualizó el documento SIO-040-GUI-002 Guía de administración de riesgos y oportunidades. 2. Revisando el sistema 20 no se encuentran los soportes de avance de la actividad. Adicionalmente, al revisar el micrositio de seguridad y privacidad en el SharePoint de la entidad se evidencia que los mapas de riesgos son de la vigencia 2022. 3. No se evidencia el cargue de los soportes de los planes de tratamiento de tratamiento de riesgos en el sistema 20.	<i>MSPI – ISO 27001(8.2 y 8.3) – Política de Administración de Riesgos numeral 3.4.2 Primera línea de defensa</i> <i>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</i> <i>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.</i> <i>b) La organización debe conservar información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información.</i>
H8	No se reportan avances de las actividades del diseño e implementación de indicadores de seguridad y privacidad. Sin embargo, la fecha de finalización planteada en el plan de mejoramiento es 29/03/2024.	<i>MSPI – ISO 27001(9.1)</i> <i>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.</i>
H13	Al momento de revisar el documento SIO-040-GUI-011 Guía para la identificación, clasificación, valoración y etiquetado de activos de información, no se evidencian lineamientos sobre un esquema de etiquetado que permite identificar el tipo de información que trata o almacenan los activos de información.	<i>MSPI (AD.4.2.2) – ISO 27001 (A.8.2.2)</i> <i>Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de</i> <i>Información adoptada por la organización.</i>
H14	1. Al momento de revisar el documento SIO-040-GUI-011 Guía para la identificación, clasificación, valoración y etiquetado de activos de información, no se evidencian lineamientos sobre el manejo de los activos de información de conformidad con su clasificación. 2. Sobre esta actividad se reportan soportes de una capacitación sobre activos de información para que los colaboradores entiendan el manejo de la herramienta	<i>MSPI (AD.4.2.3) – ISO 27001 (A.8.2.3)</i> <i>Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.</i>

No.	Descripción de la Situación	criterio
	de levantamiento de activos y los conceptos necesarios para hacer el levantamiento. Sin embargo, sobre el etiquetado de activos no se presentan avances. La fecha de finalización propuesta para la actividad es el 29/03/2023.	

5. CONCLUSIONES

- 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 de los planes de mejoramiento, a corto plazo pueden llegar a un nivel de madurez Alto.
- La entidad logró robustecer de manera significativa el Programa de Protección de Datos Personales, dando cumplimiento a lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
- La OSIS ha logrado mejorar significativamente las estrategias de contingencia ante desastres tecnológicos; garantizando alta disponibilidad y protección de la confidencialidad, integridad y disponibilidad de la información.

6. RECOMENDACIONES (dirigidos a atacar la causa encontrada por el auditor)

- Para futuras actualizaciones del Alcance del MSPI, se recomienda establecer los límites de implementación a nivel de procesos, áreas de trabajo, infraestructura tecnológica e infraestructura física.
- 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.
- 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.
- 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.
- Se debe definir una estrategia de 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.
- Seguir trabajando en el plan de continuidad del negocio para garantizar alta disponibilidad en caso de desastres o catástrofes tecnológicas.

20241400000523

contestar por favor cite estos datos:

Radicado No.: *20241400000523*

Fecha: *Miércoles 17 de Enero 2024*

Página 25 de 26

7. APROBACIÓN INFORME PRELIMINAR DE AUDITORÍA		
Nombre Completo	Responsabilidad (cargo)	Firma
JORGE LUIS VARGAS BUITRAGO	Auditor Líder	(FIRMADO ELECTRONICAMENTE) JORGE LUIS VARGAS BUITRAGO 13.861.633
DUVY JOHANNA PLAZAS SOCHA	Jefe Oficina de Control Interno	 Firmado digitalmente por PLAZAS SOCHA DUVY JOHANNA

8. Soportes Documentales – Auditoría					
No	Nº. Del Hallazgo u Observación	Nombre del Documento	Ubicación Física o Magnético	Área Responsable	Responsable
1	H1	Contexto Institucional Septiembre 2023	Sistema 20/ Planes de Mejoramiento	OCI	
2	H2	No se evidenció documento			
3	H3	GTE-040-MAN-002 Manual de Políticas Complementarias de Seguridad Digital			
4	H4	Declaración de aplicabilidad (no existe aún)			
5	H5	Política de seguridad de la Información			
6	H6	Resolución 1248 del 17 de agosto de 2023			
7	H7	Resolución 1452 de 2023			
8	H8	Política de administración de riesgos fue octubre de 2023			
8	H9	Sitio del sistema integrado de gestión en SharePoint			
8	H9	GTE-040-MAN-002 Manual de Políticas Complementarias de Seguridad Digital			
10	H12	SIO-040-GUI-011 Guía para la identificación, clasificación, valoración y etiquetado de activos de información.			
11	H13	SIO-040-GUI-011 Guía para la identificación, clasificación, valoración y etiquetado de activos de información.			
12	H14	SIO-040-GUI-011 Guía para la identificación, clasificación, valoración y etiquetado de activos de información.			
13	H15	GTE-040-MAN-002 Manual de Políticas Complementarias de Seguridad Digital			
14	H16	GTH-060-PDT-001-f-009 Acuerdo de confidencialidad		OCI	
15	H17	GTE-040-MAN-002 Manual de Políticas Complementarias de Seguridad Digital			
16	H18	GTE-040-MAN-002 Manual de Políticas Complementarias de Seguridad Digital			
17	H19	Prueba de recorrido en sesión virtual con la OSIS Listados de asistencia a capacitaciones Documentos de depuración de políticas en el Firwall – Fortigate Documento de migración a la política VPN_SSL			
18	H20	GTE-020-GUI-002 Guía Metodológica de Sistemas de Información			
19	H21	GTE-040-MAN-002 Manual de Políticas Complementarias de Seguridad Digital Listados de asistencia a capacitaciones Acta comité de seguridad y privacidad de la información			

Departamento Administrativo Nacional de Estadística

Carrera 59 No. 26 - 70, Interior CAN, Edificio DANE

Bogotá D.C. Colombia / Código postal 111321

Teléfono (601) 5978300

www.dane.gov.co / contacto@dane.gov.co

20241400000523

contestar por favor cite estos datos:

Radicado No.: *20241400000523*

Fecha: *Miércoles 17 de Enero 2024*

Página 26 de 26

8. Soportes Documentales – Auditoría					
No	N°. Del Hallazgo u Observación	Nombre del Documento	Ubicación Física o Magnético	Área Responsable	Responsable
20	H23	22092023 Análisis de Impacto del Negocio BIA2.			
21	H24	Presentación de solución Oracle Prueba de recorrido en sesión virtual con la OSIS			
19	H26	Autorización de Recolección y Tratamiento de Datos Personales para Pasantes/Practicantes del DANE. GTH-070-PDT-010-f-005. Autorización de Recolección y Tratamiento de Datos Personales para funcionarios. GTH-060-PDT-001-f-014 Autorización de Recolección y Tratamiento de Datos Personales de Postulantes de Contratación o Contratistas. GCO-050-PDT-001-f-010 Autorización de recolección y tratamiento de datos personales de oferentes. GCO-040-PDT-002-f-018 Autorización y registro de ingreso menores de edad en las instalaciones del DANE. GBS-030-PDT-001-f-009 Autorización consulta datos personales en registro de inhabilidades delitos sexuales. GCO-040-PDT-008-f-008 Formato registro de captura de huellas y/o imágenes faciales - personal interno. GBS-030-PDT-001-f-013. Autorización de tratamiento de datos sensibles (datos biométricos) para el ingreso a las instalaciones del DANE. Planilla control acceso - personal. GBS-030-PDT-003-f-001 Planilla control acceso áreas restringidas. GBS-030-PDT-003-f-002 Ingreso masivo para eventos internos DANE central GBS-030-PDT-001-f-011 Formato autorización ingreso sede fin de semana GBS-030-PDT-001-f-012 PROCEDIMIENTO PARA EL TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES A CARGO DEL DANE SIO-040-PDT-006. Manual de Políticas Internas para el Tratamiento y Protección de Datos Personales. SIO-020-MAN-003. Procedimiento Atención de solicitudes relacionadas con datos personales. COM-070-PDT-009. Formato complementario solicitud de datos personales. COM-070-PDT-009-f-001.			
20	No Aplica	20231100026513_Rta_Informe_Preliminar_OPLAN	Z:\14. CONTROL DE GESTIÓN - CGE\Oficina Control Interno 2023\AUDITORÍA INTERNA\35. MSPI	OCI	OPLAN
21	No aplica	20231300026433 Rta_informe preliminar – OSIS		OCI	OSIS
22	No Aplica	Correo Electrónico del 26 de Diciembre de 2023 Respuesta Informe Preliminar Secretaría General		OCI	Secretaría 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.					