OFICINA DE CONTROL INTERNO

INFORME DE AUDITORÍA AL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ASI 2026-002

PERIODO AUDITADO
01 DE ENERO DE 2023 A 28 DE FEBRERO DE 2026

ENRIQUE CASTIBLANCO BEDOYA
JEFE DE OFICINA

CLAUDIA MARCELA QUICENO DUQUE
JEFE COORDINACIÓN DE AUDITORÍA INTEGRAL

EQUIPO AUDITOR:
SANDRA YASMÍN FLÓREZ ABRIL - LÍDER
JUAN FELIPE SOLÓRZANO GARCÍA

EVALUADOR DESPACHO
JUAN RAFAEL LOZANO RODRÍGUEZ

BOGOTÁ, JULIO DE 2026

CONTENIDO

Pág.

AUDITORÍA AL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
ASI 2026-002

1. DESCRIPCIÓN GENERAL

En el desarrollo de la auditoría se tuvo en cuenta la Planeación Estratégica vigente para el periodo evaluado, en este sentido el ejercicio se enmarcó en los componentes del Mapa de alineación total DIAN 2026[1], con el cual se pretende unificar las acciones de todos los colaboradores en busca de una visión compartida, una estrategia acordada, y corresponsabilidad en los resultados alcanzados; es así como, con este ejercicio se aporta al cumplimiento del lineamiento estratégico: "*Consolidar la modernización de la DIAN*" y el elemento de visión "*Entidad moderna, cercana y humana*", para el cumplimiento de los objetivos institucionales y además, generar confianza en los ciudadanos y grupos de valor e interés.

Es de resaltar que en desarrollo del ejercicio auditor la Oficina de Control Interno se vio impactada en el desempeño de sus labores, por el retiro de funcionarios que participaban en este ejercicio por parte de la Dirección General de la entidad, sin embargo, honrando el compromiso adquirido por la OCI con el Comité Institucional de Coordinación de Control Interno se desarrolló y concluyo la labor encomendada tal como se expone en el presente documento.

2. OBJETIVOS

2.1 Objetivo General.

Evaluar la implementación y adopción del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, para el fortalecimiento institucional y mejoramiento continuo del mismo.

2.2 Objetivos Específicos.

1. Revisar y evaluar los incidentes de indisponibilidad de las Soluciones Tecnológicas - ST de la DIAN, con el fin de realizar un diagnóstico integral que permita identificar las instancias afectadas, ubicaciones, causas que originaron la situación y las acciones implementadas para subsanar la misma.

2. Verificar la adopción y efectividad de las medidas para evitar la reiteración de las situaciones ocurridas de indisponibilidad de aplicativos de alto impacto para la misionalidad de la entidad.

3. Evaluar los componentes de Sistema de Control Interno - SCI, asociados con el Sistema de Seguridad y Privacidad de la Información, en relación con los aplicativos evaluados.

[1] Plan-Estrategico-Institucional-2026-V2.pdf

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

4. Fortalecer las actividades de fomento de la cultura de control para la mejora continua del proceso evaluado.

3. DESARROLLO DE LA AUDITORÍA

A partir de las fuentes de información, se realizaron verificaciones sobre las causas que dieron origen a eventos o incidentes de indisponibilidad total o parcial en las soluciones tecnológicas institucionales, las acciones implementadas y a la efectividad de las medidas adoptadas para evitar la reiteración de las situaciones ocurridas, en cumplimiento de las políticas de seguridad en el atributo de disponibilidad de la información, establecidos en el manual *"MN-IIT-0072 Manual de Políticas y Lineamientos de Seguridad y Privacidad de la Información V6*" y los lineamientos del Plan de Continuidad del Negocio - PCN.

Las dependencias auditadas responsables de la información aportada para verificación y análisis fueron: Oficina de Seguridad de la Información - OSI; Direcciones de Gestión de: Innovación y Tecnología - DGIT, Impuestos - DGI, Aduanas - DGA, Fiscalización - DGF, Estratégica y de Analítica - DGEA, Corporativa - DGC, Jurídica - DGJ y a las Direcciones Seccionales de Impuestos y de Aduanas – DSI y DSA Medellín, teniendo en cuenta los procedimientos "*PR-IIT-0454 Disponibilidad de la operación tecnológica V2*", "*PR-IIT-0458 Gestión de incidentes tecnológicos V3, PR-IIT-0504 Gestión de incidentes de seguridad de la información V1*" y protocolos asociados al PCN y considerando 45 Soluciones Tecnológicas - ST.

La selección de la muestra de las ST se efectuó, atendiendo los criterios de riesgos de seguridad digital de las matrices de gestión de los procesos evaluados y los riesgos registrados en la herramienta de Gobierno Riesgos y Cumplimiento – GRC para los activos de información, que impactan a los usuarios externos; de otra parte, para las direcciones seccionales visitadas se establecieron cómo resultado del análisis de los casos de indisponibilidad de las ST, registrados en comunicados de prensa, reportes de PQRSD, herramienta de soporte Aranda y por las contingencias declaradas, entre otras.

Producto del ejercicio auditor, se identificó la exposición a los riesgos de las matrices de los siguientes subprocesos:

- Innovación y Tecnología V3, R4. "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información*".
- Operación Logística V4, R3 "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad*"
- Asistencia al Usuario V2, R2 "*Canales de servicio institucionales con inconvenientes en términos de calidad y oportunidad en la atención*".
- "*Factura Electrónica y Servicios Digitales*" V1; R2 "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad*".
- Recaudo Devoluciones V5, R7 "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad*".
- Seguridad de la Información V2, R3. "*Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad, y disponibilidad de los datos*".

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

De otra parte, se evidencio la materialización de los riesgos[2] de las matrices: Subproceso Seguridad de la Información V2, R3. "*Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad, y disponibilidad de los datos*", (ST Agendamiento de citas (Digiturno) (marzo 2026), SYGA – Siglo XXI (segundo semestre 2023), SIEX (primer semestre 2025)) y del Subproceso de Innovación y Tecnología riesgo R1 "*Sistemas de información y servicios digitales indisponibles (no programada-fortuita) para las partes interesadas*" (ST SIEX (21 de marzo 2024), Servicios Aduaneros y Tributarios MUISCA (14 de abril de 2024)) y falla total en el hardware o software de comunicaciones afectando la conectividad en todas las sedes por configuración inadecuada (segundo semestre de 2023).

Lo anterior se evidencia en los cinco hallazgos que se relacionan a continuación:

Hallazgo 01. Indisponibilidad total o parcial en soluciones tecnológicas.
Hallazgo 02. Deficiencias en la gestión de eventos e incidentes de seguridad de la información y en la gestión de vulnerabilidades.
Hallazgo 03. Falencias en la gestión de activos de información y controles de seguridad y privacidad de la información.
Hallazgo 04. Deficiencias en la gobernanza, control de desarrollo y gestión de accesos en soluciones LCNC (Low-Code / No-Code).
Hallazgo 05. Falencias en la Gestión de la Continuidad del Negocio.

4. RELACIÓN DETALLADA DE HALLAZGOS

Como resultado de la auditoría fueron dadas a conocer las situaciones encontradas a los procesos auditados mediante correo del 05 de junio de 2026; frente a las cuales, los mismos ejercieron el derecho a la contradicción y a presentar observaciones; respuestas que fueron recibidas mediante correo electrónico[3], las cuales una vez analizadas por el equipo auditor, dieron lugar a la configuración de cinco (5) hallazgos.

Cabe anotar, que la auditoría basada en la valoración de riesgos atiende un modelo de gestión por procesos y los resultados muestran situaciones evidenciadas durante la misma.

Hallazgo 01. Indisponibilidad total o parcial en soluciones tecnológicas.

Analizadas 45 ST priorizadas frente a los objetivos de la auditoría, se evidenciaron las siguientes situaciones. (Ver anexo 1.)

A continuación, se presentan la tabla de referencia de cada una de las ST con una breve descripción de su funcionalidad.

[2] Fuente: Informes cuatrimestrales de gestión de riesgos en la vigencia 2023, 2024 y 2025, remitidos por la DGIT y la OCI en los formatos FT-PEC-2096 "*Informe de monitoreo de riesgos*" y FT-PEC-2097 "*Reporte materialización de riesgos*"
[3] OSI 100202252-300-2026 del 11/06/2026, DGC 12/06/2026, DGJ 100202208 – 1058, DGF 100202211_1311, DGEA 100202152 – 336 16/06/2026, DSA Medellín 17/06/2026, DGI 100202153-0831 18/06/2026, DGA 100202210_2838 y DGIT 100202154 – 344 del 19/06/2026

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

Tabla No 01. Relación de soluciones tecnológicas

Solución Tecnológica	Descripción funcionalidad
ADA WEB	ST que permite a la Subdirección Logística administrar, controlar, así como de disponer en forma eficaz y eficiente de las mercancías aprehendidas, decomisadas o abandonadas.
Bitácora	ST que permite el registro de trámites manuales, tanto para Importaciones como para Exportaciones.
CCC20 - Cuenta Corriente Contribuyente	ST que permite el cálculo y actualizan de los saldos de cada una de las obligaciones tributarias que los contribuyentes. Permite el procesamiento de los documentos que afectan el estado de las obligaciones tributarias y la consulta de los saldos.
SIPAC - Sistema de Información de Planeación y Administración de CARTERA	ST que permite llevar control de las deudas que tienen los contribuyentes por impuestos tributarios, controla la gestión del área de Cobranzas en cada una de las administraciones.
OBLIGA	ST que permite para dar cumplimiento a lo establecido en el numeral 2.1.6 Control de obligaciones no creadas en SIPAC del memorando 319 de 2017.
SISCOBRA	ST que permite registrar actuaciones del proceso de cobro, es la versión anterior a SIPAC. Entre SIPAC y candado son independientes, es decir los expedientes no pueden estar en candado y a la vez en Sipac, solo debe estar en uno de ellos.
Sistema de Agendamiento de Citas (Digiturno)	ST que permite administra el Control de Turnos y Agendamiento Citas DIAN.
Diligenciamiento	ST que permite a los contribuyentes la presentación vía Internet de sus declaraciones correspondientes a sus obligaciones Tributarias, Aduaneras y Cambiarias.
Factura Electrónica	ST adoptado a través del Decreto 2242 de 2015 que permite la masificación del uso de la factura electrónica en Colombia a través de la interoperabilidad entre quienes facturan electrónicamente y quienes adquieren bienes que son facturados por ese medio.
Sistema Integra	ST que permite la administración y trazabilidad del expediente virtual, desde que se abre hasta su culminación en el proceso de fiscalización y liquidación en materia tributaria, internacional y cambiaria.
Obligación Financiera	ST que permite el procesamiento de los documentos que afectan el estado de las obligaciones tributarias y la consulta de los saldos y movimientos detallados de los documentos con vigencias 2007 y posteriores.
SYGA - Siglo XXI	ST que permite realizar de forma automatizada los procesos de "Registro de Tránsitos Aduaneros" y "Nacionalización de Mercancías de procedencia extranjera o de zona franca".
Remate Virtual	ST que permite hacer de forma virtual los remates de los bienes de los contribuyentes a los cuales se les han embargado y que llegaron hasta esta etapa final de rematarlos.
SIEX - Sistema Estadístico de Comercio Exterior de la DIAN	ST que almacena la información consolidada de importaciones, exportaciones y balanza comercial para consulta de usuarios general.
Carrara y Ferrajoli	ST que se utiliza para el registro de los procesos penales de la Seccional incluyendo los datos desde la radicación de la denuncia hasta la terminación del proceso.
SIEPP	ST que administra la Información Electrónica para los procesos penales

Fuentes: Anexo "Roles de las soluciones tecnológicas" según procedimientos y procesos_V4_R029, Catálogo de Sistemas de Información Dian, 12/02/2026 – DGIT.

Respecto de las mismas se establece lo siguiente:

a. ADA Web. La infraestructura que soporta la ST "*ADA Web*" presenta brechas en la seguridad de la información y vulnerabilidades técnicas, debido a que el cliente opera en máquinas virtuales con un sistema operativo obsoleto, el cual carece de soporte del fabricante, sin protección de software antivirus ni la instalación del agente de gestión de TI Aranda. Mantener este activo expuesto en la red sin monitoreo, control de parches ni herramientas de defensa, genera un alto riesgo de incidentes de seguridad de la información, tales como: la infiltración de malware[4], accesos no autorizados, pérdida de integridad y confidencialidad de los datos procesados, y la posible propagación de amenazas hacia el resto de la red institucional. Responsable: DGIT - SD Logística.

[4] Programa maligno

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

b. Bitácora (ST de contingencia). Se identificaron deficiencias en la ST de contingencia "*Bitácora*", debido a su obsolescencia tecnológica y a la falta de integración con la ST principal SYGA - Siglo XXI, lo que interrumpe la trazabilidad por los trámites manuales. La herramienta presenta fallas recurrentes, restringe las consultas históricas a seis meses y así mismo, cuenta con un catálogo de causales desactualizado que obliga al uso masivo de la opción genérica *"Otras Causales",* distorsionando las estadísticas del negocio. Esta situación, sumada a la falta de alertas automáticas, la inexistencia de campos clave para el seguimiento y al incumplimiento general de las necesidades del negocio por parte de la plataforma principal, ha obligado a las Direcciones Seccionales de Aduanas como Medellín, a implementar registros complementarios de tipo manual en Excel; lo que genera riesgo de pérdida de integridad y trazabilidad de los datos, afectando la toma de decisiones y aumentado la carga operativa. Responsable: DGIT - SD Operación Aduanera.

c. CCC20 - Cuenta Corriente Contribuyente, SIPAC, OBLIGA, SISCOBRA. Se evidenció que las ST referenciadas, se vieron afectadas por un evento del 21/08/2025, que implicó indisponibilidad durante 16 minutos, debido a una falla eléctrica que impactó todos los anteriores servicios. Responsable: DGIT - SD Recaudo.

d. Sistema de Agendamiento de Citas (Digiturno). Se evidenció la ocurrencia de un evento de seguridad de la información en la ST Digiturno por exfiltración de datos, el cual no fue detectado por las herramientas de seguridad institucionales e implicó la declaración de contingencia desde el 03 hasta el 30 marzo de 2026, generando indisponibilidad de la herramienta. Además, se encontró documentación técnica sensible alojada en un equipo de un punto de atención al usuario en la DSI Medellín en visita realizada entre el 11 y 15 de mayo de 2026, el cual es utilizado por usuarios externos, pudiendo generar riesgo de fuga de información. Responsable: DGIT - SD Servicio al Ciudadano en Asuntos Tributarios.

e. Diligenciamiento. En mayo de 2025 se presentaron dos (2) eventos de indisponibilidad de los servicios informáticos de la DIAN, relacionados con las funcionalidades para presentar declaraciones, información exógena tributaria, pagos y servicios aduaneros gestionados en la Plataforma Muisca, el primero entre el 13 y el 23 de mayo y el segundo entre el 26 y 27 de mayo de 2025. También se reportan casos en la solución tecnología de soporte, evidenciándose fallas relacionadas con: errores en el ingreso, lentitud de la página, dificultades para la firma y formalización de los formularios. En cuanto a la disponibilidad, el promedio en algunos días del primer trimestre de 2026 muestra porcentajes por debajo de los ANS establecidos del 99.98% en los formularios[5]: F110, F490, F690, F310, F420, F350, F260 y F2593.

Por otro lado, la retención de logs se realiza hasta por tres (3) meses, incumpliéndose con los términos establecidos en el *"Manual MN-IIT-0072".* Responsable: DGIT - SD Recaudo.

f. Factura Electrónica. Verificadas las contingencias reportadas en portal web institucional para el periodo evaluado, las contingencias remitidas por la Subdirección de Factura Electrónica y Soluciones Operativas - SFESO, los Formatos "*FT-IIT-2714 Bitácora de eventos*" 2024 y 2025, los casos de soporte registrados en ARANDA y los de desarrollo registrados en la herramienta DevOps, el reporte de denuncias, las Actas de Comité de

[5] https://www.dian.gov.co/atencionciudadano/formulariosinstructivos/Paginas/default.aspx

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

Cambios, el reporte sobre disponibilidad archivo *"I_1_a_Anexo 04 - Indicadores_DIAN_Agosto_2023"* y el reporte de PQRSD, se evidencian falencias que ocasionan facturación sin validación previa por parte de la DIAN, requiriendo la transmisión una vez se restablece el servicio por indisponibilidad o contingencia en la ST Factura Electrónica, las cuales se originaron principalmente por las siguientes causas: fallas por ajustes al sistema, errores en la validación de CUFE - Código Único de Factura Electrónica o documentos y lentitud en la validación.

Adicionalmente, se identificó un problema de contingencia por fallo regional en el proveedor de los servicios de nube que se prolongó por 78 horas, esto según el registro remitido por la SFESO, con lo publicado en el portal Web Institucional, incidente que ocasionó la generación de facturas electrónicas sin validación previa por parte de la DIAN, requiriendo la transmisión finalizada la contingencia.

Por último, es importante resaltar que el servicio de Facturación Electrónica no cuenta actualmente con un esquema de alta disponibilidad regional total, lo que ocasiona la exposición a un riesgo de indisponibilidad o intermitencias y se afecte la validación de la facturación electrónica y consecuentemente al usuario final.

De otra parte, durante el periodo evaluado la SFESO informó que el volumen de registros producto de las contingencias, superó los 300 millones. Responsable: DGIT - SFESO.

g. Sistema Integra. Verificadas las contingencias reportadas para las ST en el portal web institucional durante el periodo evaluado, incluidos el formato *"FT-IIT-2714 Bitácora de eventos"* de 2024 y 2025, los casos de soporte registrados en ARANDA, los de desarrollo registrados en la herramienta DevOps, el reporte de actos administrativos generados por contingencia de la ST Integra, las Actas de Comité; así como, la información recopilada en visita a la DSI Medellín, se evidenciaron falencias en la ST Integra, que obligaron por contingencia a gestionar información de actos administrativos de manera manual.

Las anteriores situaciones se originaron principalmente por las siguientes causas:

- Problemas de acceso derivados por deficiencia en la gestión y oportunidad en la asignación de roles informáticos.
- Fallo en diferentes funcionalidades de la ST y ausencia de estas (Ej. fiscalización internacional, precios de transferencia, actos no disponibles) o desactualización de la ST.
- Fallas en la infraestructura de telecomunicaciones o en las bases de datos a nivel nacional.

Adicionalmente, se identificaron problemas con los contextuales con la herramienta OpenOffice: entre ellos eliminación de datos (ej. impuesto y número del programa), falta de estandarización de los formatos (tipo de letra, disposición de márgenes), problema al abrir la herramienta, repetición de filas del formato en la tabla (ej. requerimiento especial tabla "*Modificar Propuesta*"), documento contextual con datos incorrectos, los cuales se corrigen únicamente en la herramienta ocasionando inconsistencias en los datos en la base de datos, contextual que cuando supera más de 25 hojas genera error en el cargue de la

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

información mostrando hojas en blanco, falencia en la notificación de actos cuando se marca la casilla de apoderado debido a que no se notifica a la empresa; en el pliego de cargos el sistema borra los campos en el 90% de los casos, en la sección "*sanción no pecuniaria*", los cuales deben ser diligenciados nuevamente por el funcionario.

Por otro lado, el promedio de disponibilidad en algunos días del primer trimestre de 2026 muestra porcentajes por debajo de los ANS establecidos del 99.98%, bajando hasta el 33,33%. Responsable: DGIT - SD Fiscalización Tributaria.

h. Obligación Financiera. Se presentan errores identificados con el número 500 (error de servidor) en la ST Obligación Financiera y casos de fallas en el procesamiento de pagos formulario 490 que no afectan la Obligación, generando saldos irreales para el contribuyente; ajustes que dependen de los desarrollos tecnológicos sujetos a priorización por el área responsable. Situaciones que fueron evidenciadas en visita a la DSI Medellín.

Adicionalmente, se observó el incumplimiento de ANS's en el primer trimestre de 2026, con porcentajes inferiores al 99.98% y para los otros periodos (2023, 2024, 2025) no suministraron reportes. Responsable: DGIT - SD Recaudo.

i. Solución Tecnológica SYGA - Siglo XXI. Se evidenció la generación de contingencia en la plataforma SYGA - Siglo XXI posterior a las actualizaciones de la ST, por una falta de pruebas exhaustivas de carga y estrés, previo a la puesta en producción de las actualizaciones realizadas el 15 noviembre de 2023, generándose desde el 20 de noviembre del mismo año hasta el 10 de enero de 2024, con indisponibilidad de funcionalidades que durante los 50 días afectaron al usuario final.

Así mismo, se observó ocurrencia de errores en la ST SYGA - Siglo XXI, reportados en visita en la DSA Medellín, con mensajes genéricos del tipo "*Error Sistema. Se presentó un error inesperado en el sistema (...) intente nuevamente*", lo que no permite determinar las causales del mismo ni orientación al usuario final sobre cómo proceder ante estos e impiden, continuar con el flujo normal del proceso por lo que se debe gestionar como trámite manual en la ST Bitácora, afectando la trazabilidad de la información.

Por otro lado, en el primer trimestre de 2026, se evidenció incumplimiento de los ANS's con porcentajes inferiores al 99.98%. para los demás periodos (2023, 2024, 2025) no fueron suministrados reportes, lo que incumple lo establecido el "*Manual MN-IIT 0072*". Responsable: DGIT - SD Operación Aduanera.

j. Remate Virtual. Se evidenciaron 30 casos de error asociados a la ST Remate Virtual, los cuales fueron registrados desde septiembre de 2022 y a la fecha de la auditoria no se evidenciaron soluciones definitivas.

Adicionalmente, durante los meses de enero a marzo de 2026, se evidenciaron incumplimientos de los ANS'S, con porcentajes inferiores al 99.98%. Responsable: DGIT - SD Recaudo.

k. SIEX. Durante el periodo evaluado se evidenció que la ST SIEX, presentó indisponibilidad en tres ocasiones así: en el 2024 una con duración de 7 horas, otra de 6:02 horas en las

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

que fue necesario el reinicio del servidor virtual para el restablecimiento de los servicios, situación asociada a la obsolescencia del servidor de aplicaciones web que, además, funciona en un sistema operativo para el cual ya finalizó la vida útil; por lo tanto, no tiene soporte del fabricante y la del 21/08/2025 con duración de 16 minutos ocasionada por falla eléctrica que afectó a todos los servicios. Responsable: DGIT - SD Estudios Económicos.

l. Carrara, Ferrajoli, SIEPP. Falencias en los aplicativos ("*Carrara*" y "*Ferrajoli*" no corporativos) que apoyan la gestión de los procesos penales de la entidad, debido a que se encuentran obsoletos y la ST desarrollada en la plataforma MUISCA en 2021 para su reemplazo, denominado Sistema de Información Electrónica para Procesos Penales (SIEPP) quedó inconcluso, limitando su alcance únicamente a la fase de radicación de la denuncia. Esta situación impide registrar el avance de las denuncias finalizadas o que continúan en etapas posteriores en el SIEPP, obligando a los funcionarios a realizar un doble registro de la información en ambas plataformas; lo que afecta la trazabilidad del proceso, distorsiona las estadísticas institucionales y aumenta la carga operativa por duplicidad en el registro o reprocesos. Responsable: DGIT - DG Jurídica.

m. Incumplimiento de ANS. De las 45 ST objeto de auditoría, para 20 no se suministraron reportes de disponibilidad diaria, para cinco el reporte suministrado no permite determinarla y para las restantes, se tienen los siguientes resultados con porcentajes promedio diarios inferiores al 99.98% establecidos en los ANS's:

Tabla No 02. Porcentaje diario de ANS's de soluciones tecnológicas

Solución Tecnológica - ST	% Incumplimiento ANS
Carga Masiva	18%
Certificados del proveedor	13%
Declaración Andina de Valor	10%
Denuncias de Fiscalización	10%
Flujo De Documentos	8%
Garantías	11%
Identidad	50%
Importaciones Carga	25%
Selectividad aduanera	32%
Numeración de facturación	41%
RUT	84%
Tránsito Aduanero	10%
SINOT	13%
PROFIA	7%
RUB	25%

Fuente: Respuesta solicitud No. 11 por parte de la DGIT dentro del ejercicio auditor.

n. Gestión documental electrónica. Falta de firmas digitales para la totalidad de responsables que permitan la gestión electrónica de todos los actos administrativos, conllevando a que se deba hacer un manejo documental híbrido, por la falta de una ST de gestión documental institucional, que permita la conformación integral del expediente electrónico, debiéndose hacer uso de diferentes herramientas ofimáticas como el correo electrónico, documentos gestionados en algunos casos en buzones personales y otros en los buzones de las oficinas o en carpetas compartidas en SharePoint, lo que dificulta la trazabilidad de la información y la estandarización de la documentación electrónica a nivel

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

nacional. Responsable: DGIT.

Tabla No. 03. Elementos del hallazgo 01

Criterios	Directiva Presidencial No. 02 de 2022, directrices: No. 3. Estrategia de seguridad digital; No. 4. Servicios en nube; No. 5 Gestión efectiva de riesgos; No.12 Continuidad del negocio; No. 14. Monitoreo permanente a la infraestructura; No. 17. Actualizaciones de seguridad del software liberadas por los fabricantes; No. 18. Acceso remoto; y los Lineamiento "*5.23 Seguridad de la Información para el uso de servicios en la nube*"; "*5.33 Protección de registros*"; "5.34 Privacidad y *protección de los datos personales*"; "*8.15 Registro*" del "*Manual MN-IIT-0072 V6*", literal H, artículo 4 de la Ley 594 de 2000 del Archivo General de la Nación.
Dimensiones MIPG	Dimensión 3 "*Gestión con Valores para Resultados*" en las políticas: "*Gobierno Digital*" y "*Seguridad Digital*".
Causas	Obsolescencia y ausencia de un esquema de mantenimiento, soporte y actualización periódico de las soluciones tecnológicas, situación que limita su adaptación a las necesidades institucionales, no se cuenta actualmente con un esquema total de alta disponibilidad regional para FE. Ausencia de una solución tecnológica que se consolide la gestión documental de la entidad.
Efectos	Exposición a incidentes de ciberseguridad debido al aprovechamiento de vulnerabilidades y brechas de seguridad no mitigadas en las plataformas; asimismo, se generan restricciones y limitaciones en el acceso oportuno a la información; afectación en la prestación de servicios; alteración en la operación; afectación de la imagen institucional.
Riesgos	Exposición a los riesgos: R4. "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información*", del subproceso Innovación y Tecnología V3; R3 "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad*" de la matriz de riesgos del subproceso Operación Logística V4; R2 "*Canales de servicio institucionales con inconvenientes en términos de calidad y oportunidad en la atención*" de matriz de riesgos del subproceso "Asistencia al Usuario" V2; R2 "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad*" de la matriz de riesgos del subproceso de "*Factura Electrónica y Servicios Digitales*" V1; R7 "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad*" de la matriz de riesgos del subproceso de Recaudo Devoluciones V5. Materialización del riesgo R3. "*Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad, y disponibilidad de los datos*", del subproceso Seguridad de la Información V2. (ST Agendamiento de citas (Digiturno) (marzo 2026), SIGLO XXI, SIEX (primer semestre 2025)). Materialización del riesgo R1 "*Sistemas de información y servicios digitales indisponibles (no programada-fortuita) para las partes interesadas*" de la matriz de riesgos del subproceso de Innovación y Tecnología (ST SIEX (21/03/2024), Servicios Aduaneros y Tributarios MUISCA (14/04/2024)); falla total en el hardware o software de comunicaciones afectando la conectividad en todas las sedes por configuración inadecuada (segundo semestre de 2023).
	Exposición al riesgo digital "*Pérdida de Disponibilidad*" identificados, registrados y aprobados en el Sistema GRC, de la siguiente manera: **Software** - Afectación por vulnerabilidades en el Software (OWASP[6] 2017 Top 10: inyección código, pérdida autenticación, exposición datos sensibles, referencias entidades externas, pérdida control de acceso, incorrecta configuración de seguridad, etc.) pueden causar afectación por abuso de privilegios de acceso a software causando pérdida de disponibilidad a los Servicios Informáticos de Normalización de Saldos, Normaliza Cuenta Corriente, Siscobra Aduanero, Siscobra Candado, Obliga, SIPAC, CCC20 (Cuenta Corriente Contribuyentes), Corrección de inconsistencias, Diligenciamiento, Gestión Masiva, Obligación Financiera. - Fallas en el funcionamiento del software derivadas de migraciones o actualizaciones de sistemas operativos (nuevas versiones), pueden ocasionar errores en el equipo, caída del sistema por agotamiento de recursos, fallas en el procesamiento, modelamiento inadecuado o visualización incorrecta de datos en procesos analíticos, afectando la disponibilidad del SI Tránsito Aduanero. - La inadecuada gestión de capacidad del sistema puede facilitar la caída del sistema por agotamiento de recursos o denegación de servicio lo cual causaría la pérdida de disponibilidad del Servicio Digital Registro Único Tributario (RUT)

[6] Open Web Application Security Project

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

	- Mal funcionamiento del software por migración o actualización de sistemas operativos (nuevas versiones de software) pueden causar caída del sistema por agotamiento de recursos causando pérdida de disponibilidad de los activos de información Sistema de Factura Electrónica. - Mal funcionamiento del software por migración o actualización de sistemas operativos (nuevas versiones de software), puede causar fallas o mal funcionamiento del equipo, caída del sistema por agotamiento de recursos o falla, inadecuado modelamiento o visualización errónea de datos en los procesos de analítica, generando la pérdida de disponibilidad del SIEX Plan Vallejo MUISCA.
	Información - La inadecuada aplicación de los procesos de gestión del cambio en el software puede conllevar a la denegación del servicio, ocasionando pérdida de disponibilidad al activo de información SIGLOXXI- COMEX (importaciones). - Desactualización del Plan de Continuidad del Negocio (PCN) o la deficiencia en su implementación incrementa la probabilidad de sufrir una pérdida de la disponibilidad de activos ante cualquier evento disruptivo mayor, como ciberataques, interrupción del suministro eléctrico o afectación grave de instalaciones y personal. Base de datos del Registro Único Tributario (RUT). - El incumplimiento de las políticas, lineamientos, normas o procedimientos de seguridad de la información o de protección de datos personales en los procesos de recolección, almacenamiento, acceso y uso de los datos personales, circulación y disposición final de los datos, genera perdida de afectación de la información por errores de los usuarios, fuga de información intencional y eliminación no autorizada de información relacionada con datos personales, lo cual causaría perdida de disponibilidad en el activo de informes de selectividad Aduanera. - Insuficientes o inadecuados controles en materia de protección de información o datos electrónicos; clasificados, reservados o personales que se almacenan o transfieren al interior de la entidad pueden causar fuga de información, falla por errores de monitoreo (log), utilización no previsto o no permitido de datos o información, causando pérdida de disponibilidad en las Bases de datos de Obligación Financiera, Gestión Masiva, Corrección de Inconsistencias, Normalización de Saldos, Cuenta corriente contribuyentes, Normaliza Cuenta Corriente, Títulos de Deposito Judicial, SIPAC, Siscobra Aduanero, Obliga y Diligenciamiento. - La inadecuada aplicación de los procesos de gestión del cambio en el software pueden conllevar a la denegación del servicio, ocasionando la pérdida de disponibilidad al activo de información Sistemas de información MUISCA - Garantías, Importación Temporal de Medios de Transporte de Turistas (sistema de información Azure), MUISCA - Carga Importaciones, MUISCA - Salida de mercancías. - Los procedimientos para el monitoreo de capacidad y rendimiento inadecuados pueden causar denegación de servicio y generar perdida de disponibilidad del activo de información exógena tributaria.

Fuente: Elaborado por el equipo auditor.

Recomendaciones específicas frente Hallazgo 01:

- Implementar mecanismos para la retención de logs con un tiempo mínimo de un año atendiendo el lineamiento "*5.33 Protección de registros*" y "*8.15 Registro*" del "*Manual MN-IIT-0072 V6*".
- Realizar mantenimiento periódico a las ST; así como, renovación de sistemas operativos y de software base sobre el que operan.
- Revisar las actividades para la gestión de cambios de software, que estén ocasionando indisponibilidad o denegación del servicio en producción, en el marco del Procedimiento *"PR-IIT-0457 – Habilitación de Cambios de TI".*

Hallazgo 02. Deficiencias en la gestión de eventos e incidentes de seguridad de la información y en la gestión de vulnerabilidades.

Responsable: Oficina de Seguridad de la Información - OSI.

a. La OSI cuenta con las herramientas, tales como: SIEM y Firewall de bases de datos y

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

realiza monitoreos, entre otros a: vulnerabilidades de Bases de Datos, transacciones anómalas, tráfico de red; sin embargo, recopila datos de pocas fuentes, desaprovechándose insumos importantes como: logs de auditoría de bases de datos, logs de servidores de aplicaciones, de las herramientas de seguridad administradas por la DGIT, que favorecerían la correlación de eventos y la prevención proactiva frente a amenazas y vulnerabilidades; además, el análisis se realiza de forma esporádica dependiendo de la disponibilidad de tiempo de los dos (2) funcionarios a cargo, quienes además, tienen asignados otros asuntos propios de la OSI.

b. La identificación de vulnerabilidades es limitada, la herramienta de gestión establecida para tal fin en la matriz de riesgos del Subproceso de Seguridad de la Información V.3 se observó en etapa de configuración; por lo tanto, no se ha hecho uso de la misma, además presenta problemas de actualización de componentes y los funcionarios a cargo no han recibido capacitación especializada para la configuración y uso de ésta. No obstante, se lleva un registro de vulnerabilidades desde finales de 2025 en la herramienta GRC, con dependencia de la información de entes externos o comunicados a través de grupos de interés, a manera de bitácora; sin embargo, no se evidenció trazabilidad documentada de la gestión de las mismas en dicha herramienta.

c. El proyecto SOC a la fecha de respuesta a las situaciones se informó que, se encuentra en etapa de evaluación de ofertas. Se evidencia que es una solución a largo plazo y que depende del avance del proceso de contratación.

Tabla No. 04. Elementos del hallazgo 02.

Criterios	Directiva Presidencial No. 02 de 2022, directrices: No. 5 Gestión efectiva de riesgos; No. 6. Grupo de Seguridad Digital; No. 7. Procedimiento de incidentes; No. 14. Monitoreo permanente a la infraestructura. Lineamientos: "*5.7 Inteligencia de amenazas*"; "*5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información*"; "*5.25 Evaluación y decisión sobre eventos de seguridad de la información*"; "*5.26 Respuesta a incidentes de seguridad*"; "*5.27 Aprendiendo de los incidentes de seguridad de la información*" del *"Manual MN-IIT-0072 V6.", "Anexo 4 Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas" de Mintic 2018.*
Dimensiones MIPG	Dimensión 3 "*Gestión con Valores para Resultados*" en las políticas: "*Gobierno Digital*" y "*Seguridad Digital*".
Causas	Insuficiente capacitación en la instalación, configuración y uso de la herramienta de gestión de vulnerabilidades; falta de un equipo de trabajo con dedicación exclusiva a la ejecución de todo el ciclo de la gestión de incidentes y vulnerabilidades; falta de una mayor articulación con la DGIT, área que administra las herramientas fuente de información; falta de completitud scripts con la respectiva parametrización para la recopilación de datos en la herramienta SIEM que permita la correlación de eventos; desaprovechamiento de la información capturada por herramientas de seguridad (TVO, IDS/IPS, logs de servidores de aplicación y bases de datos; inoportuna renovación de licencias de la herramienta SIEM por falta de presupuesto.
Efectos	Afectación en la visibilidad por parte de la entidad de las amenazas y vulnerabilidades a la que se puede estar expuesta; respuesta tardía ante la explotación de vulnerabilidades; afectación de la imagen institucional.
Riesgos	Exposición a los riesgos: R4. "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información*", del Subproceso Innovación y Tecnología V3 y R3. "*Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad, y disponibilidad de los datos*", del Subproceso Seguridad de la Información V2.

Fuente: Elaborado por el equipo auditor.

Recomendaciones específicas frente Hallazgo 02:

- Implementar la funcionalidad de la herramienta de identificación de vulnerabilidades y capacitar a los funcionarios en la configuración y manejo de la misma.

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

- Ampliar las fuentes de información y realizar una correlación de eventos con mayor alcance para la profundidad del análisis.
- Mejorar la documentación, trazabilidad y seguimiento de la bitácora en la herramienta GRC en el registro de las vulnerabilidades.
- Realizar oportunamente las solicitudes de presupuesto requerido, para gestionar la actualización y soporte del licenciamiento SIEM, para garantizar su operación futura.

Hallazgo 03. Falencias en la gestión de activos de información y controles de seguridad y privacidad de la información.

Frente a la gestión de activos, se evidenciaron las siguientes situaciones:

a. Máquinas virtuales. De 174 máquinas virtuales identificadas instaladas en equipos de funcionarios para la operación de aplicativos antiguos, se reportó durante la ejecución de la auditoría la eliminación de 20 que no fueron identificadas; 31 no soportan la instalación de antivirus ni agente de monitoreo de recursos; 21 presentan errores en la instalación del agente; se suministró la hoja de vida de 85 máquinas virtuales, de las cuales coinciden 70 con el reporte enviado para la validación; evidenciándose falta de controles sobre las mismas, lo que genera riesgos de seguridad para la información y limitaciones para el adecuado monitoreo. Responsable: DGIT. (Ver anexo 2.)

b. Software base sin soporte del fabricante. ST que operan con licencias que no cuentan con soporte del fabricante por finalización de la vida útil, tales como: sistemas operativos, motores de bases de datos, navegadores web y herramientas de desarrollo. Responsable: DGIT. (Ver anexo 3.)

c. Equipos encendidos en horarios no laborales sin justificación de la necesidad. De un universo de 2.699 equipos reportados por la DGIT identificados encendidos en horarios habitualmente no laborales, se seleccionó una muestra de 347 pertenecientes a 10 Subdirecciones del Nivel Central y dos (2) Direcciones Seccionales, de las cuales el 17 %, justificó la necesidad; el 3.7% indicó que el equipo o el funcionario ya no hacía parte del área y el 69,7% indicó no requerir dejarlo encendido; sin embargo, en donde se manifiesta la necesidad, en algunos casos se indica que, el equipo de soporte técnico dio dicha instrucción para realizar actualizaciones o se realiza conexión remota por TVO, no se aportaron evidencias. Cabe aclarar, que dos Subdirecciones no dieron respuesta a la solicitud dentro del término requerido (33 equipos). Responsable: DGIT-DGI-DGA-DGF-DGEA-DGC-DGJ-DSI Medellín y DSA Medellín. (Ver anexo 4.)

d. Datacenter (NC) y cuartos de comunicaciones (NL). En el datacenter visitado de la DIAN, se evidenció: un sólo funcionario operador por cada turno, quien debe monitorear simultáneamente varias pantallas, las cuales generan diferentes tipos de alertas, lo que puede resultar insuficiente para las necesidades de la entidad; la distancia entre los datacenter puede poner en riesgo la seguridad de la información ante potenciales catástrofes, debido a la cercanía entre estos; los logs de auditoría del sistema de accesos a los datacenter, tienen un tiempo de retención de 3 meses, incumpliendo con las políticas de seguridad de la información que establece mínimo un año según el *"Manual MN-IIT-0072 V6*" y falta de señalización que indique la prohibición del consumo de alimentos, bebidas o fumar en el interior del mismo. Responsable: DGIT - DGC.

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

En cuanto a los cuartos de comunicaciones de las Direcciones Seccionales DSI y DSA Medellín, se identificaron brechas en su infraestructura, tales como: falta de sensores de temperatura y humedad, no se cuenta con planta eléctrica, el aire acondicionado se percibe insuficiente en uno de los cuartos y no se observaron cámaras de seguridad internas. Asimismo, a nivel administrativo y de control de accesos faltan bitácoras en donde se registre el ingreso del personal a los cuartos y falta de señalética de identificación y prohibición de consumo de alimentos o de fumar; y en el cuarto principal de las dos direcciones seccionales, además de los elementos de comunicación y servidores de aplicaciones legacy, se utiliza como bodega de almacenamiento de otros elementos como computadores portátiles, sin división o aislamiento entre las áreas. Responsable: DGC-DSI Medellín - DSA Medellín.

e. Falta de licencias de software. En la DSI y DSA Medellín, se evidenciaron la falta de 21 licencias de la Suite Office 365 para cubrir las necesidades de dichas áreas, cuya solicitud se realizó a través del Sistema de Soporte, encontrándose en estado suspendido, solo dos casos tienen el estado solucionado, situación que afecta el adecuado desempeño de las funciones de los funcionarios. Responsable: DGIT. (Ver anexo 5.)

f. Se observaron documentos con datos personales (números de identificación, nombres, firmas, correos electrónicos, direcciones, teléfonos) abandonados en impresoras y papeleras de reciclaje. Responsable: DSI - DSA Medellín.

g. Se evidenciaron equipos desatendidos sin bloqueo de pantalla. Responsable: DSI - DSA Medellín.

h. Se presentó indisponibilidad de servicios por inoportuna actualización de la clave en un componente tecnológico, ante la separación del cargo de un exfuncionario. Responsable: DGIT.

i. El equipo de cómputo del laboratorio de la DSA Medellín (placa 305297) opera con un sistema operativo antiguo, sin soporte del fabricante y presenta fallas técnicas que ponen en riesgo el proceso que apoya el software especializado instalado en el mismo. Responsable: DGC - SD Administrativa - DSA Medellín.

Tabla No. 05. Elementos del hallazgo 03

Criterios	Directiva Presidencial No. 02 de 2022, directrices: No.2. Catálogos; No. 3. Estrategia de seguridad digital; No. 4. Servicios en nube; No. 5 Gestión efectiva de riesgos; No.12 Continuidad del negocio; No. 13. Backups; No. 14. Monitoreo permanente a la infraestructura; No. 17. Actualizaciones de seguridad del software liberadas por los fabricantes; No. 18. Acceso remoto. Lineamientos: 6.3 Concientización, educación y capacitación en seguridad de la información"; "7.7 Escritorio y pantalla despejados"; "*8.8 Gestión de vulnerabilidades técnicas*"; "*8.19 Instalación de software en sistemas operativos*" del *"Manual MN-IIT-0072 V6."*
Dimensiones MIPG	Dimensión 3 "*Gestión con Valores para Resultados*" en las políticas: "*Gobierno Digital*" y "*Seguridad Digital*".
Causas	Falta de: Renovaciones tecnológicas; Fortalecimiento de los valores éticos relacionados con el cuidado de lo público; Identificación del número de licencias de la Suite de Office 365 requeridas para cubrir las necesidades de la entidad; fortalecimiento en la sensibilización de las políticas de seguridad y privacidad de la información.
Efectos	Exposición a riesgos de seguridad y privacidad de la información; afectación de la imagen institucional; desgaste de las máquinas, pago de mayores costos en el servicio de energía, aumento de la huella de carbono, contaminación ambiental.

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

Riesgos	Exposición a los riesgos: R4. "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información*", del Subproceso Innovación y Tecnología V3 y R3. "*Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad, y disponibilidad de los datos*", del Subproceso Seguridad de la Información V2.

Fuente: Elaborado por el equipo auditor.

Recomendaciones específicas frente Hallazgo 03:

- Implementar políticas de Directorio Activo para el apagado de equipos de cómputo (Computadores de escritorio y equipos portátiles) de manera automática durante horarios no laborales, teniendo en cuenta las excepciones a que haya lugar.
- Implementar mecanismos de liberación con clave en las impresoras de la entidad, con el fin de tener un mejor control de los documentos y mayor protección de datos personales.
- Realizar un análisis de necesidades de licencias de la Suite de Oficina y de monitoreo y realizar las gestiones a que haya lugar, para cubrir el número de usuarios que requieren hacer uso de esta.
- Considerar los riesgos a los que se expone la información institucional, al hacer uso de licencias de software sin soporte del fabricante.
- Fortalecer a los funcionarios en el conocimiento de las políticas de seguridad de la información y en el cuidado de lo público.
- Realizar en Aranda la actualización de la información de computadores con nombres de usuarios, ubicación física de funcionarios en el área correspondiente.

Hallazgo 04. Deficiencias en la gobernanza, control de desarrollo y gestión de accesos en soluciones LCNC (Low-Code / No-Code).

Se reportó la existencia de un inventario descentralizado de 1.247 desarrollos de bajo código o sin código (LCNC)[7] a nivel nacional, de los cuales 235 dan acceso a más de un funcionario, construidas en Power Platform y Power BI y de estas, 31 pertenecen a la DSI Medellín (solo 6 en producción) y una en construcción en la DSA Medellín.

De otra parte, en un segundo listado, sólo se relacionaron 1.020 soluciones; sin embargo, no se suministró por parte de la DGIT, la información requerida relacionada con: Descripción, objetivo, datos almacenados, módulos, funcionalidades, tipo de uso (Interno/Externo), fechas de aprobación y de puesta en producción, registro en la RNDB (en caso de almacenar datos personales), integración con Directorio Activo y continuidad del negocio.

Las herramientas LCNC, operan sin clasificación ni separación técnica de ambientes (desarrollo, pruebas y producción) y en algunos casos, permiten el acceso directo a datos extractados de ambientes de producción para generar reportes.

Aunque existe un documento de lineamientos para las herramientas LCNC, no se observa incorporado en el Listado Maestro de Documentos ni en las tipologías documentales establecidas por la entidad. Responsable: DGIT. (Ver anexo 6.)

[7] Low-Code permite cierta intervención con código, mientras que No-Code no requiere programación alguna

Tabla No. 06. Elementos del hallazgo 04

Criterios	Normativa y las regulaciones aplicables a la entidad, Lineamientos "*5.33 Protección de registros*", "*6.6 Acuerdos de confidencialidad y no divulgación*"; "*8.25 Ciclo de vida de desarrollo seguro"; "8.26 Requisitos de seguridad de la aplicación*"; "*8.28 Codificación segura*"; "*8.31 Separación de los entornos de desarrollo, prueba y producción*" del *"Manual MN-IIT-0072 V6."*
Dimensiones MIPG	Dimensión 3 "*Gestión con Valores para Resultados*" en las políticas: "*Gobierno Digital*" y "*Seguridad Digital*".
Causas	Falta de definición normativa en los marcos de control de la DGIT y la OSI frente a las nuevas tecnologías de desarrollo ciudadano (LCNC); situación que ha impedido la formalización de un proceso de gobernanza obligatorio, la asignación de responsabilidades y la definición de perfiles de acceso restringidos para salvaguardar los datos sensibles del negocio.
Efectos	Exposición a incidentes de ciberseguridad debido al aprovechamiento de vulnerabilidades y brechas de seguridad no mitigadas en la plataforma; fuga de información sensible y riesgos en la continuidad del negocio ante la desvinculación de personal; pérdida de la trazabilidad de la información y falta de control frente a la información extractada de los esquemas de bases de datos de producción.
Riesgos	Exposición a los riesgos: R4. "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información*", del Subproceso Innovación y Tecnología V3 y R3. "*Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad, y disponibilidad de los datos*", del Subproceso Seguridad de la Información V2.

Fuente: Elaborado por el equipo auditor

Recomendaciones específicas frente Hallazgo 04:

- Incorporar los lineamientos frente a las nuevas tecnologías de desarrollo ciudadano LCNC en el listado maestro de documentos.
- Formalizar el proceso de gobernanza y control de los aplicativos con asignación de responsabilidades y la definición de perfiles de acceso, restringido para la salvaguarda de los datos sensibles de la entidad.
- Elaborar el inventario detallado de las soluciones LCNC con la información mínima de descripción, objetivo, datos almacenados, módulos, funcionalidades, tipo de uso (Interno/Externo), fechas de aprobación y de puesta en producción, registro en la RNDB (en caso de almacenar datos personales), integración con Directorio Activo y continuidad del negocio.

Hallazgo 05. Falencias en la Gestión de la Continuidad del Negocio.

Responsable: DGEA - Subdirección de Procesos - SP

Se evidencian falencias en la Gestión de la Continuidad del Negocio, puesto que, pese a que la DIAN cuenta con documentos, entre otros: Plan de Continuidad del Negocio con referencia a la norma NTC-ISO 22301:2019, Protocolos relacionados con manejo de Incidentes y de Crisis; Plan de Recuperación de Desastres - DRP; sin embargo, estos no se encuentran estructurados en el marco de un Sistema de Gestión, observándose las siguientes situaciones:

- La DIAN cuenta con el "*Código de Buen Gobierno*", en donde se establecen las políticas institucionales y los documentos mencionados anteriormente; sin embargo, no se observa una política específica de continuidad del negocio, según lo establece el requisito "*5.2 Políticas*" de la norma NTC-ISO 22301:2019; no obstante, en las Políticas de: "*Administración de Riesgos*" y de "*Seguridad y Privacidad de la Información*", se hace mención en diferentes apartes sobre la contribución de estas para la continuidad del negocio.

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

- Se establecen responsabilidades en los documentos de protocolos: *“OD-PEC-0002 Protocolo de gestión de comunicaciones en momento de crisis”*, *“OD-PEC-0003 Protocolo de manejo de incidentes e identificación de crisis*”, “*OD-PEC-0004 Protocolo de manejo de crisis”*; sin embargo, falta claridad en la asignación de roles y responsabilidades en el Plan de Continuidad del Negocio.

- En las Tablas de Retención Documental - TRD, se encuentra establecida la serie "*037 Planes*" y subserie "*012 Planes de Continuidad del Negocio*" que contiene los tipos documentales: "*Protocolo de Manejo de Crisis, Escenarios de riesgos de continuidad, Estrategias para continuidad de negocio y Protocolo de Manejo de Incidentes e Identificación de Crisis*" de la Subdirección de Procesos; no obstante, no se observaron en dicha TRD ni en las de otras dependencias, las series y/o subseries referentes a la documentación producto de las mesas de incidentes y de los Puestos de Mando Unificado - PMU ni en dónde deben reposar, como por ejemplo, el "*Reporte de incidentes FT-PEC-2843*".

- Se observa en los activos de información publicados en el micrositio de "*Transparencia*" los "*Documentos Plan de Continuidad de Negocio y las estrategias respectivas - SP*" y "*Documentos de análisis y soporte para el Plan de continuidad de negocio - SP*", pero no se observan los referentes a la documentación producto de las mesas de incidentes y PMU.

- No se evidenció la existencia de un repositorio unificado en donde se recopile la documentación de los incidentes y/o crisis ocurridas, los balances postcrisis; quedando dispersas en las diferentes áreas que asumen el liderazgo, situación que dificulta la trazabilidad de las mismas.

- Se evidenció desconocimiento del PCN y falta de socialización y sensibilización en los temas relacionados con la continuidad del negocio, pese a estar establecido en el PCN, en el compromiso con la mejora continua, no se evidenciaron ejercicios al respecto.

- Se identificaron 14 comunicados informando eventos de contingencia, pero sólo se suministraron actas de un PMU del evento relacionado con la plataforma Muisca de agosto de 2024. De los 13 restantes no se aportaron actas de mesa de incidentes ni de PMU y en las suministradas, no se evidenció la responsabilidad de la Secretaría Técnica.

- Se informó sobre un incidente presentado con la ST RUT y las dos actas aportadas, no se formalizaron con las firmas respectivas.

Tabla No. 07. Elementos del hallazgo 05

Criterios	Directiva Presidencial No. 02 de 2022, directrices: No. 5 Gestión efectiva de riesgos; No.12 Continuidad del negocio; *"5.29 Seguridad de la información durante la interrupción"*; *"5.30 Preparación de las TIC para la continuidad del negocio"* y *"8.14 Redundancia de las instalaciones de procesamiento de información" del Manual MN-IIT-0072 V6"*. Norma Técnica NTC-ISO 22301:2019 Seguridad y Resiliencia. Sistema de Gestión de Continuidad del Negocio. Requisitos.
Dimensiones MIPG	Dimensión 3 “*Gestión con Valores para Resultados*” en las políticas: “*Gobierno Digital*” y “*Seguridad Digital*”.

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

Causas	Falta de rigurosidad en la aplicación de la norma NTC-ISO 22301:2019, teniendo en cuenta que dicha norma se toma como referencia; falta de una política unificada de continuidad del negocio; falta de sensibilización en los temas relacionados con la continuidad del negocio y la centralización de la información asociada a los incidentes o eventos de crisis.
Efectos	Afectación a la imagen institucional y adecuada toma de decisiones; posible pérdida de la memoria institucional relacionada con la gestión de la continuidad del negocio ante la falta de centralización de la documentación producto de los eventos de incidentes y/o crisis; falta de gestión de las lecciones aprendidas; afectación a la trazabilidad de la información; y posible fuga de conocimiento.
Riesgos	Exposición a los riesgos: R4. "*Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información*", del subproceso Innovación y Tecnología V3 y R3. "*Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad, y disponibilidad de los datos*", del subproceso Seguridad de la Información V2.

Fuente: Elaborado por el equipo auditor

Recomendaciones específicas frente Hallazgo 05:

- Configurar la continuidad del negocio enmarcado en un Sistema de Gestión tomando como referencia la norma NTC-ISO 22301:2019, cumpliendo los requisitos con mayor rigurosidad.
- Formular la Política específica de Continuidad del Negocio conforme lo indica el lineamiento "*5.2.1 Establecimiento de la Política de Continuidad de Negocio*" de la norma NTC-ISO 22301:2019.
- Establecer un repositorio unificado con la documentación resultado de los eventos e incidentes de seguridad de la información y definir la ubicación de esta, en las TRD que corresponda.
- Fomentar la socialización y sensibilización en los temas relacionados con la continuidad del negocio.

5. EVALUACIÓN DE LOS COMPONENTES DEL SISTEMA DE CONTROL INTERNO - SCI

En cumplimiento de las funciones de la Oficina de Control Interno (OCI) y con el propósito de evaluar el avance en la implementación de los cinco componentes del SCI, correspondientes a la séptima dimensión del Modelo Integrado de Planeación y Gestión (MIPG), se verificaron los siguientes aspectos: Ambiente de Control, Evaluación del Riesgo, Actividades de Control, Información y Comunicación, y de las Actividades de Monitoreo. Estos componentes contribuyen al logro de los objetivos institucionales y sus resultados se presentan a continuación. No obstante, en cada uno de los hallazgos formulados se han identificado los componentes del MIPG, que requieren especial atención por parte de los líderes de los procesos auditados, con el fin de fortalecer su gestión y mejorar su nivel de implementación.

5.1 Ambiente de control.

Régimen de inhabilidades e incompatibilidades y conflicto de interés.

En relación con la socialización o divulgación de las situaciones en las que se puede incurrir en inhabilidad, incompatibilidad y/o conflicto de interés, y cuál ha sido su tratamiento, se evidenció la divulgación sobre el tratamiento a las situaciones en las que se puede generar

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

inhabilidad, incompatibilidad y/o conflicto de interés en los procesos auditados: DGIT, OSI, DGI, DGA, DGF, DGC, DGEA, DGJ, en las Subdirecciones y Oficinas, mediante la implementación de acciones tendientes a la apropiación con cursos de reinducción, capacitaciones, charlas y comunicaciones institucionales. En la DGC específicamente, la Subdirección Financiera manifestó, que no se les han socializado. De igual forma en la DSI Medellín, esta socialización se llevó a cabo mediante una capacitación y en la DSA Medellín, se realizaron tres actividades durante el año 2023, entre las que se destacan: la "*Actividad práctica de apareamiento sobre conceptos de conflictos de intereses en la función pública*", realizada el 28/04/2023; la *"Divulgación y capacitación sobre la gestión preventiva de conflictos de intereses en el marco de la política de integridad pública (Evidencia Gestión Ética)*", llevada a cabo el 19 de abril de 2023; y una tercera actividad desarrollada el 27 de abril de 2023.

En la vigencia 2025 en las direcciones de gestión y oficinas: DGIT, OSI, DGI, DGA, DGF, DGEA y DSA y DSI Medellín no se presentaron casos relacionados con inhabilidades, incompatibilidades o conflictos de interés. Sin embargo, en la Subdirección de Compras y Contratos de la DGC, se evidencio una situación relacionada con "*impedimento y recusación*" y, en la DGJ se evidenciaron ocho casos así: en la Subdirección de Asuntos Penales: "*impedimento presentado por 3 funcionarios para participar en el análisis de dos valoraciones de conductas punibles*", en la Subdirección de Representación Externa: se gestionó una declaración de conflicto de interés manifestado por la Subdirectora y por último, el Director de Gestión Jurídica se declaró impedido en 6 casos en el CCDJ[8], situaciones de inhabilidades, incompatibilidades y/o de conflictos de interés, las cuales fueron tramitadas y resueltas.

Procesos disciplinarios por presuntas faltas disciplinarias.

Para el periodo comprendido entre el 1/01/2023 y el 28/02/2026, la Subdirección de Asuntos Disciplinarios informó que: respecto a procesos disciplinarios en trámite y/o fallados contra servidores públicos de la DIAN, asociados a los atributos de seguridad de la información (integridad, confidencialidad y disponibilidad) de las ST de la entidad, se identificaron siete expedientes los cuales se clasificaron así: tres (3) en etapa de "*Indagación Preliminar*", tres (3) en etapa de "*Investigación Disciplinaria*", y uno (1) con "*Fallo*".

Al corte 28/02/2026, el estado de los expedientes antes mencionados era el siguiente: los relacionados con la solución tecnológica de correo electrónico uno registraba "*fallo absolutorio"*, uno con "*cierre de investigación*", uno en "*investigación disciplinaria*", y uno en "*archivo*" (este también vinculado al uso de Teams). Por su parte el expediente relacionado con el Aplicativo Público No Institucional Portal SAR (D), se encontraba en etapa de indagación preliminar. Finalmente, los expedientes asociados a la Obligación Financiera (MUISCA) y Factura Electrónica Nube se encontraban en estado de "*terminación*".

Actualización de procedimientos y otras normas.

En relación con el procedimiento "*PR-IIT-0454 Disponibilidad de la Operación Tecnológica*"

[8] Comité de Conciliación y Defensa Judicial de la UAE DIAN

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

se evidencia que este se actualizó el 13/08/2025 a la Versión 2, comprobando que en esta versión se realizaron varios ajustes entre los que se destacan la modificación del objetivo, el alcance del documento y se añadieron dos secciones nuevas así:

- "*Criterios para evaluar en la mesa de incidentes, basados en el protocolo OD-PEC-0003 con una tabla que evalúa impacto en: servidores públicos, Reputación, legalidad, servicio*." y
- "*Gestión de datos personales, alineado con la normativa interna sobre privacidad.*"

Adicionalmente y en cumplimiento de la Resolución 000002 del 24 de enero de 2024, la DIAN adoptó el Modelo de Gestión por Procesos[9] como marco para fortalecer la modernización institucional, la mejora continua y la alineación de los procesos con los objetivos estratégicos. Este modelo integra el negocio con la Arquitectura de Tecnologías de la Información, promoviendo la coordinación entre las áreas responsables e impulsando la incorporación de ST para optimizar el desempeño institucional. Asimismo, estructura la gestión mediante subprocesos y actividades documentadas en "*procedimientos*", y establece lineamientos para garantizar una adecuada gestión documental, asegurando la trazabilidad, consistencia y actualización de la información, así como la homologación de la documentación del Listado Maestro de Documentos - LMD ante cualquier diseño o mejora de los procesos; por lo anterior, las áreas auditadas realizan gestiones para la actualización o creación de procedimientos, instructivos, cartillas, formatos, manuales[10].

Código de Integridad Institucional[11].

Los funcionarios de las áreas auditadas han participado en diversas actividades que han facilitado la apropiación de los principios y valores institucionales definidos en el Código de Integridad de los servidores públicos de la DIAN. Entre las que se destacan jornadas de inducción y reinducción, capacitaciones presenciales y virtuales, socializaciones, estrategias de comunicación interna, espacios de reflexión y apropiación; así como, en compromisos individuales.

Norma Técnica Colombiana NTC 6047.

De conformidad con la Dimensión 3 de MIPG V6, se analizó la política de servicio al ciudadano y el relacionamiento del Estado con el ciudadano, evidenciando que en los espacios de Servicio al Ciudadano de las DSI y DSA Medellín cumplen en términos generales con los requerimientos establecidos en la Norma Técnica Colombiana NTC 6047. No obstante, se identificaron oportunidades de mejora en lo relacionado con la señalética.

En el caso de la DSI Medellín, se evidencia que parte de las señales es insuficiente, ya que varias están elaboradas en papel, en blanco y negro, y no cuentan con características de accesibilidad como alto relieve ni sistema Braille. Por su parte, en la DSA Medellín – punto de atención Monterey, también presenta deficiencias, debido a que algunas señales no incorporan alto relieve. Además, en este punto de atención se presenta una limitación de acceso para las personas con movilidad reducida que no pueden utilizar escaleras, por

[9] MN-PEC-0228 Modelo de Gestión por Procesos de Negocio, DGEA - Subdirección de Procesos
[10] Documentos: OSI 24, DGIT 28, SFESO 7, SP 24, fuente respuesta a solicitud de información No 13.
[11] CG-TAH-0002 Versión 3, https://diancolombia.sharepoint.com/sites/diannetpruebas/Areas/Carpetas%20Control%20Disciplinario/Codigo-de-Integridad-DIAN.pdf

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

cuanto no pueden acceder al segundo piso y, en consecuencia, deben ser atendidas en el primer nivel.

Finalmente, se recomienda retomar los procesos de capacitación en lenguaje de señas, para fortalecer la atención a la población con discapacidad auditiva en ambos puntos de atención de las DSI y DSA Medellín.

5.2 Evaluación del Riesgo.

En cumplimiento de la "*Política para la administración de riesgos de la Dirección de Impuestos y Aduanas Nacionales – UAE DIAN*" (Versión 4 del 16/06/2026), la cual establece un marco objetivo, integral, participativo y dinámico; en este sentido, la segunda línea de defensa ha venido adelantando acciones estratégicas orientadas a mitigar de forma proactiva el riesgo de afectación de la información en su integridad, confidencialidad y disponibilidad, bajo el enfoque institucional de seguridad digital, destacándose los siguientes frentes de gestión tecnológica y operativa impulsados desde la DIGIT en el periodo evaluado:

Robustecimiento de Accesos y Autenticación: Se implementó el Doble Factor de Autenticación (MFA) para las aplicaciones corporativas de Microsoft 365 (Outlook y Teams) y se gestionó su adopción en Muisca mediante mecanismos OTP[12]. Así mismo, se optimizó la seguridad perimetral con la eliminación de las conexiones vía VPN, se definieron roles de acceso a recursos en la nube y se ejecutó el enrolamiento formal de usuarios.

Protección de Infraestructura y Activos de Información: Con el fin de salvaguardar los datos institucionales frente a incidentes de seguridad, se implementó el cifrado de discos duros en equipos portátiles de la entidad, de igual forma, se participó en la identificación, valoración y clasificación de los activos tecnológicos en función de su criticidad y nivel de riesgo.

Gobernanza y Normalización Documental: Se contribuyó al fortalecimiento del Sistema de Gestión de la Calidad, mediante la elaboración y actualización de instrumentos normativos, tales como: la cartilla *"Lineamientos de Seguridad y Privacidad en el Desarrollo Seguro de Software - CT-IIT-0153",* el procedimiento de *"Gestión de Accesos - PR-IIT-0455"*, la cartilla "*Gestión de Riesgos de Seguridad de la Información - CT-IIT-0132*" y el *"Manual de Políticas y Lineamientos de Seguridad y Privacidad de la Información - MN-IIT-0072."*

De otra parte, en relación con los informes cuatrimestrales de gestión de riesgos en la vigencia 2023, 2024 y 2025, remitidos por la DGIT y la OSI en los formatos FT-PEC-2096 "*Informe de monitoreo de riesgos*" y FT-PEC-2097 "*Reporte materialización de riesgos*", se observó lo siguiente:

Tabla No. 08. Reporte de materialización de riesgos - OSI

Riesgo	Periodo	Descripción de la causa
R3. Medidas de control implementadas parcialmente o sin implementar.	2023 - I	Indisponibilidad servicios ORION y caída de páginas de certificados de origen.
	2023 - II	Afectación de la disponibilidad de Orión, VPN y Comunicaciones administradas por el proveedor Claro.

[12] Código dinámico de seguridad que expira tras un corto periodo de tiempo

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

Riesgo	Periodo	Descripción de la causa
	2023 - III	Inestabilidad en el sistema Siglo XXI, mal funcionamiento de algunas opciones del software reportados por los usuarios.
	2024 - I	1. Realizaron un Failover del Servidor, donde se encuentra la administración de Bogotá de Siglo XXI, lo que permite asegurar que el sistema siga operando. 2. Se genera un reporte interno sobre el evento con el fin de ser el insumo principal para generar el material multimedia y realizar las actividades de difusión en medios de comunicación masiva y redes sociales. Adicionalmente, se envió la notificación e informe al COLCERT y CSIRT Presidencia, para realizar el bloqueo en la web. 3. Se reportó por correo electrónico y por Teams a los Grupos de la SITO de Despliegue, Directorio Activo. Se realiza reinicio del servidor virtual, y se efectúan pruebas, y se restablece 06:02 a.m.

Elaboró: Equipo Auditor
Fuente: Formatos FT-PEC-2096 y FT-PEC-2097, OSI.

Tabla No. 09. Reporte de materialización de riesgos – DGIT

Riesgo	Periodo	Descripción de la causa
R1. Sistemas de información y servicios digitales indisponibles (no programada-fortuita) para las partes interesadas.	2023 - II	Degradación de MPLS[13] que afectó la operación a nivel nacional incluyendo los servicios corporativos y el servicio de internet.
	2023 - III	Ajustes y actualización del sistema SYGA – Siglo XXI, Inestabilidad, Fallas en la operación.
	2024 - I	**Caso No.1.** El 31/03/2024 se presentó una caída Pagina SIEX por indisponibilidad del servicio OracleiSuitesHTTPServer. **Caso No.2.** El 14/04/2024 hubo Indisponibilidad de los servicios aduaneros y tributarios Muisca, ocupación archivelog que van a la nube.
	2024 - II	**Caso No.1.** Funcionario de CLARO desconecta el puerto 47 del switch.228, para verificar la potencia del puerto, después se presentaron las fallas en los servicios MUISCA. **Caso No.2.** La clave del usuario con el que el servicio WSO2 se conecta al LDAP se había cambiado y esto generaba problemas de conexión y de identificación. **Caso No.3.** El 14 de agosto sobre el mediodía, se determinó que el servicio (motor de búsqueda desplegado en nube) que permite consultar a la ciudadanía si está o no obligado a presentar declaración de renta, estaba generando gran cantidad de conexiones al servicio de identidad, servicio que es transversal a todos los sistemas. **Caso No.4.** Ruptura de fibra por corto eléctrico en recámara de Codensa, evento ubicado en la carrera 9 con calle 9. La red WAN de todas las sedes se quedan sin servicio. **Caso No.5.** Claro realiza sin previo aviso de ventana de mantenimiento redistribución de cargas en sus troncales

[13] El switching de etiquetas multiprotocolo (MPLS) es un protocolo diseñado para llevar paquetes de datos a sus destinos de manera rápida y eficiente, https://www.fortinet.com/lat/resources/cyberglossary/mpls.

Riesgo	Periodo	Descripción de la causa
R1. Sistemas de información y servicios digitales indisponibles (no programada-fortuita) para las partes interesadas.	2025 - I	Unificación de Formatos
	2025 - II	En el mes de mayo el indicador de disponibilidad de la plataforma tecnológica presentó una desviación (99,29%) de acuerdo con la meta establecida (99.8%), este resultado corresponde a las contingencias declaradas el 12 y 26 de mayo 2025 por indisponibilidad de los servicios de Muisca durante los vencimientos de las declaraciones.
	2025 - III	**Caso No.1.** Se presentó un error en firma de documentos en los diferentes servicios y sistemas de la DIAN, Indisponibilidad de los SIEs Muisca Carga, Salida de Mercancías, Tránsito Aduanero y SYGA – Siglo XXI Importaciones, este evento corresponde a la contingencia declarada el 28 y 29 de noviembre 2025 para estos aplicativos. **Caso No.2.** El 30 de diciembre de 2025, luego de una ventana de mantenimiento sobre los sistemas de información se declara indisponibilidad parcial e intermitencia de los servicios informáticos por incidentes técnicos que desde el 27 y hasta el 31 de diciembre de 2025 generaron que algunos contribuyentes no pudieron realizar pagos y presentar sus declaraciones, Usuarios aduaneros experimentaron dificultades en carga importaciones, tránsito aduanero, salida de mercancías, Sistema de Información y Gestión Aduanera (SYGA – Siglo XXI).

Elaboró: Equipo Auditor
Fuente: Formatos FT-PEC-2096 y FT-PEC-2097, DGIT.

Con base en la información analizada, se evidencio la materialización recurrente de los riesgos R1 "*Sistemas de información y servicios digitales indisponibles (no programada-fortuita) para las partes interesadas*" de la DGIT y R3 "*Medidas de control implementadas parcialmente o sin implementar*" de la OSI, durante los periodos evaluados. Los eventos registrados afectaron la disponibilidad, continuidad y desempeño de los servicios tecnológicos críticos de la entidad entre ellos ST SYGA - Siglo XXI, la caída de la página SIEX y fallas en los servicios MUISCA y en otras plataformas. En resumen, las causas estuvieron relacionadas con factores internos y externos tales como fallas de infraestructura, problemas de conectividad, actividades de proveedores, errores de configuración y mantenimientos, lo que impactó la prestación de servicios tributarios y aduaneros y el indicador de disponibilidad tecnológica.

Lo anterior evidencia debilidad en los controles preventivos, detectivos y correctivos implementados para la gestión de la disponibilidad de los servicios y la continuidad operativa, lo que invita a fortalecer la gestión integral del riesgo tecnológico con el fin de mitigar la probabilidad de impacto de eventos semejantes o similares y garantizar la continuidad de los servicios ofrecidos a contribuyentes o partes interesadas.

Por consiguiente, se considera necesario revisar, fortalecer y de ser pertinente, implementar nuevos controles asociados a dichos riesgos, con el fin de prevenir y mitigar la ocurrencia de estas causas, así como, reducir la probabilidad de materialización de eventos similares en el futuro. No obstante, se evidencia un avance en el registro de los riesgos de seguridad de la información en los módulos de gestión de riesgos de la herramienta GRC, los cuales se encuentran parametrizados y alineados con los procesos y macroprocesos definidos por la entidad, mejorando el seguimiento, monitoreo y control de manera automatizada.

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

5.3 Actividades de Control

Avance en la implementación de controles del SGSPI.

De un universo de 1.375 controles establecidos en el "*MN-IIT-0072 Manual de Políticas y Lineamientos de Seguridad y Privacidad de la Información V6"*, se seleccionó una muestra de 1.088 considerando los más representativos por tipo de control con el fin de hacer seguimiento a la implementación de éstos, conforme a ello se evidenció que 296 controles tienen un porcentaje de avance del 100%, 104 entre el 60 y el 95 %, 55 entre el 5 y el 50% y 633 reportan el 0% de avance. Adicionalmente, en la relación del SGSPI, se evidenció que no existen controles asociados a la DGA, en cuanto a la DGIT no se reportó el avance de los controles a cargo de esta, así como de la Subdirección de Innovación y Proyectos y Subdirección de Soluciones y Desarrollo.

En la siguiente tabla, se registra el avance de los controles referidos así:

Tabla No. 10. Resumen avance implementación controles SGSPI según muestra

Tipo de Control*	Total, controles de la muestra por tipo	Porcentaje de avance			
		100%	Entre el 95% y el 60%	Entre el 50% y el 5%	0 %, N/A o no reporta avance
5. Controles organizacionales	373	79	62	28	204
6. Controles de personas	85	41	6	0	38
7. Controles físicos	159	35	5	3	116
8. Controles tecnológicos	439	130	25	19	265
9. Controles adicionales	32	11	6	5	10
Total, controles muestra	**1088**	**296**	**104**	**55**	**633**
Porcentaje de avance frente al total de controles de la muestra		**27%**	**10%**	**5%**	**58%**

Elaboró: Equipo Auditor
Fuente: Respuesta Controles SGSPI - SITO 100202204-1401 ASI 2026-002. Solicitud No. 13. Evaluación SCI.
*La numeración del tipo de control obedece a la establecida en el "*MN-IIT-0072 Manual de Políticas y Lineamientos de Seguridad y Privacidad de la Información V6*".

De acuerdo con la tabla de correlación de riesgos, hallazgos y controles se identificaron oportunidades de mejora en la coordinación y alineación de los controles asociados al monitoreo, la gestión de incidentes tecnológicos y de seguridad, la continuidad de los servicios y la activación de las medidas de protección al usuario. Actualmente, estos procesos no interactúan de manera articulada, lo que dificulta la detección temprana de eventos, retrasa su escalamiento y limita una respuesta oportuna y coordinada frente a fallas operativas, incidentes de ciberseguridad o interrupciones no previstas de los servicios tecnológicos evidenciándose como insuficientes para atacar la causa raíz.

Asimismo, la falta de lineamientos y controles integrados para la gestión de desarrollos Low-Code/No-Code, la administración de los activos de información según su criticidad y el aprovechamiento de los resultados de las evaluaciones de seguridad se reduce la capacidad de anticipar y gestionar riesgos de manera efectiva. Esta situación incrementa la exposición de la entidad a eventos que pueden afectar la confidencialidad, integridad y disponibilidad de la información, impactando la continuidad de los servicios, aumentando los tiempos de recuperación y generando afectaciones en la operación y en la atención a los usuarios. (Ver anexo 1 al final del informe correlación de riesgos y controles).

Plan de Mejoramiento Institucional (corte 28/04/2026).

Se tomo una muestra seleccionando los hallazgos que se relacionan con el tema auditado y las 45 ST, los cuales inciden directamente a la DGIT y la DGEA con planes de mejoramiento vigentes y suscritos con la Contraloría General de la República - CGR, la Agencia del Inspector General de Tributos, Rentas y Contribuciones Parafiscales – ITRC y la Oficina de Control Interno - OCI. Del análisis se observa que el universo revisado está conformado por 22 hallazgos y 123 acciones de mejora que despliegan 148 actividades; de las cuales, 53 se encuentran en proceso y 95 están cumplidas, asociadas principalmente a temas tecnológicos, no se reflejan incumplimientos.

En cuanto al origen de los hallazgos, las causas comunes identificadas se relacionan con: rezago tecnológico, falta de soporte o actualización de software, deficiencias en la administración de usuarios y roles, ausencia de controles automatizados, debilidades en la trazabilidad de operaciones, falta de integración entre ST, uso de controles manuales, información inconsistente, ausencia de lineamientos claros para aplicativos no corporativos y deficiente articulación entre las áreas funcionales y tecnológicas.

5.4 Información y Comunicación

Se evidencian oportunidades de mejora en la gestión de continuidad y transformación digital institucional, relacionadas con la insuficiente socialización y apropiación del Plan de Continuidad del Negocio (PCN), el fortalecimiento de los mecanismos de comunicación y coordinación para la gestión oportuna de indisponibilidades de las ST, la ampliación del uso de firmas digitales para garantizar la gestión electrónica integral de los actos administrativos y la implementación de una solución institucional de gestión documental que permita la conformación y administración centralizada del expediente electrónico. Estas situaciones generan procesos documentales híbridos, dificultades en la trazabilidad y estandarización de la información y limitaciones en la capacidad de respuesta frente a contingencias, impactando la continuidad operativa y la calidad del servicio prestado a usuarios internos y contribuyentes.

En cuanto a los activos de información de los procesos auditados, se estableció que estos se encuentran registrados en la herramienta GRC, no obstante, no se evidencio en todos los casos la publicación de los mismos en el portal institucional de la DIAN en el enlace de "*Transparencia y acceso a la información*", en cumplimiento de lo establecido en la Ley 1712[14] de 2014.

5.5 Actividades de Monitoreo

Se evidencia por parte de los lideres de los procesos un compromiso permanente con el fortalecimiento de la seguridad y privacidad de la información, atendiendo de manera oportuna y responsable los requerimientos de monitoreo, validación y seguimiento realizados por la OSI. Este trabajo articulado ha permitido no solo cumplir con los

[14] 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", Art 3 principios.

lineamientos establecidos en el SGSPI, sino también en la generación de información confiable para identificar oportunidades de mejora y fortalecer continuamente los controles institucionales establecidos.

Entre las actividades de monitoreo informadas, se relacionan: el reporte de alertas, la revisión y seguimiento a roles y repositorios, carpetas, el conocimiento y análisis de incidentes de seguridad reportados por las direcciones seccionales a la OSI, seguimiento a los indicadores, así como, al uso adecuado de las ST y activos de información, la aplicación de lineamientos técnicos y operativos para el manejo y tratamiento de la información, la adopción de medidas preventivas, revisiones internas adelantadas en mesas técnicas, verificación del manejo de información, sensibilizaciones periódicas, verificación de suscripción y cargue de acuerdos de confidencialidad, control regular de los planes de acción registrados en la herramienta GRC, permitiendo verificar su progreso, cumplimiento y efectividad, frente a los riesgos identificados.

En las DSI y DSA Medellín, se realizaron actividades de monitoreo y control para verificar el cumplimiento de los lineamientos de seguridad y privacidad de la información por parte de los funcionarios, mediante auditorías periódicas con el fin de identificar y desinstalar software no autorizado, así como, proceso de cifrado de BIOS y de discos duros, actualización de sistemas operativos, aplicación de políticas a equipos de Kiosco y actualización de certificados digitales y doble factor de autenticación. No obstante, se identificó falta de monitoreo en el uso de scripts desarrollados en Python y, en algunos casos, el acceso directo a información extraída de ambientes en producción para la generación de reportes.

Así mismo, se estableció que el almacenamiento de códigos fuente y archivos asociados, se realiza en cuentas personales de OneDrive, particularmente en el caso de los scripts de Python, en lugar de utilizar repositorios institucionales centralizados de la herramienta SharePoint establecida para cada lugar administrativo. Esta situación pone de manifiesto la necesidad de que la DGIT, establezca lineamientos y controles que regulen el desarrollo, almacenamiento y acceso a este tipo de información, garantizando que las personas competentes con acceso y manejo de los datos cuenten con las autorizaciones respectivas.

Denuncia Ciudadana Identificada con Número de proceso 7600125020052026XXXXXX

De acuerdo con lo informado por la SFESO, el radicado 2026DP00000XXXX fue tramitado por la Coordinación de Denuncias de Fiscalización y respondido por la Subdirección de Asuntos Disciplinarios. Respecto a la misma denuncia relacionada con la ST de Facturación Electrónica, la SFESO atendió los radicados 2025DP0002829XXXX, 2025DP000306XXXX, 2025DP00030XXXX y 2025DP00038XXXX mediante los oficios respectivos, en los cuales precisó que sus competencias se limitan a la verificación de requisitos tributarios y técnicos de los documentos electrónicos, conforme al artículo 34 de la Resolución DIAN 165 de 2023. Asimismo, se aclaró que no le corresponde investigar conductas penales, determinar falsedad documental, realizar peritajes, certificar la realidad económica de las operaciones, intervenir en controversias entre particulares ni calificar actuaciones de otras entidades.

De otra parte, frente a los Indicadores SGSPI, la entidad cuenta con un esquema formalizado para la medición y seguimiento del desempeño de los controles de seguridad

y privacidad de la información. Los indicadores definidos se encuentran conforme a los lineamientos de la Norma ISO/IEC 27001:2022 y se indica que se disponen de elementos esenciales para su gestión, tales como: responsable, período de medición, meta y fórmula de cálculo. Así mismo, se informó que, con corte al 24 de abril de 2026, dichos indicadores están debidamente registrados en las herramientas GRC y en el Informe ITERA, donde se realiza su medición y seguimiento periódico. Esto fortalece la capacidad de la entidad para evaluar el nivel de madurez del SGSPI, verificar el cumplimiento de los requisitos normativos y contar con información confiable para la toma de decisiones, orientadas a la mejora continua de la seguridad y privacidad de la información.

En la vigencia 2025, se evidenció dentro del Mapa de Alineación Total de la DIAN que, para la OSI, se establecieron 10 indicadores, de los cuales, el porcentaje total de cumplimiento fue del 118.95%.

Retiro de los hallazgos de los planes de mejoramiento.

La revisión de los soportes con los cuales se solicitó el retiro de los hallazgos de los planes de mejoramiento de los procesos auditados en el primer y segundo semestre de 2025, permiten evidenciar un avance positivo en el cumplimiento de los compromisos establecidos en los planes de mejoramiento derivados de auditorías de la OCI y de la CGR. En términos generales, las dependencias responsables demostraron la implementación de acciones y actividades correctivas de mejora, que contribuyeron a subsanar las causas que generaron los hallazgos y al fortalecimiento de los controles institucionales.

Se destaca que varios de los retiros, estuvieron asociados a la implementación de funcionalidades, ajuste o fortalecimiento de ST, así como a la formalización, actualización de activos de información, mejoras en mecanismos de control, consultas, monitoreo de operaciones, además en la optimización de procesos soportados en herramientas institucionales tales como: Obligación Financiera, SYGA - Siglo XXI, Integra, GRC y, en el portal de la entidad en el botón de transparencia. Las evidencias presentadas muestran que las acciones y actividades de mejora ejecutadas, permitieron alcanzar los resultados esperados y superaron las pruebas de efectividad realizadas.

Asimismo, se observó que algunos hallazgos fueron retirados por cumplimiento total de las actividades comprometidas, en otros correspondieron a situaciones que una vez analizadas, no mantenían relación directa con deficiencias tecnológicas, sino con aspectos operativos o procedimentales, que se deben continuar gestionando por las áreas responsables dentro de sus competencias. Es importante resaltar el trabajo articulado entre las áreas funcionales y la DGIT, permitiendo mejoras que fortalecen la gestión de riesgos, la calidad de la información, la seguridad de los activos tecnológicos y la transparencia institucional. Estos resultados reflejan una gestión orientada al mejoramiento continuo y al cierre efectivo de las brechas identificadas por los entes de control.

6. FOMENTO DE LA CULTURA DEL CONTROL

Se llevó a cabo la sensibilización de "*Fomento a la cultura del control*" el 12 de junio de 2026, en el que se trataron temas relacionados con: Gestión del riesgo, Modelo Integrado de Planeación y Gestión – MIPG, Modelo Estándar de Control Interno – MECI y Comité de

Organizaciones Patrocinadoras de la Comisión Treadway – COSO, Líneas de Defensa, Comité de Operación del MIPG – Resolución 021 de 2022, Mapa de Aseguramiento, Formulario Único de Reporte de Avance de la Gestión - FURAG, Dimensión 2, Direccionamiento Estratégico, Dimensión 4. Evaluación de Resultados, Micrositio Oficina de Control Interno, Planes de Mejoramiento, Gestión de Accesos, Plan de Continuidad del Negocio – PCN, contando con una participación de 10 funcionarios de las áreas DGIT, DGF, SDFI, SFA, DGC, DGA, DSA Medellín.

7. CONCLUSIONES

- La auditoría evidenció oportunidades de mejora relevantes asociadas a la disponibilidad total o parcial de la Soluciones Tecnológicas - ST, así como deficiencias en la gestión de eventos e incidentes de seguridad de la información, la gestión de vulnerabilidades, la administración de activos de información y la implementación de controles de seguridad y privacidad.

- De igual manera, se identificaron debilidades en la gobernanza de datos, el control del desarrollo y la gestión de accesos en soluciones Low-Code/No-Code (LCNC), así como, falencias en la gestión de la continuidad del negocio. Situaciones que incrementan la exposición de la entidad a riesgos de seguridad y operativos que podrían afectar la integridad, confidencialidad y disponibilidad de la información y los datos, comprometiendo el cumplimiento de los objetivos institucionales y la prestación adecuada de los servicios.

- Resulta prioritario definir e implementar planes de acción orientados a fortalecer los controles, cerrar las brechas identificadas y mitigar los riesgos asociados, promoviendo una gestión integral y sostenible de la seguridad de la información.

- La atención oportuna de los hallazgos permitirá fortalecer la resiliencia organizacional, mejorar la capacidad de respuesta ante eventos adversos y consolidar un entorno de control más robusto, contribuyendo a generar y mantener la confianza de los ciudadanos, usuarios y demás grupos de valor en la gestión y protección de la información institucional.

- Si bien la UAE DIAN dispone del procedimiento PR-IIT-0454 "*Disponibilidad de la Operación Tecnológica*" – V2, que define medidas de protección al usuario y establece lineamientos para la gestión interna de fallas técnicas en los servicios tecnológicos, los hallazgos identificados reflejan la necesidad de fortalecer la efectividad de los controles y mecanismos de seguimiento.

- Del análisis realizado a la implementación de los controles del SGSPI se evidencia que, aunque existen avances importantes en algunos frentes, el nivel general de implementación aún representa un desafío significativo para la consolidación del sistema. Si bien el 27 % de los controles evaluados se encuentran completamente implementados, más de la mitad de la muestra el 58 % no registra avances, no reporta información o fue clasificada como no aplica, lo que limita la capacidad de asegurar una gestión integral y efectiva de los riesgos identificados.

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

- Adicionalmente, se identificaron debilidades en los mecanismos de seguimiento, monitoreo y reporte de la implementación de controles, así como en la definición y ejecución de responsabilidades por parte de algunas dependencias. Especial atención merece la ausencia de información en determinados procesos y la inexistencia de controles asociados a la Dirección de Gestión de Aduanas, lo que limita la visibilidad sobre el estado real del SGSPI y afecta la capacidad de evaluar de manera integral la eficacia de los controles establecidos.

- Debilidades en la gestión de la información y el desarrollo tecnológico, particularmente en el uso de scripts de Python con acceso a datos en producción y en el almacenamiento de códigos fuente en repositorios personales. Lo anterior, genera riesgos asociados a la seguridad, trazabilidad y control de los activos de información, por lo que resulta necesario fortalecer los lineamientos institucionales, los mecanismos de supervisión y los controles de acceso.

- El retiro de los hallazgos analizados evidencia un nivel adecuado de madurez en la gestión de los planes de mejoramiento, así como el compromiso institucional con la corrección de las observaciones formuladas por la OCI y la CGR.

- La operación aislada entre las áreas de monitoreo, seguridad digital y gestión de incidentes tecnológicos limita la perspectiva integral de la gestión tecnológica de la entidad, impidiendo que las alertas tempranas se transformen en acciones inmediatas de contingencia. Esta desarticulación bloquea la activación oportuna de las medidas de protección al usuario y consolida un enfoque netamente reactivo, que prolonga de manera crítica los tiempos de indisponibilidad imprevista de las ST, incrementando la exposición de la entidad a riesgos operativos de alto impacto, comprometiendo la continuidad de sus servicios esenciales y la perdida reputacional de la entidad.

- Aunque las áreas reportan oportunamente la materialización de riesgos conforme a los lineamientos establecidos, se identificó que los eventos y riesgos evidenciados durante los ejercicios de auditoría de la OCI no son considerados de manera integral dentro del proceso de gestión de riesgos. Esta situación genera una subvaloración de la exposición real al riesgo de la entidad, limita la trazabilidad de las debilidades identificadas y dificulta la adopción de acciones de mejora basadas en las lecciones aprendidas derivadas de los hallazgos de auditoría, afectando la efectividad del sistema de gestión de riesgos institucional

- Resulta necesario fortalecer la orientación del plan de mejoramiento hacia la solución efectiva de las causas que dieron origen a los hallazgos, priorizando acciones estructurales, medibles y sostenibles en el tiempo. Esto implica que el cierre de los compromisos no se limite a la generación de evidencias o al cumplimiento formal de actividades, sino que permita demostrar mejoras reales en el gobierno tecnológico, la seguridad de la información, la calidad de los datos, la continuidad operativa y la administración de las ST.

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

8. RECOMENDACIONES

- Sin perjuicio de las recomendaciones específicas formuladas frente a cada uno de los hallazgos y las oportunidades de mejora identificadas, se considera pertinente:

- Incorporar los lineamientos de desarrollo ciudadano con tecnologías LCNC en el listado maestro de documentos, formalizar la gobernanza y el control de los aplicativos, y consolidar un inventario de las soluciones LCNC con la información esencial para su gestión, seguridad y continuidad del negocio.

- Mantener una revisión periódica de las matrices de riesgos operacionales y los registrados en la herramienta GRC, asegurando que los controles definidos para los activos de información sean pertinentes, efectivos y suficientes para mitigar los riesgos identificados, reducir la probabilidad de su materialización y prevenir posibles afectaciones de los servicios de las ST.

- Implementar un modelo de gobernanza tecnológica transversal que articule y se coordine ente las áreas el monitoreo, la seguridad digital y la gestión de incidentes bajo un enfoque proactivo que minimice cualquier alerta temprana o evento de ciberseguridad y se activen de inmediato contingencias coordinadas y medidas de protección al usuario, permitiendo así, mitigar proactivamente los riesgos operativos, reducir los tiempos de indisponibilidad de las ST y salvaguardar la continuidad de los servicios esenciales de la entidad.

- Fortalecer la gobernanza, el monitoreo y la articulación institucional del SGSPI, promoviendo una mayor apropiación de las responsabilidades de control, el reporte oportuno de información y la implementación efectiva de los controles pendientes, con el fin de incrementar la capacidad de la entidad para gestionar los riesgos y salvaguardar la integridad, confidencialidad y disponibilidad de la información.

- Optimizar la gestión de la información y el desarrollo tecnológico mediante la implementación de lineamientos institucionales que regulen el uso de scripts de Python en ambientes de producción y el almacenamiento del código fuente en repositorios corporativos, estableciendo controles de acceso, mecanismos de supervisión y trazabilidad que garanticen la seguridad, integridad y adecuada administración de los activos de información.

- Resulta fundamental mantener las actividades de seguimiento y monitoreo permanente, de las situaciones que fueron retiradas del Plan de Mejoramiento Institucional, para garantizar la sostenibilidad de las acciones implementadas, preservar la efectividad de los controles y prevenir la recurrencia de situaciones similares en el futuro.

- Registrar los riesgos materializados que resulten de los ejercicios de auditoría interna, utilizando el forms del formato “*FT-PEC-2097 Reporte Materialización de Riesgos*” y seleccionando explícitamente como fuente de identificación la opción "*Auditoría Interna*", con el fin de unificar el control de los hallazgos y garantizar un monitoreo continuo y disponer de la completitud de la información para los reportes.

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

- Implementar mecanismos formales de articulación entre las áreas responsables de infraestructura, seguridad de la información, continuidad del negocio y gestión de riesgos, con el propósito de garantizar que las pruebas de infraestructura y de estrés sean planificadas y ejecutadas bajo un enfoque integral de riesgos.

- Las acciones de mejora planteadas en los planes de mejoramiento no deben limitarse a capacitaciones, socializaciones, informes o verificaciones periódicas, ya que este tipo de actividades, aunque pueden ser complementarias, no corrigen por sí mismas, la causa que originó el hallazgo. En estos casos, las acciones de mejora se deben orientar principalmente a la implementación de soluciones estructurales, tales como, automatización de controles, integración entre ST, depuración de datos, parametrización de validaciones, trazabilidad de operaciones, generación de alertas y definición clara de responsables funcionales y tecnológicos.

- Finalmente, se recomienda considerar la viabilidad para la sostenibilidad del Centro de Operaciones de Seguridad (SOC), que actualmente se encuentra en proceso de contratación, con el fin de contar de manera permanente con capacidades de monitoreo, gestión y operación de los controles e instrumentos de seguridad de las tecnologías de la información, fortaleciendo así, la protección y respuesta oportuna y efectiva ante incidentes de ciberseguridad.

ENRIQUE CASTIBLANCO BEDOYA
Jefe Oficina de Control de interno

Proyectó: Equipo Auditor.
Juan Felipe Solórzano García
Sandra Yasmín Flórez Abril – Líder (09/06/2026 – 21/07/2026)
Sandra del Pilar Chuquín Badillo – Líder (17/02/2026-08/06/2026)
Yamile Fresno Forero (17/02/2026-08/07/2026)

Revisó: Juan Rafael Lozano Rodríguez – Evaluador Despacho OCI
Claudia Marcela Quiceno Duque – Jefe Coordinación Auditoría Integral

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

ANEXO 1. Correlación de riesgos y controles, asociados a los hallazgos identificados

Matriz	Riesgo	Hallazgo	Controles de los procedimientos y matriz de riesgos	E/M	Observaciones frente a los controles
Matriz Subproceso Innovación y Tecnología V3	R1. Sistemas de información y servicios digitales indisponibles (no programada-fortuita) para las partes interesadas.	H1. Indisponibilidad total o parcial en soluciones tecnológicas. ST (SIEX (21/03/2024), Servicios Aduaneros y Tributarios MUISCA (14/04/2024)); falla total en el hardware o software de comunicaciones afectando la conectividad en todas las sedes por configuración inadecuada (segundo semestre de 2023)	C4. Decretar medidas de protección al usuario a través del procedimiento PR-IIT-0454 Disponibilidad de la operación tecnológica. C5. Analizar y solucionar los incidentes tecnológicos a través del procedimiento PR-IIT-0458 Gestión de incidentes.	M	Falta de alineación operativa entre los controles que manejan la gestión de incidentes tecnológicos (C5 / PR-IIT-0458) y la activación de las medidas de protección al usuario (C4 / PR-IIT-0454), lo que impide mitigar la indisponibilidad imprevista de las soluciones tecnológicas de forma oportuna. Debido a que el análisis y la solución de fallas opera de manera reactiva, lo que conlleva a la materialización del riesgo.
	R4. Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información	H1. Indisponibilidad total o parcial en soluciones tecnológicas ADA Web - Bitácora - CCC20 - Cuenta Corriente Contribuyente, SIPAC, OBLIGA, SISCOBRA - Sistema de Agendamiento de Citas (Digiturno) - Diligenciamiento - Factura Electrónica - Sistema Integra - Obligación Financiera - Solución tecnológica SYGA - Remate Virtual - SIEX - Carrara, Ferrajoli, SIEPP - Incumplimiento de ANS - Gestión documental electrónica.	C6. Gestionar los incidentes de seguridad digital a través del instructivo IN-IIT-0253 Gestión de incidentes de seguridad digital. C3. Monitorear el funcionamiento de la plataforma tecnológica, a través del instructivo IN-IIT-0241 Monitoreo de plataforma. C4. Decretar medidas de protección al usuario a través del procedimiento PR-IIT-0454 Disponibilidad de la operación tecnológica. C5. Analizar y solucionar los incidentes tecnológicos a través del procedimiento PR-IIT-0458 Gestión de incidentes.	E	Falta de articulación y controles complementarios entre el monitoreo de la plataforma (C3 / IN-IIT-0241), la gestión de incidentes tecnológicos (C5 / PR-IIT-0458) y de seguridad digital (C6 / IN-IIT-0253), lo que limita la activación oportuna de las medidas de protección al usuario enfocadas en la disponibilidad (C4 / PR-IIT-0454) ante fallas no causadas por mantenimientos.
		H2. Deficiencias en la gestión de eventos e incidentes de seguridad de la información y en la gestión de vulnerabilidades.	C6. Gestionar los incidentes de seguridad digital a través del instructivo IN-IIT-0253 Gestión de incidentes de seguridad digital. C3. Monitorear el funcionamiento de la plataforma tecnológica, a través del instructivo IN-IIT-0241 Monitoreo de plataforma. C4. Decretar medidas de protección al usuario a través del procedimiento PR-IIT-0454 Disponibilidad de la operación tecnológica. C5. Analizar y solucionar los incidentes tecnológicos a través del procedimiento PR-IIT-0458 Gestión de incidentes.	E	El monitoreo y la gestión de incidentes de seguridad digital operan de forma aislada y reactiva frente a la solución de incidentes tecnológicos, lo que impide que las alertas de ciberseguridad o fallas imprevistas activen oportunamente las medidas de protección al usuario para la continuidad del servicio, exponiendo las soluciones tecnológicas a tiempos prolongados de indisponibilidad no planificada y exponiendo riesgos que afectan la operación.
		H3. Falencias en la gestión de activos de información y controles de seguridad y privacidad de la información	C6. Gestionar los incidentes de seguridad digital a través del instructivo IN-IIT-0253 Gestión de incidentes de seguridad digital. C3. Monitorear el funcionamiento de la plataforma tecnológica, a través del instructivo IN-IIT-0241 Monitoreo de plataforma. C4. Decretar medidas de protección al usuario a través del procedimiento PR-IIT-0454 Disponibilidad de la operación tecnológica. C5. Analizar y solucionar los incidentes tecnológicos a través del procedimiento PR-IIT-0458 Gestión de incidentes.	E	El monitoreo y la gestión de incidentes de seguridad digital operan de forma aislada y reactiva frente a la solución de incidentes tecnológicos, lo que impide que las alertas de ciberseguridad o fallas imprevistas activen oportunamente las medidas de protección al usuario para la continuidad del servicio, exponiendo las ST a tiempos prolongados de indisponibilidad no planificada y materializando riesgos que afectan la operación.
		H4. Deficiencias en la gobernanza, control de desarrollo y gestión de accesos en soluciones LCNC (Low-Code / No-Code)	C6. Gestionar los incidentes de seguridad digital a través del instructivo IN-IIT-0253 Gestión de incidentes de seguridad digital. C3. Monitorear el funcionamiento de la plataforma tecnológica, a través del instructivo IN-IIT-0241 Monitoreo de plataforma. C4. Decretar medidas de protección al usuario a través del procedimiento PR-IIT-0454 Disponibilidad de la operación tecnológica. C5. Analizar y solucionar los incidentes tecnológicos a través del procedimiento PR-IIT-0458 Gestión de incidentes.	E	Falta de controles relacionados con los desarrollos LCNC impide su gobernanza, control de la información y la detección temprana de sus fallas, obstaculizando la activación oportuna de las medidas de protección al usuario para garantizar la continuidad del servicio (C4 / PR-IIT-0454) ante incidentes imprevistos de indisponibilidad.

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

		H5. Falencias en la Gestión de la Continuidad del Negocio.	C6. Gestionar los incidentes de seguridad digital a través del instructivo IN-IIT-0253 Gestión de incidentes de seguridad digital. C3. Monitorear el funcionamiento de la plataforma tecnológica, a través del instructivo IN-IIT-0241 Monitoreo de plataforma. C4. Decretar medidas de protección al usuario a través del procedimiento PR-IIT-0454 Disponibilidad de la operación tecnológica. C5. Analizar y solucionar los incidentes tecnológicos a través del procedimiento PR-IIT-0458 Gestión de incidentes.	E	Falta de controles que eviten que estos instructivos operen de manera aislada y sin un enfoque de recuperación de negocio, ante fallas fortuitas y no planificadas, lo que ocasiona retrasos en la activación del procedimiento para decretar las medidas de protección al usuario (C4 / PR-IIT-0454), debilitando la capacidad de respuesta de la organización y prolongando los tiempos de indisponibilidad imprevista de las soluciones tecnológicas.
Matriz Subproceso Seguridad de la información V2	R3. Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad, y disponibilidad de los datos.	H1. Indisponibilidad total o parcial en soluciones tecnológicas. ST Agendamiento de citas (Digiturno) (marzo 2026), SIGLO XXI, SIEX (primer semestre 2025)	C6. Monitorear los eventos de los sistemas de información de la DIAN que puedan generar un incidente de seguridad y privacidad de la información, que atente contra la confidencialidad, integridad o disponibilidad de los activos de información. C7. Realizar evaluaciones de vulnerabilidades.	M	Falta de controles para articular de manera preventiva el análisis de fallas técnicas con la detección de brechas de seguridad, los eventos que atentan contra la confidencialidad, integridad y disponibilidad de los activos de información no son contenidos a tiempo, traduciéndose en interrupciones imprevistas que afectan la continuidad de las ST y la materialización del riesgo.
		H2. Deficiencias en la gestión de eventos e incidentes de seguridad de la información y en la gestión de vulnerabilidades.	C6. Monitorear los eventos de los sistemas de información de la DIAN que puedan generar un incidente de seguridad y privacidad de la información, que atente contra la confidencialidad, integridad o disponibilidad de los activos de información. C7. Realizar evaluaciones de vulnerabilidades.	E	La falta de articulación en los controles impide que los hallazgos técnicos de las evaluaciones de seguridad alimenten proactivamente el monitoreo, limitando la capacidad de detectar de manera temprana incidentes que atenten contra la confidencialidad, integridad o disponibilidad de los activos de información antes de que generen un impacto negativo en la operación.
		H3. Falencias en la gestión de activos de información y controles de seguridad y privacidad de la información	C6. Monitorear los eventos de los sistemas de información de la DIAN que puedan generar un incidente de seguridad y privacidad de la información, que atente contra la confidencialidad, integridad o disponibilidad de los activos de información. C7. Realizar evaluaciones de vulnerabilidades.	E	Al no estar correctamente alineados los activos de información, el monitoreo y las pruebas de seguridad se ejecutan de manera generalizada y no basada en criticidad, lo que impide mitigar de forma oportuna las brechas que atentan contra la confidencialidad, integridad o disponibilidad de los datos sensibles de la entidad.
		H4. Deficiencias en la gobernanza, control de desarrollo y gestión de accesos en soluciones LCNC (Low-Code / No-Code)	C6. Monitorear los eventos de los sistemas de información de la DIAN que puedan generar un incidente de seguridad y privacidad de la información, que atente contra la confidencialidad, integridad o disponibilidad de los activos de información. C7. Realizar evaluaciones de vulnerabilidades.	E	La falta de lineamientos de control sobre los desarrollos Low-Code / No-Code impide mapear de forma integral estos aplicativos como activos de información de la DIAN, lo que genera zonas ciegas en la detección de incidentes y brechas de seguridad que exponen a riesgos latentes la confidencialidad, integridad y disponibilidad de los datos institucionales.
		H5. Falencias en la Gestión de la Continuidad del Negocio.	C6. Monitorear los eventos de los sistemas de información de la DIAN que puedan generar un incidente de seguridad y privacidad de la información, que atente contra la confidencialidad, integridad o disponibilidad de los activos de información. C7. Realizar evaluaciones de vulnerabilidades.	E	Al operar estos controles de seguridad de manera aislada y no orientados a la resiliencia operativa, la identificación de brechas técnicas o incidentes críticos de seguridad no activa de forma ágil las estrategias de contingencia institucionales, lo que incrementa la probabilidad de que un evento adverso afecte la disponibilidad a largo plazo y prolongue los tiempos de interrupción de los procesos de negocio.
Matriz Subproceso Operación Logística V4	R3. Información afectada en su integridad y/o confidencialidad y/o disponibilidad	H1. Indisponibilidad total o parcial en soluciones tecnológicas ADA Web.	C54. Reportar oportunamente el incidente al área de servicios tecnológicos C55. Solicitar la declaratoria de contingencia del área de servicios tecnológicos C56. Asegurar que los tramites manuales llevados a cabo durante la contingencia se incorporen en los servicios informáticos una vez se reestablezcan	E	La falta de un flujo inmediato para reportar el incidente al área de servicios tecnológicos (C54) retrasa la declaratoria formal de contingencia (C55), comprometiendo la disponibilidad del servicio; asimismo, las debilidades en los mecanismos para asegurar la posterior incorporación de los trámites manuales en los servicios informáticos (C56) elevan el riesgo de pérdida, duplicidad o alteraciones en la integridad de los datos una vez restablecida la operación.

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co

Matriz Subproceso Asistencia al Usuario V2	R2. Canales de servicio institucionales con inconvenientes en términos de calidad y oportunidad en la atención.	H1. Indisponibilidad total o parcial en soluciones tecnológicas Sistema de Agendamiento de Citas (Digiturno).	C1. Registrar el incidente detectado en la herramienta de gestión de la mesa de servicio de acuerdo al PR-IIT-0458 Gestión de Incidentes y PR-IIT-0454 Disponibilidad de la operación tecnológica. C8. "*Analizar la situación con el fin de identificar las afectaciones que impacten la prestación del servicio CT-CAC-0056 Cartilla de Atención Presencial. En caso de ser necesario, activar el protocolo de manejo de incidentes e identificación de crisis OD-PEC-0003 y Protocolo de manejo de crisis OD-PEC-0004*."	E	La falta de sincronización obstaculiza la activación ágil y oportuna de los protocolos de manejo de incidentes e identificación de crisis (OD-PEC-0003 y OD-PEC-0004), prolongando la afectación del servicio al ciudadano y comprometiendo la trazabilidad de los datos de la operación.
Matriz Subproceso Factura Electrónica y Servicios Digitales V1	R2. Información afectada en su integridad y/o confidencialidad y/o disponibilidad	H1. Indisponibilidad total o parcial en soluciones tecnológicas Factura Electrónica.	C9. Reportar oportunamente el incidente al área de servicios tecnológicos C10. Decretar Situación de Contingencia dando aplicación al instructivo IN-IIT-0254 "Gestión de incidentes masivos, mayores y problemas" y a los procedimientos PR-IIT-0458 "Gestión de incidentes" y PR-IIT-0454 "Disponibilidad de la operación tecnológica".	E	Las demoras en el reporte oportuno del incidente al área de servicios tecnológicos (C9) retrasan directamente la activación de los mecanismos para decretar la Situación de Contingencia (C10), cuya declaración formal depende de la aplicación estricta del instructivo de incidentes masivos (IN-IIT-0254) y los procedimientos de gestión de incidentes y disponibilidad (PR-IIT-0458 y PR-IIT-0454); esta desarticulación prolonga el tiempo de caída de la plataforma, impactando la continuidad del servicio fiscal y la seguridad de los datos transaccionales.
Matriz Subproceso Recaudo - Devoluciones V5	R7. Información afectada en su integridad y/o confidencialidad y/o disponibilidad	H1. Indisponibilidad total o parcial en soluciones tecnológicas CCC20 - Cuenta Corriente Contribuyente, SIPAC, OBLIGA, SISCOBRA - Obligación Financiera.	C75. Decretar Situación de Contingencia dando aplicación a los instructivos IN-IIT-0254 "*Gestión de incidentes masivos, mayores y problemas*", IN-IIT-0253 "*Gestión de incidentes de seguridad digital*", IN-IIT-0255 "*Gestión de incidentes y problemas asociados a las soluciones tecnológicas*" y a los procedimientos PR-IIT-0458 "Gestión de incidentes" y PR-IIT-0454 Disponibilidad de la operación tecnológica.	E	Debilidades en la oportunidad y aplicación del control para decretar la Situación de Contingencia (C75). Al presentarse fallas imprevistas en estos sistemas de Obligación Financiera, se evidencia un rezago en la activación articulada de los instructivos para incidentes masivos y mayores (IN-IIT-0254), seguridad digital (IN-IIT-0253), e incidentes asociados a ST (IN-IIT-0255), así como de los procedimientos de gestión de incidentes y disponibilidad (PR-IIT-0458 y PR-IIT-0454); esta falta de agilidad institucional prolonga el tiempo de suspensión de los servicios financieros y de cobro, comprometiendo la trazabilidad y la seguridad de los datos de los contribuyentes.

Fuente: Matrices Operaciones DIAN.
Elaboró: Equipo auditor.
E=Exposición M= Materialización

Oficina de Control Interno
Carrera 8 # 6C-38. Piso 6. Edificio San Agustín | PBX 601 4823294 - (+57) 3009140830
Código postal 111711
www.dian.gov.co