

INFORME GERENCIAL AUDITORÍA A LA GESTIÓN DE ACCESOS AGA 2025-002

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 2025, 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.

2. OBJETIVOS

2.1 Objetivo General

Desarrollar auditoría basada en riesgos al control de acceso de usuarios a las plataformas tecnológicas, soluciones tecnológicas y/o redes de comunicaciones de la infraestructura de la UAE DIAN, que apoyan los procesos misionales para preservar la disponibilidad, integridad y confidencialidad de la información de la Entidad.

2.2 Objetivos Específicos

1. Verificar la gestión de accesos a usuarios internos y externos o terceros (considerando contratistas, proveedores, pasantes, convenios, entes de control, Operadores Económicos Autorizados - OEA's, Usuarios Aduaneros con Trámite Simplificado - UTS's) de la UAE DIAN, con permisos a los sistemas de información, instalaciones de procesamiento de información y/o a la información disponible en la infraestructura tecnológica de la Entidad.
2. Verificar las actividades de control ejecutadas por los procesos responsables para la inactivación de usuarios y roles de soluciones tecnológicas, considerando funcionarios en situaciones administrativas, contratistas, proveedores, pasantes, convenios, entes de control; determinando, la necesidad en la extensión del plazo o inactivación del (los) rol(es) asignado(s) según corresponda, con el fin de identificar oportunidades de mejora en el proceso.
3. Evaluar la asignación, control y cumplimiento de requisitos de los derechos de accesos privilegiados.
4. Verificar que los accesos a la infraestructura de red de la UAE-DIAN en el Nivel Central, cumplan con controles de seguridad establecidos, en lo relacionado a la gestión de accesos de los equipos de red, conexiones remotas, VPN's, TrendVision, WebServices, accesos a terceros y en atención a las políticas de seguridad de la información.

5. Evaluar los sistemas de información o herramientas que apoyan al procedimiento de gestión de accesos, bajo los principios de las políticas de gobierno digital y de seguridad digital (integridad, confidencialidad, disponibilidad y autenticidad), con el fin de asegurar el cumplimiento normativo de la DIAN y fortalecer el Sistema de Control Interno de la Entidad.
6. Evaluar los componentes del Sistema de Control Interno y la implementación de las políticas del Modelo Integrado de Planeación y Gestión – MIPG V6, que apliquen en los procedimientos auditados.
7. Fortalecer las actividades de fomento a la cultura del control, para la mejora continua del proceso auditado.

3. ALCANCE

La auditoría a la gestión de accesos AGA-2025-002, se llevó a cabo entre el 17 de febrero y el 25 de julio de 2025, para el período comprendido entre el 01 de enero de 2024 y el 15 de marzo de 2025, de manera presencial a las direcciones seccionales de: Aduanas de Bogotá – Aeropuerto El Dorado, de Impuestos y de Aduanas de Barranquilla, de Impuestos y de Aduanas de Cartagena e Impuestos y Aduanas de Buenaventura, al Datacenter sitio dos (2) de la Dirección de Gestión de Innovación y Tecnología (DGIT); y de manera virtual a siete (7) Direcciones de Gestión, la Dirección Operativa de Grandes Contribuyentes (DOGC), la Subdirección de Gestión del Empleo Público y 43 Direcciones Seccionales, en el marco de los procedimientos: “*Gestión de Accesos PR-IIT-0455 V3*” y de “*Gestión de activos de información PR-IIT-0366 V6*”, entre otros.

4. DESARROLLO DE LA AUDITORÍA

A partir de las fuentes de información, se realizaron verificaciones sobre la oportunidad en la activación e inactivación de roles en las soluciones tecnológicas, roles privilegiados, cuentas de usuarios de Directorio Activo, cuentas de correo electrónico, VPN¹s, cuentas de accesos a dispositivos de red, cumplimiento de las políticas de seguridad en los atributos de integridad, confidencialidad y disponibilidad establecidos en el MN-IIT-0072 V5.

La selección de muestras se efectuó atendiendo los criterios de riesgos previamente definidos en el ejercicio auditor y como producto del análisis se generaron los resultados plasmados en el presente informe.

5. RELACIÓN DE HALLAZGOS

Como resultado de la auditoría, se identificaron trece (13) situaciones encontradas que fueron dadas a conocer a los auditados mediante correo del 20 de junio de 2025, frente a las cuales, los procesos auditados tuvieron la oportunidad de ejercer el derecho a la contradicción y presentar observaciones que, una vez analizadas por el equipo auditor, dieron lugar a la configuración de doce (12) hallazgos.

¹ Red Privada Virtual.

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

1. Coherencia entre el Anexo "*Roles de las soluciones tecnológicas según procedimientos y procesos*" y los reportes "*Roles Activos Usuarios DIAN*".
2. Deficiencias en la gestión de roles informáticos en las soluciones tecnológicas institucionales.
3. Deficiencias en la depuración de roles en sistemas corporativos que no figuran en los reportes "*Roles Activos Usuarios DIAN*".
4. Deficiencias en la gestión de aplicativos no corporativos.
5. Uso de aplicativo público no institucional Portal SAR (D).
6. Falencias en la gestión de accesos y suplantación de usuarios en el Sistema RUT (D).
7. Debilidades en la gestión de roles asignados en periodos de situaciones administrativas superiores a 15 días calendario (P).
8. Cuentas activas sin uso, vinculadas a funcionarios con situaciones administrativas o retirados de la Entidad o terceros con relación terminada.
9. Deficiencias en la seguridad de los logs de las contraseñas y manejo de usuarios de prueba en producción en las bases de datos de SYGA Siglo XXI.
10. Deficiencias en la aplicación de políticas de seguridad de información en las terminales de autogestión (Kioscos).
11. Deficiencias en la gestión de cuentas institucionales con inactividad prolongada en servicios como VPN y plataforma de correo electrónico Institucional a nivel nacional.
12. Incumplimiento en la prestación del servicio "*Zona WiFi Gratis para la Gente*".

6. CONCLUSIONES

La Información constituye actualmente uno de los activos más importantes para planeación, gestión y toma de decisiones en las organizaciones; por tal razón, es necesario fortalecer los controles que garanticen la seguridad de ésta en los atributos de integridad, confidencialidad y disponibilidad.

En virtud de lo anterior y teniendo en cuenta que, uno de los elementos esenciales en esta estructura corresponde a la gestión de accesos, la presente auditoría abordó este aspecto, mediante la ejecución de un objetivo general y siete (7) específicos, permitiendo identificar tanto fortalezas, como retos que se deben atender desde las cuatro líneas de defensa a nivel institucional, en un esquema de gestión por procesos bajo el modelo estratégico de

“*Alineación Total*” implementado por la entidad, dando lugar a 12 hallazgos, dos (2) con presunta incidencia disciplinaria y uno (1) con incidencia penal.

Es importante resaltar que la entidad cuenta con políticas, procedimientos, instructivos, cartillas y manuales, que dan orientaciones sobre la gestión de accesos a los diferentes macroprocesos, procesos y subprocesos institucionales.

Como resultado de los objetivos específicos del 1 al 5, desarrollados en la auditoría se identificaron falencias que deben ser atendidas, con el fin controlar la exposición y/o materialización de riesgos, relacionados con: falta de coherencia entre el Anexo “*Roles de las soluciones tecnológicas*” y los reportes “*Roles Activos Usuarios DIAN*”; deficiencias en la gestión de roles informáticos; uso de un aplicativo no autorizado por la entidad; suplantación de usuarios en el sistema RUT; uso de aplicativos no corporativos o huérfanos para suplir funcionalidades no cubiertas por los institucionales y brechas de seguridad en algunos de estos; deficiencias en la seguridad de las contraseñas y uso de usuarios de prueba en ambientes producción; deficiencias en la seguridad de la información en las terminales de autogestión; deficiencias en la gestión de cuentas institucionales con inactividad prolongada en servicios de VPN y plataforma de correo electrónico; e incumplimiento en la prestación del servicio “*Zona WiFi Gratis para la Gente*” en algunos de los puntos de contacto.

En cuanto a la evaluación de los componentes del Sistema de Control Interno, enmarcado en el objetivo 6, se observan oportunidades de mejora, entre otras, en lo relacionado con la claridad que se debe dar a algunos incisos del procedimiento “*Gestión de Accesos PR-IIT-0455 V3*”; la armonización de este con el “*Manual de Políticas y Lineamientos de Seguridad de la Información MN-IIT-0072 V5*”; la necesidad de actualización de la Resolución 484 de 2013; actualización de los procedimientos y matrices de riesgos con el actual Mapa de Procesos; el aprovechamiento de la herramienta de protección de bases de datos en las soluciones tecnológicas; la necesidad de la apropiación de MN-IIT-0072 V5 por parte de todos los funcionarios, para fortalecer la seguridad de la entidad y evitar estar inmersos en posibles sanciones de tipo disciplinario, fiscal o penal; y el cumplimiento a cabalidad de los lineamientos del mismo.

Dada la materialización de riesgos, y conforme a los resultados de correlación entre riesgos y controles, se recomienda actualizar las matrices de riesgos institucionales, la cual debe orientarse a identificar, evaluar y gestionar los riesgos y sus respectivos controles, con el fin de mitigar la probabilidad de ocurrencia de eventos adversos que puedan afectar el cumplimiento de los objetivos institucionales; así mismo, analizar la procedencia de remisión a los órganos competentes.

Con respecto al objetivo 7, se realizó sensibilización en “*Fomento de la cultura del Control*”, con una participación de **236** funcionarios, a nivel nacional, en donde se fortalecieron conocimientos relacionados con la gestión de accesos y el control interno.

7. RECOMENDACIONES

Sin perjuicio de las recomendaciones realizadas en cada uno de los hallazgos y oportunidades de mejora, se considera atender los lineamientos y normatividad vigente en



la DIAN en materia de gestión de accesos, en especial los relacionados con el “Manual de Políticas y Lineamientos de Seguridad de la Información MN-IIT-0072 V5” y el “Procedimiento de Gestión de Accesos PR-IIT-0455 V3”; así como también, fortalecer la apropiación y aplicación del “Código de Integridad de la DIAN CG-TAH-0002 V3” y la revisión permanente de las matrices de riesgos contemplando controles que aseguren el efectivo tratamiento, a fin de evitar la exposición o materialización de estos.

ENRIQUE CASTIBLANCO BEDOYA
Jefe Oficina de Control de interno

Proyectó: Equipo Auditor.
Yamile Fresno Forero
Edgar Javier Ríos Molina
Sandra del Pilar Chuquín Badillo – Líder
Juan Felipe Solórzano García – Apoyo Análisis de datos
Revisó: Juan Rafael Lozano Rodríguez – Evaluador Despacho OCI
Claudia Marcela Quiceno Duque – Jefe Coordinación Auditoría Integridad



OFICINA DE CONTROL INTERNO

**INFORME DE
AUDITORÍA A LA GESTIÓN DE ACCESOS
AGA 2025-002**

**PERIODO AUDITADO
01 DE ENERO DE 2024 A 15 DE MARZO DE 2025**

**ENRIQUE CASTIBLANCO BEDOYA
JEFE DE OFICINA**

**CLAUDIA MARCELA QUICENO DUQUE
JEFE COORDINACIÓN DE AUDITORÍA INTEGRAL**

**EQUIPO AUDITOR:
YAMILE FRESNO FORERO
EDGAR JAVIER RÍOS MOLINA
SANDRA DEL PILAR CHUQUÍN BADILLO – LÍDER**

**APOYO ANÁLISIS DE DATOS
JUAN FELIPE SOLÓRZANO GARCÍA**

**EVALUADOR DESPACHO
JUAN RAFAEL LOZANO RODRÍGUEZ**

BOGOTÁ, JULIO DE 2025

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

Formule su petición, queja, sugerencia o reclamo en el Sistema PQSR de la DIAN

CONTENIDO

	Pág.
1. DESCRIPCIÓN GENERAL.....	3
2. OBJETIVOS	3
2.1 Objetivo General	3
2.2 Objetivos Específicos	3
3. ALCANCE	4
4. DESARROLLO DE LA AUDITORÍA.....	4
5. RELACIÓN DE HALLAZGOS	4
6. EVALUACIÓN DE LOS COMPONENTES DEL SISTEMA DE CONTROL INTERNO	24
6.1 Ambiente de control	24
6.2 Evaluación del Riesgo	25
6.3 Actividades de Control	26
6.4 Información y Comunicación	27
6.5 Actividades de Monitoreo.....	28
7. FOMENTO DE LA CULTURA DEL CONTROL	28
8. RECOMENDACIONES PARTICIPACIÓN CONCURRENTE DE LA OFICINA DE SEGURIDAD DE LA INFORMACIÓN Y LA AUDITORÍA AGA2025002	28
9. CONCLUSIONES.....	29
10. RECOMENDACIONES	30
ANEXO 1. Correlación de riesgos y controles, asociados a los hallazgos identificados.....	31

AUDITORÍA A LA GESTIÓN DE ACCESOS AGA 2025-002

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 2025, 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.

2. OBJETIVOS

2.1 Objetivo General

Desarrollar auditoría basada en riesgos al control de acceso de usuarios a las plataformas tecnológicas, soluciones tecnológicas y/o redes de comunicaciones de la infraestructura de la UAE DIAN, que apoyan los procesos misionales para preservar la disponibilidad, integridad y confidencialidad de la información de la Entidad.

2.2 Objetivos Específicos

1. Verificar la gestión de accesos a usuarios internos y externos o terceros (considerando contratistas, proveedores, pasantes, convenios, entes de control, Operadores Económicos Autorizados - OEA's, Usuarios Aduaneros con Trámite Simplificado - UTS's) de la UAE DIAN, con permisos a los sistemas de información, instalaciones de procesamiento de información y/o a la información disponible en la infraestructura tecnológica de la Entidad.
2. Verificar las actividades de control ejecutadas por los procesos responsables para la inactivación de usuarios y roles de soluciones tecnológicas, considerando funcionarios en situaciones administrativas, contratistas, proveedores, pasantes, convenios, entes de control; determinando, la necesidad en la extensión del plazo o inactivación del (los) rol(es) asignado(s) según corresponda, con el fin de identificar oportunidades de mejora en el proceso.
3. Evaluar la asignación, control y cumplimiento de requisitos de los derechos de accesos privilegiados.
4. Verificar que los accesos a la infraestructura de red de la UAE-DIAN en el Nivel Central, cumplan con controles de seguridad establecidos, en lo relacionado a la gestión de accesos de los equipos de red, conexiones remotas, VPN's, TrendVision, WebServices, accesos a terceros y en atención a las políticas de seguridad de la información.

5. Evaluar los sistemas de información o herramientas que apoyan al procedimiento de gestión de accesos, bajo los principios de las políticas de gobierno digital y de seguridad digital (integridad, confidencialidad, disponibilidad y autenticidad), con el fin de asegurar el cumplimiento normativo de la DIAN y fortalecer el Sistema de Control Interno de la Entidad.
6. Evaluar los componentes del Sistema de Control Interno y la implementación de las políticas del Modelo Integrado de Planeación y Gestión – MIPG V6, que apliquen en los procedimientos auditados.
7. Fortalecer las actividades de fomento a la cultura del control, para la mejora continua del proceso auditado.

3. ALCANCE

La auditoría a la gestión de accesos AGA-2025-002, se llevó a cabo entre el 17 de febrero y el 25 de julio de 2025, para el período comprendido entre el 01 de enero de 2024 y el 15 de marzo de 2025, de manera presencial a las direcciones seccionales de: Aduanas de Bogotá – Aeropuerto El Dorado, de Impuestos y de Aduanas de Barranquilla, de Impuestos y de Aduanas de Cartagena e Impuestos y Aduanas de Buenaventura, al Datacenter sitio dos (2) de la Dirección de Gestión de Innovación y Tecnología (DGIT); y de manera virtual a siete (7) Direcciones de Gestión, la Dirección Operativa de Grandes Contribuyentes (DOGC), la Subdirección de Gestión del Empleo Público y 43 Direcciones Seccionales, en el marco de los procedimientos: “*Gestión de Accesos PR-IIT-0455 V3*” y de “*Gestión de activos de información PR-IIT-0366 V6*”, entre otros.

4. DESARROLLO DE LA AUDITORÍA

A partir de las fuentes de información, se realizaron verificaciones sobre la oportunidad en la activación e inactivación de roles en las soluciones tecnológicas, roles privilegiados, cuentas de usuarios de Directorio Activo, cuentas de correo electrónico, VPN¹s, cuentas de accesos a dispositivos de red, cumplimiento de las políticas de seguridad en los atributos de integridad, confidencialidad y disponibilidad establecidos en el MN-IIT-0072 V5.

La selección de muestras se efectuó atendiendo los criterios de riesgos previamente definidos en el ejercicio auditor y como producto del análisis se generaron los resultados plasmados en el presente informe.

5. RELACIÓN DE HALLAZGOS

Como resultado de la auditoría, se identificaron trece (13) situaciones encontradas que fueron dadas a conocer a los auditados mediante correo del 20 de junio de 2025, frente a las cuales, los procesos auditados tuvieron la oportunidad de ejercer el derecho a la contradicción y presentar observaciones que, una vez analizadas por el equipo auditor, dieron lugar a la configuración de doce (12) hallazgos.

¹ Red Privada Virtual.

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

Hallazgo 1. Coherencia entre el Anexo "Roles de las soluciones tecnológicas según procedimientos y procesos" y los reportes "Roles Activos Usuarios DIAN".

Responsable: Dirección de Gestión de Innovación y Tecnología.

Verificada la relación entre el anexo "*Roles de las soluciones tecnológicas según procedimientos y procesos V4_R011*" y los reportes "*Roles Activos Usuarios DIAN*", con corte a febrero y marzo de la vigencia 2025 se evidenció:

a. 117 códigos de rol en el reporte de "*Roles activos usuarios DIAN*" plataforma MUISCA, 424 códigos de rol en el reporte de la plataforma SIAT, 82 en el Sistema SIGLO XXI, uno (1) en SIFARO y cuatro (4) en el Sistema KACTUS, asignados a usuarios internos, que no se encuentran relacionados en el Anexo "*Roles de las soluciones tecnológicas según procedimientos y procesos_V4_R011*", en consecuencia no es posible determinar, a través de esta herramienta, la solución tecnológica a la que pertenecen ni la funcionalidad que ejecutan.

b. Falta de completitud en los reportes de "*Roles activos usuarios DIAN*" debido a que no se observa la relación de asignaciones de roles a usuarios en las soluciones tecnológicas: "*Bitácora SYGA*", "*Administración de contratos*", "*Formulación Análisis de operaciones*", "*Control EAR*", "*DEVYCOM*" y "*Anotaciones fiscales*", de la muestra de soluciones tecnológicas seleccionadas y establecidas en el "*Anexo Roles (...)*".

c. Reportes de "*Roles activos usuarios DIAN*" de las plataformas MUISCA y algunos de SIAT que no relacionan la solución tecnológica a la que pertenece cada uno de los roles, lo que dificulta la identificación.

d. Falta de estandarización entre los roles establecidos en el "*Anexo Roles (...)*" y los reportes "*Roles activos usuarios DIAN*", encontrándose diferencias en la nomenclatura utilizada entre los instrumentos, como por ejemplo: en anexo de roles figura el rol "*(Básico 1279 - Concreto 1280)*", mientras que en el reporte "*Roles activos usuarios DIAN*" figura "*1279*", lo que dificulta el cruce de información; y la nomenclatura utilizada en los campos, como por ejemplo, en "*Dirección Seccional*", para unas registra el nombre completo, en otros abreviado o solamente de la ciudad.

(Ver anexo: "Roles_asignados_No_Encontrados_Anexo" en la carpeta DGIT-OSI).

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 1. Elementos del hallazgo No. 1.

Criterios	Directiva Presidencial 02 de 2022, directriz 2, controles de la Norma NTC-ISO/IEC 27001:2022 Anexo A y de la Guía GTC-ISO/IEC 27002:2022, MN-IIT-0072 V5 ² , PR-IIT-0455 V3 ³ , MSPI V4 ⁴ , relacionados con controles de "Gestión de identidad".
Dimensiones MIPG V6	Dimensión 3 "Gestión con Valores para Resultados" en las políticas: "Gobierno Digital" y "Seguridad Digital".
Causas	Falta de articulación entre la DGIT y los procesos responsables para la gestión de roles en el nivel central; carencia de herramientas automatizadas; deficiencias en el seguimiento y control de los roles asignados; desactualización del "Anexo Roles (...)" ; falta de completitud de la información de los roles en el reporte "Roles Activos Usuarios DIAN" y estandarización en la nomenclatura de campos.
Efectos	Limitación en el adecuado control y seguimiento de los roles asignados; dificultad en la identificación de los roles y la generación de reportes de forma automática.
Riesgos	Exposición al riesgo R4. "Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información", del Subproceso Innovación y Tecnología y R3 "Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad y disponibilidad de los datos", del Subproceso de Seguridad de la información.

Fuente: Elaborado por el equipo auditor.

Recomendaciones:

- Incluir todos los roles de las soluciones tecnológicas institucionales en el Anexo "Roles de las soluciones tecnológicas según procedimientos y procesos (...)", versión vigente.
- Incluir todas las soluciones tecnológicas institucionales y sus respectivos roles en los reportes de "Roles activos usuarios DIAN" e incluir una columna que indique la solución tecnológica a la que pertenece cada rol.
- Crear reportes con todos los roles asignados a terceros en las soluciones tecnológicas institucionales y herramientas de apoyo (Soporte TIC, GRC), tales como: contratistas por prestación de servicio, entes de control externo (CGR, ITRC), pasantes, POLFA, personal provisto por proveedores, judicantes, aprendices, etc., incluyendo una columna que permita determinar el tipo de relación que tienen con la DIAN.
- Estandarizar la información de los catálogos (Nombres de dependencia, roles) para que se facilite la generación de reportes, construcción de herramientas de inteligencia de negocios y cuadros de mando para la toma de decisiones basada en la información.
- Ajustar la periodicidad de la generación de los reportes "Roles Activos Usuarios DIAN" con frecuencias y fechas constantes, preferiblemente semanal, de manera que se cuente con información que facilite la toma de decisiones, en atención a una necesidad generalizada expresada por los auditados.

Hallazgo 2. Deficiencias en la gestión de roles informáticos en las soluciones tecnológicas institucionales.

Responsable: Dirección de Gestión de Innovación y Tecnología.

Corresponsables: Direcciones de Gestión, Operativa y Direcciones Seccionales.

- a. En el reporte "Roles activos usuarios DIAN", con corte a 07 de marzo de 2025, en

² Manual de Políticas y Lineamientos de Seguridad de la Información.

³ Procedimiento de Gestión de Accesos.

⁴ Modelo de Seguridad y Privacidad de la Información.

plataforma MUISCA se evidenciaron 14 exfuncionarios con roles activos, ubicados en: Dirección de Gestión de Impuestos (DGI), Dirección de Gestión de Aduanas (DGA), Dirección de Gestión Operativa de Grandes Contribuyentes (DOGC); ; Dirección Seccional de Impuestos (DSI) Bogotá; Direcciones Seccionales de Aduanas (DSA): Bogotá, Barranquilla, Cali; Direcciones Seccionales de Impuestos y Aduanas (DSIA): Ibagué, Manizales, Villavicencio. (Ver Anexo: "EX_rolés_activos_MUISCA" de Direcciones de Gestión, Operativa y Direcciones Seccionales).

b. En el reporte "*Roles activos usuarios DIAN*", con corte a 07 de marzo de 2025, en la plataforma MUISCA se evidenciaron 19 usuarios, no encontrados en planta, clasificados como funcionarios, ubicados en: DGI, DGIT, OTROS-DGIT, DOGC, DSIA Ipiales, DSIA Sincelejo. (Ver anexo: "NE_planta_MUISCA" de Direcciones de Gestión, Operativa y Direcciones Seccionales).

c. En el reporte "*Roles activos usuarios DIAN*", con corte a 01 de marzo de 2025, en la plataforma SIAT, se evidenciaron un total de 74 usuarios no encontrados en planta de personal, ubicados en: DGC, DGI, POLFA, OTROS-DGIT, DOGC; DSA: Barranquilla, Cartagena, Medellín; DSI: Barranquilla, Bogotá, Cali, Cartagena, Medellín; DSIA: Bucaramanga, Ipiales, Pasto, Pereira, Rihacha, Santa Marta, Tunja, Urabá, Valledupar. Algunos casos corresponden a funcionarios de entes de control externo (CGR), según respuesta a situaciones encontradas. (Ver anexo: "NE_planta_SIAT" por Direcciones de Gestión, Operativa y Direcciones Seccionales).

d. En el reporte "*Roles activos usuarios DIAN*", con corte a 28 de febrero de 2025, en la solución tecnológica SIFARO se evidenciaron 228 usuarios, no encontrados en la planta activa de personal, ubicados en las siguientes dependencias: DGF, DOGC; DSA: Aeropuerto El Dorado, Medellín, Bogotá, Cali, Cartagena, Barranquilla, Cúcuta; DSI: Medellín, Bogotá, Barranquilla; DSIA: Buenaventura, Manizales, Santa Marta, San Andrés, Yopal, Pasto, Ipiales, Bucaramanga, Armenia, Palmira, Montería, Maicao, Valledupar, Villavicencio, Tumaco, Pereira; Dirección Seccional Delegada de Impuestos y Aduanas (DSDIA) Leticia; Pamplona. (Ver anexos: Archivo "SIFARO" de cada Dirección de Gestión o Seccional).

e. Falta de reportes que evidencien los roles asignados a terceros relacionados con la entidad, a los que se asignan roles en soluciones tecnológicas; tales como contratistas, proveedores, personal provisto por proveedores en el marco de contratos u órdenes de compra, auditores de entes de control, pasantes, judicantes, usuarios *ad honorem*, funcionarios de la POLFA, que prestan servicio a la entidad sin vínculo laboral con la DIAN; no obstante, se evidenciaron casos de contratistas y personal de entes de control externo relacionados en los reportes de "*Roles activos usuarios DIAN*" clasificados como funcionarios, sin que se observe un criterio que indique esta situación.

f. Falta de claridad sobre cómo proceder con la inactivación de dos (2) roles en el sistema SIAT denominados "CONNECT" y "ROLCON", compartidos y necesarios para el uso de las soluciones tecnológicas que pertenecen a esta plataforma; sin embargo, por sí solos no están asociados a una determinada solución tecnológica ni funcionalidad.

g. Roles en la plataforma SIAT que han sido desactivados mediante solicitud y nuevamente figuran activos en posteriores reportes de "*Roles activos usuarios DIAN*", generando reprocesos y riesgos de uso de estos.

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 2. Elementos del hallazgo No. 2.

Criterios	Directiva Presidencial 02 de 2022, directriz 2, controles de la Norma NTC-ISO/IEC 27001:2022 Anexo A y de la Guía GTC-ISO/IEC 27002:2022, MN-IIT-0072 V5, PR-IIT-0455 V3, MSPI V4, relacionados con controles de " <i>Gestión de identidad</i> ".
Dimensiones MIPG V6	Dimensión 3 " <i>Gestión con Valores para Resultados</i> " en las políticas: " <i>Gobierno Digital</i> " y " <i>Seguridad Digital</i> ".
Causas	Fallas en la sincronización entre el Sistema KACTUS y la plataforma MUISCA; falta de integración entre el Sistema KACTUS y las plataformas SIAT, Siglo XXI, SIFARO; desactualización del Anexo de Roles (...); ausencia de campos en los reportes " <i>Roles Activos usuarios DIAN</i> " que permitan identificar el tipo del usuario (funcionario DIAN, funcionario de ente de control externo, nombre del ente de control externo, contratista, pasante, judicante, <i>ad honorem</i>); falta de aplicación del lineamiento 5.1.18 Derechos de Acceso literal c) del MN-IIT-0072 V5.
Efectos	No se garantiza que los roles estén activos únicamente para quienes lo requieran en el desempeño de las labores asignadas y limitación en el adecuado control y seguimiento,
Riesgos	Exposición al riesgo R4 " <i>Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información</i> ", del Subproceso Innovación y Tecnología V3.

Fuente: Elaborado por el equipo auditor.

Recomendaciones:

- Ajustar la interfaz KACTUS – MUISCA para asegurar la activación e inactivación oportuna de roles, en cumplimiento de lo establecido en el procedimiento "*Gestión de accesos PR-IIT-0455 V3*" a cargo de la Subdirección de Gestión del Empleo Público (SGEP), con el acompañamiento de la Subdirección de Soluciones y Desarrollo (SSD) e implementar mecanismos de alerta oportuna ante eventuales fallas.
- Poner en operación la interfaz KACTUS - SIAT, según lo establecido en los procedimientos "*Gestión de Accesos PR-IIT-0455 V3*" y "*Gestión de requerimientos PR-IIT-0460 V4*", para la activación e inactivación de roles.
- Implementar el sistema centralizado de identidades, mediante el cual se asignen los roles de acceso a los sistemas de información actuales y aquellos que se implementen en la ejecución del Programa de Modernización, de acuerdo con las funciones de cada usuario interno, a cargo de la OSI, según lo establecido en el numeral "*5.1.18 Derechos de acceso*", literal b, del MN-IIT-0072 V5.
- Considerar la implementación de la interfaz con KACTUS, en las soluciones tecnológicas que actualmente no cuentan con esta (SYGA SIGLO XXI, PQRS Dynamic 365, SIFARO, Digiturno, entre otros), con el fin de realizar la activación e inactivación automática de roles.
- Establecer el lineamiento para la inactivación de roles asignados a usuarios que figuran en los reportes de "*Roles activos usuarios DIAN*", que a la fecha no tienen relación activa con la entidad.

- Realizar seguimiento periódico de los usuarios y roles existentes en las soluciones tecnológicas, para verificar la correcta ejecución del PR-IIT-0455 V3 y en caso de encontrar usuarios y/o roles activos sin el cumplimiento de los requisitos, solicitar la suspensión de estos, por parte de la OSI, como lo establece el mismo, en el numeral 3.2 Roles de soluciones tecnológicas, ítem 16.

Hallazgo 3. Deficiencias en la depuración de roles en sistemas corporativos que no figuran en los reportes "Roles Activos Usuarios DIAN"

Responsable: Dirección de Gestión de Innovación y Tecnología.

Corresponsable: Direcciones de Gestión, Operativa y Direcciones Seccionales.

Revisada una muestra de soluciones tecnológicas cuyos roles no figuran en los reportes de "Roles Activos Usuarios DIAN", se seleccionó la solución tecnológica "Bitácora SYGA" con corte 15/03/2025, remitidos por la Subdirección de Control y Registro Aduanero; identificando (12) usuarios con roles que no fueron encontrados activos en la planta de personal de la entidad, según reportes de los cortes suministrados por la SGEP, distribuidos de la siguiente manera: DGA, DOGC, DSA Medellín y DSI Bogotá . (Ver Anexos: Archivos "Bitácora" de cada Dirección de Gestión, Operativa o Seccional).

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 3. Elementos del hallazgo No. 3.

Criterios	Directiva Presidencial 02 de 2022, directriz 2, controles de la Norma NTC-ISO/IEC 27001:2022 Anexo A y de la Guía GTC-ISO/IEC 27002:2022, MN-IIT-0072 V5, PR-IIT-0455 V3, MSPI V4, relacionados con controles de "Gestión de identidad".
Dimensiones MIPG V6	Dimensión 3 "Gestión con Valores para Resultados" en las políticas: "Gobierno Digital" y "Seguridad Digital".
Causas	Falta de inclusión de los roles asignados en Bitácora SYGA en los reportes "Roles Activos Usuarios DIAN"; deficiencias en el proceso de revisión y depuración de roles y perfiles; falta de herramientas de control y supervisión en la asignación de los roles.
Efectos	Limita el adecuado control y seguimiento de los roles asignados, así como la revisión y depuración de roles y perfiles de las soluciones tecnológicas.
Riesgos	Exposición a los riesgos: R4. "Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información"; R5. "Información usada de manera indebida para beneficio propio o de terceros", del Subproceso Innovación y Tecnología V3; 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:

- Incluir todas las soluciones tecnológicas institucionales y sus respectivos roles en los reportes de "Roles activos usuarios DIAN".

Hallazgo 4. Deficiencias en la gestión de aplicativos no corporativos.

Responsables: Dirección de Gestión de Innovación y Tecnología, Oficina de Seguridad de la Información.
Corresponsables: Direcciones de Gestión, Operativa y Direcciones Seccionales.

Se evidenciaron aplicativos no corporativos que, según Memorando No. 000203 del 13 de noviembre de 2020 de la Oficina de Seguridad de Información de la DIAN, se definen como: *"Las herramientas de soporte no corporativas corresponden a todos aquellos desarrollos generados (por ejemplo, en Visual Basic, Access o cualquier otra herramienta informática) sin asesoría o participación por parte de la Subdirección de Gestión de Tecnología de Información y Telecomunicaciones - SGTIT y que actualmente se encuentran operativas en forma paralela a los sistemas de información administrados por la SGTIT⁵"*, con las siguientes situaciones:

a. Aplicativos que se ejecutan en sistemas operativos antiguos: versiones de Windows Server 2000, 2003 y Windows 7 e implementados en versiones de Access 2000 y 2010, no soportadas por el fabricante, lo que impide que se reciban nuevas actualizaciones, correcciones, alertas de seguridad y parches críticos.

b. Un aplicativo no corporativo que opera en un servicio en *"nube Render"*, con plan *"free Hobby"*, el cual no se encuentra en la infraestructura de la entidad. (DSI Cali).

c. Un aplicativo no corporativo denominado *"Conhora"* utilizado para el registro y control de horario de los funcionarios; no obstante, las direcciones seccionales auditadas manifiestan la necesidad del uso de este, debido a que el Sistema KACTUS no contempla funcionalidades como generación de reportes de liquidación de horas extras y trabajo suplementario; sin embargo, el sistema operativo y motor de base de datos de éste, no cuenta con soporte del fabricante, lo que expone a la entidad a riesgos de seguridad. (DSI Bogotá, DSA Bogotá - Aeropuerto El Dorado).

d. Aplicativos reportados como no corporativos que no fueron encontrados como activos de información en el Sistema GRC. (DGA, DGC, DGJ, DOGC, DSA: Bogotá - Aeropuerto El Dorado, Cúcuta; DSI: Bogotá, Medellín, Cali; DSIA: Bucaramanga, Villavicencio, Buenaventura).

e. Se identificó un aplicativo Web no corporativo para manejo de *"Actas manuales"*, que contiene información sensible relacionada con el resultado de las inspecciones de importación de mercancías, que opera en un equipo de cómputo de la Seccional y la construcción, mantenimiento y soporte es prestado por una persona sin vínculo contractual con la entidad ni firma de acuerdos de confidencialidad, según información suministrada en visita realizada durante la auditoría; adicionalmente, no cuenta con documentación ni tampoco ha sido clasificado como activo de información en el Sistema GRC. (DSIA Buenaventura).

(Ver anexo: Aplicativos_no_corporativos_Conclusiones/Columnas AC y AD en la carpeta DGIT-OSI. Nota: no se incluyen activos elaborados en hoja de cálculo).

⁵ SGTIT hoy DGIT

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 4. Elementos del hallazgo No. 4.

Criterios	Directiva Presidencial No. 02 de 2022, directriz No. 17 - Actualizaciones de seguridad del software liberadas por los fabricantes; MN-IIT-0072 V5 lineamiento 5.4.19 <i>"Instalación de software en sistemas operativos"</i> .
Dimensiones MIPG V6	Dimensión 3 <i>"Gestión con Valores para Resultados"</i> en las políticas: <i>"Gobierno Digital"</i> y <i>"Seguridad Digital"</i> .
Causas	Uso de tecnologías obsoletas y sin soporte por parte de los fabricantes; soluciones tecnológicas que no cubren las necesidades de la operación del negocio.
Efectos	Exposición al aprovechamiento de vulnerabilidades y brechas de seguridad. Posibles cobros de servicios prestados sin contrato, en el caso de aplicativo no corporativo <i>"Actas Manuales"</i> .
Riesgos	Exposición a los riesgos: R3. <i>"Plataforma tecnológica inadecuada para soportar los servicios tecnológicos"</i> , del Subproceso Innovación y Tecnología V3 y R3. <i>"Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad, y disponibilidad de los datos"</i> , del Subproceso Seguridad de la Información V2.

Fuente: Elaborado por el equipo auditor

Recomendaciones:

- Implementar en las soluciones tecnológicas institucionales, las funcionalidades que cubran de forma completa las necesidades de la operación del negocio.
- Cumplir con lo establecido en la directriz No.17 de la Directiva Presidencial No. 02 de 2022 y numeral 2, literal m, del numeral 5.4.19 *"Instalación de software en sistemas operativos"* del MN-IIT-0072 V5.
- Capacitar en el CG-TAH-0002⁶ V3 y en el MN-IIT-0072 V5, haciendo énfasis en los controles relacionados con: Gestión de identidad, control y derechos de acceso, autenticación segura, prevención en la fuga de datos e inicio de sesión.
- Cumplir con lo establecido en el procedimiento *"Gestión de Activos de Información PR-IIT-0366 V6"*, en cuanto a la identificación, clasificación y gestión de riesgos de los activos de información de la DIAN.
- Observar el artículo 6 de la Resolución 0484 del 24 de enero de 2013 de la DIAN⁷, que señala que la SGTIT hoy DGIT, en el Nivel Central, es la dependencia que tiene asignada la competencia exclusiva de evaluar la construcción y adquisición de software en la Entidad, siguiendo los procedimientos establecidos.

⁶ Código de Integridad de la DIAN.

⁷ *Por la cual se determinan las directrices del uso de los equipos de cómputo y el manejo de la información; del uso, instalación y desinstalación de software, del uso del servicio del correo electrónico institucional; del uso institucional de servicios web y de la conexión a Internet en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN.*

Hallazgo 5. Uso de aplicativo público no institucional Portal SAR (D)

Responsable: Dirección de Gestión de Fiscalización.

Corresponsable: Dirección de Gestión de Innovación y Tecnología, Oficina de Seguridad de la Información, DSIA Buenaventura.

Verificados los aplicativos de información, se identificó uno denominado "*Portal SAR - Aplicación diseñada para manejo de control posterior, revisión documental y alertamiento*" desplegado en un sitio Web Público bajo la dirección URL: <https://portalsar.azurewebsites.net/#/sign-in?redirectURL=%2Fexample>, el cual contiene información relacionada con contenedores que salen de la terminal portuaria, y no se encuentra reportado como aplicativo corporativo y/o no corporativo; lo que puede generar riesgos de seguridad y privacidad de la información, la falta de reconocimiento, autorización y supervisión frente al mismo, ha permitido que se acceda a este sin la debida protección, pudiéndose determinar que: 57 usuarios con dominio DIAN (funcionarios DIAN (52), externos (3), Pasante (1), Contratista de servicio (1)), entre el 20 de diciembre de 2024 y 13 de mayo de 2025, invocaron el Portal SAR, a través de la red DIAN desde diferentes lugares administrativos.

Adicionalmente, se consultó la información del certificado de servidor seguro del aplicativo, el cual figura emitido para "*Microsoft Corporation*"; es decir, para el portal público desplegado en una nube Azure, que no corresponde a la DIAN ni a convenios o aplicativos de entes externos a los que se deba rendir información. Cabe anotar, que el aplicativo opera en una nube pública y los dispositivos de seguridad institucionales sólo detectan tráfico que circule por la red DIAN. Verificado el acceso el 12 de junio de 2025, ya no es posible invocar el sitio "*Portal SAR*" con la URL citada previamente.

De otra parte, el jefe de la Oficina de Control Interno remitió alerta a la Oficina de Seguridad de la Información, Dirección de Gestión de Aduanas y Dirección de Gestión de Fiscalización, con copia a la Dirección General, mediante correo de oficio No. 100202204-1061 del 03 de junio de 2025, para que se tomarán las acciones a que diera lugar.

(Ver carpeta: *Aplicativo_no_institucional*, compartida a directores y jefe de: DGF, DGIT, OSI, DSIA Buenaventura).

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 5. Elementos del hallazgo No. 5.

Criterios	Normativa y las regulaciones aplicables a la entidad, lineamientos "5.1.33 <i>Protección de registros</i> " y el "5.2.6 <i>Acuerdos de confidencialidad y no divulgación</i> " del MN-IIT-0072 V5, MSPI V4 ⁸ .
Dimensiones MIPG V6	Dimensión 3 " <i>Gestión con Valores para Resultados</i> " en las políticas: " <i>Gobierno Digital</i> " y " <i>Seguridad Digital</i> ";
Causas	Falta de cumplimiento de los acuerdos de confidencialidad de la entidad sin la debida protección, herramientas robustas que permitan correlacionar eventos generados entre diferentes fuentes de información institucionales y su respectivo análisis; falta de implementación de controles para garantizar la seguridad y privacidad de la información y prevenir accesos a aplicativos no autorizados; y de

⁸ Modelo de Seguridad y Privacidad de la Información.

Tabla No. 5. Elementos del hallazgo No. 5.

	mecanismos de monitoreo y supervisión a los aplicativos a fin de establecer el uso indebido de estos.
Efectos	Exposición de la confidencialidad y privacidad de la información institucional.
Riesgos	Materialización del riesgo R3 " <i>Medidas de seguridad y privacidad de la información inadecuadas que amenazan la integridad, confidencialidad y disponibilidad de los datos</i> ", del Subproceso de Seguridad de la Información V2; y con alta exposición a los riesgos: " <i>R4. Pérdida del prestigio institucional</i> " de la Matriz de riesgos estratégicos de la DIAN; " <i>Información usada de manera indebida para beneficio propio o de terceros</i> ", del Subproceso de Innovación y Tecnología, " <i>Activos de información utilizados de manera indebida para beneficio propio y/o de terceros</i> ", del Subproceso de Seguridad de la Información de la matriz de riesgos de corrupción DIAN 2025; y, al riesgo R8 " <i>Información afectada en su integridad y/o confidencialidad y/o disponibilidad</i> ", del Subproceso de Fiscalización y Liquidación V4 y posibles incidencias de índole disciplinario.

Fuente: Elaborado por el equipo auditor

Recomendaciones:

- Fortalecer lo establecido en el lineamiento 5.1.7 Inteligencia de amenazas, literal c), del MN-IIT-0072 V5, que señala: la OSI debe "*Recopilar la información y realizar el análisis de esta*".
- Atender el lineamiento 5.1.15 Control de Acceso, numeral 2, literal c) del MN-IIT-0072 V5, que señala que la OSI debe: "*Realizar monitoreo a través del Centro de Seguridad de las Operaciones para las actividades realizadas sobre los sistemas de información de la DIAN e informar si evidencia algún tipo de tráfico anómalo o de carácter riesgoso*"; y el numeral 3, literal d) del mismo a cargo de la DGIT, que indica: "*Monitorear y auditar las operaciones realizadas por los usuarios en los equipos, dispositivos o aplicaciones y/o servicios, sin requerir autorización expresa (...)*".
- Fortalecer el cumplimiento del lineamiento 5.4.15 Inicio de sesión, literal a) del MN-IIT-0072 V5, que señala: "*Confirmar que todas las aplicaciones tengan activos los registros de las actividades realizadas por los funcionarios (...)*" a cargo de la SITO⁹ y el 5.4.16 Actividades de seguimiento, numeral 1, literal a) a cargo de la misma área, que señala: "*Contar con un COSI (Centro de Monitoreo de Seguridad de la Información) para monitorear, identificar, correlacionar y alertar actividades de posible riesgo sobre los sistemas que registren los logs en el sistema SIEM¹⁰ de la entidad*".
- Capacitar en el CG-TAH-0002 V3 de la DIAN y del MN-IIT-0072 V5, en los controles relacionados con: Gestión de identidad, control y derechos de acceso, autenticación segura, prevención en la fuga de datos e inicio de sesión.
- Concientizar sobre el lineamiento 5.4.20 Seguridad en redes, numeral 4, literal c) del MN-IIT-0072 V5, que establece para los funcionarios y terceros: "*Evitar, bajo el riesgo de sanción por parte de la entidad, colocar información de la DIAN (independientemente de su formato o su nivel de clasificación de confidencialidad) en sitios de internet públicos (...) o fuera de las instalaciones de la DIAN que no sean aprobados por la entidad*" y el lineamiento 5.2.6 Acuerdos de confidencialidad o no divulgación que señala: "*(...) entender el compromiso de confidencialidad y no divulgación*".

⁹ Subdirección de Infraestructura Tecnológica y de Operaciones.

¹⁰ *Security Information and Event Management*, en español, Gestión de Información y Eventos de Seguridad.

Hallazgo 6. Falencias en la gestión de accesos y suplantación de usuarios en el Sistema RUT (D)

Responsable: Dirección de Gestión de Impuestos/Subdirección de Administración del Registro Único Tributario.

Corresponsable: Dirección de Gestión de Innovación y Tecnología, Oficina de Seguridad de la Información, DSI Barranquilla.

Verificada la gestión de accesos a la solución tecnología RUT, se observó inscripción de un formulario con número XXXXXXXXX972 y actualización con número XXXXXXXXX674 del 10 de enero de 2025, las cuales fueron realizadas por un usuario que no perteneció a la planta de personal de la DIAN, clasificado en el reporte "*Roles activos usuarios DIAN*" como funcionario; estableciéndose que, prestó servicios a la entidad mediante contrato de outsourcing en el año 2012. Adicionalmente, según certificado suministrado por la DSI de Barranquilla expedido por la Registraduría Nacional del Estado Civil, el usuario en mención falleció en noviembre de 2023; sin embargo, contaba con roles activos, entre otros del Sistema RUT, según Reportes "*Roles activos usuarios DIAN*" desde febrero de 2021 hasta enero de 2025, situación que pudo ser aprovechada para realizar los trámites mencionados anteriormente.

Evidenciándose debilidades en la gestión de accesos al Sistema RUT y vulnerabilidades de seguridad, que favorecen la ejecución de acciones presuntamente fraudulentas, lo cual también ha sido informado a la Dirección General, Oficina de Seguridad de la Información, Dirección de Gestión de Innovación y Tecnología, Dirección de Gestión de Impuestos, Subdirección de Administración de Registro Único Tributario por funcionarios de la DSI de Barranquilla, quienes, además, denunciaron ante la Fiscalía General de la Nación, haber detectado acciones realizadas con el usuario que les fue asignado y en algunos casos, no tenían habilitado el rol que les permitiera la formalización de formularios RUT.

(Anexo: Carpeta RUT_893, compartido a: DGI/SDARUT, DGIT, OSI, DSI Barranquilla).

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 6. Elementos del hallazgo No. 6.

Criterios	Procedimiento PR-IIT-0455 V3 " <i>Gestión de Accesos</i> "; MSPI V4.
Dimensiones MIPG V6	Dimensión 3 " <i>Gestión con Valores para Resultados</i> " en las políticas: " <i>Gobierno Digital</i> " y " <i>Seguridad Digital</i> ".
Causas	Inoportuna inactivación de roles, así como la falta de: controles en los permisos concedidos a personal que presta servicio a través de proveedores externos, integración entre el Directorio Activo y la plataforma MUISCA; control y seguimiento a los roles asignados y activos; implementación del doble factor de autenticación en la plataforma MUISCA; herramientas de seguridad que permitan la correlación de eventos entre diferentes fuentes de información; y desaprovechamiento del sistema de seguridad de auditoría de bases de datos, con el que cuenta la OSI y su correspondiente análisis.
Efectos	Accesos indebidos a las soluciones tecnológicas institucionales de personal no autorizado y manipulación de información.
Riesgos	Materialización de los riesgos R4 " <i>Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información</i> ", del Subproceso de Innovación y Tecnología V3 y del riesgo R3 " <i>Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad y disponibilidad de los datos</i> ", del Subproceso de Seguridad de la información V2.

Fuente: Elaborado por el equipo auditor

Recomendaciones:

- Implementar mecanismos de doble factor de autenticación, en las soluciones tecnológicas institucionales, de acuerdo con el lineamiento 11 del numeral 3.1 Usuarios y Contraseñas del PR-IIT-0455 V3 a cargo de la DGIT.
- Realizar *hardening*¹¹ en los servidores de bases de datos, implementando controles, tales como: aplicar el principio del mínimo privilegio, restringir el acceso a las bases de datos sólo desde direcciones IP's de servidores de aplicaciones de confianza, mantener actualizados los sistemas operativos y aplicaciones, bloquear puertos innecesarios, revisar logs con regularidad, monitorear las conexiones por acceso remoto y VPN's. En el mismo sentido, implementar controles como, por ejemplo: articular el LDAP¹² de la plataforma MUISCA con el Directorio Activo de Microsoft. Lo anterior, en atención al lineamiento 5.3.8 Ubicación y protección del equipo, numeral 2, literal n, del MN-IIT-0072 V5 a cargo de la SITO, para prevenir accesos no autorizados a los recursos tecnológicos en donde opera la solución tecnológica RUT y en general en las plataformas institucionales.

Hallazgo 7. Debilidades en la gestión de roles asignados en periodos de situaciones administrativas superiores a 15 días calendario. (P)

Responsable: Dirección de Gestión Corporativa/ Subdirección de Gestión del Empleo Público.

Corresponsables: Dirección de Gestión de Innovación y Tecnología, Oficina de Seguridad de la Información, Direcciones de Gestión, Operativa y Direcciones Seccionales.

Analizada la información relacionada con los reportes de roles asignados respecto de las situaciones administrativas, superiores a 15 días calendario, de los funcionarios reportados por la SGEF, entre el 01 de enero de 2024 y 15 de marzo de 2025, se evidenció:

- Baja confiabilidad en los procesos para la inactivación de roles entre la solución tecnológica de administración de planta de personal KACTUS y la plataforma MUISCA, ausencia de automatización integrada con la plataforma SIAT y con otras soluciones tecnológicas como SIGLO XXI, SIFARO, DYNAMIC 365 y Digiturno. (Ver anexos: SA_MUISCA_DG/OF, SA_MUISCA_DS, en la carpeta de cada Dirección de Gestión/Operativa/Oficina o Dirección Seccional).
- Deficiencias en la inactivación que se debe realizar sobre los roles informáticos asignados, para las cuales no existe inactivación automática o ésta falla y tiempos prolongados para la reactivación de roles al regreso del funcionario de la situación administrativa, especialmente en las plataformas SIAT y SIGLO XXI.
- Inoportunidad en la actualización de los actos administrativos en el sistema KACTUS, puesto que se identificó una funcionaria de la DSIA Pereira identificada con cédula XXXXX329 con Resolución de modificación de situación administrativa de vacaciones, la

¹¹ Proceso para fortalecer un sistema o red, para reducir las vulnerabilidad y ataques.

¹² Lightweight Directory Access Protocol, o en español, Protocolo Ligero de Acceso a Directorios.

cual no se encontraba registrada en el Sistema, generando inconsistencia en la información reportada y en los resultados de las transacciones evaluadas en la solución tecnológica RUT. (Ver anexo: "XXXXX329" en la carpeta DGC).

d. Se identificaron tres (3) exfuncionarias, con transacciones realizadas después del retiro de la entidad: c.c. XXXXX313 - (15), retiro 31 de diciembre de 2024, última ubicación: DSI Bogotá ; c.c. XXXXX402 - (6), retiro 30 de diciembre de 2024, última ubicación: DSIA Riohacha; y c.c. XXXXX754 - (57), retiro 31 de diciembre de 2024, última ubicación: DSIA Popayán, con roles asignados a "Servidor DIAN" por lo que se evidencia acceso indebido a los sistemas de información de la entidad, por parte de exfuncionarios que ya no ostentaban la calidad de servidores públicos de la DIAN, por lo que se establece una presunta incidencia de tipo penal, según el artículo "269A Acceso abusivo a un sistema informático" del Código Penal, modificado por la Ley 1273 de 2009. (Solución Tecnológica: Análisis de Operaciones). (Ver anexo: "313-402-754" en la carpeta 313-402-754 compartido a DGEA/Subdirección Análisis de Riesgo y Programas, DSI Bogotá, DSIA de Popayán, DSIA Riohacha, DGIT, OSI) **(P)**.

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 7. Elementos del hallazgo No. 7.

Criterios	Procedimiento PR-IIT-0455 V3 "Gestión de Accesos", MSPI V4.
Dimensiones MIPG V6	Dimensión 3 "Gestión con Valores para Resultados" en las políticas: "Gobierno Digital" y "Seguridad Digital".
Causas	Falta: i) de desarrollos que permitan la integración confiable entre la solución tecnológica KACTUS y la plataforma MUISCA, la plataforma SIAT y con otras soluciones tecnológicas; ii) de acceso en tiempo real a la información de los roles que no fueron inactivados por fallas en la integración entre soluciones tecnológicas; iii) estandarización en la frecuencia de la publicación de reportes y sincronización y/o actualización oportuna de las situaciones administrativas de las Direcciones Seccionales en el Sistema KACTUS; la multiplicidad de reportes generados de las diferentes plataformas y soluciones tecnológicas.
Efectos	Que no se garantice la inactivación de los roles durante los periodos de situaciones administrativas, vulnerabilidades ante amenazas como abuso de los derechos de acceso, procesamiento inadecuado de datos, limitación en el control y seguimiento.
Riesgos	Materialización del riesgo R4 "Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información" y alta exposición al R5. "Información usada de manera indebida para beneficio propio o de terceros", del Subproceso Innovación y Tecnología V3.

Fuente: Elaborado por el equipo auditor

Recomendaciones:

- Actualizar oportunamente el Sistema de planta de personal KACTUS o el que haga sus veces, con las situaciones administrativas y las novedades de éstas.
- Realizar oportunamente la reactivación de roles al reintegro de los funcionarios en situaciones administrativas.
- Fortalecer el control 5.2.5 Responsabilidades después de la terminación o cambio de empleo, numeral 3, literales a) y g) del MN-IIT-0072 V5 a cargo de la SGEP, que señalan: "Informar a los funcionarios que después de la terminación o cambio de empleo de la DIAN, las responsabilidades y deberes de seguridad y privacidad de la

información permanecen válidos” y “Verificar que se desactiven y/o eliminen los accesos físicos y lógicos (...)”.

Hallazgo 8. Cuentas activas sin uso, vinculadas a funcionarios con situaciones administrativas o retirados de la Entidad o terceros con relación terminada.

Responsable: Dirección de Gestión de Innovación y Tecnología.
Corresponsable: Oficina de Seguridad de la Información.

a. Resultado del análisis del reporte remitido por la DGIT con corte al 15/03/2025, se identificaron cuentas de usuario activas en el Directorio Activo pertenecientes a funcionarios que, según el reporte de situación administrativa se encuentran retirados o suspendidos temporalmente; adicionalmente, se evidencian cuentas de usuario activas perfiladas como pasantes, judicantes o asignados a entidades externas como: POLFA, CGR, ITRC entre otros. También, se observan cuentas del Directorio Activo que no registran cambios de contraseña, encontrándose las siguientes situaciones:

- Cuentas activas (431) en el Directorio Activo asociadas a funcionarios con situación administrativa superior a 15 días hábiles, sin que se les haya deshabilitado el acceso correspondiente.
- Cuentas activas (167) de judicantes sin inicio de sesión, desde 2024 o antes.
- Cuentas activas asignadas a terceros: POLFA (50), ITRC (19) y CGR (19) con actividad nula desde diciembre de 2024 hacia atrás.
- Cuentas activas asignadas a pasantes (311) que no han registrado inicio de sesión desde diciembre 2024 hacia atrás, incluyendo 15 sin ningún registro de uso.
- La cuenta del usuario "dcastiblanco" creada el 17/12/2024, no ha realizado cambio de contraseña ni registra autenticación hasta la fecha del informe, lo cual puede implicar que no se le aplican las políticas vigentes de cambio de contraseña o no se utiliza la cuenta, que según datos suministrados por la DGIT figura en: "DSI Bogota_DIV Cobranzas".

(Ver anexo: Directorio Activo en la carpeta DGIT - OSI)

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 8. Elementos del hallazgo No. 8.

Criterios	Lineamientos: "5.1.18 Derechos de acceso", "5.4.2 Derechos de acceso privilegiado" del MN-IIT-0072 V5 y los controles equivalentes del Anexo A de la Norma NTC-ISO/IEC 27001:2022; MSPI V4.
Dimensiones MIPG V6	Dimensión 3 "Gestión con Valores para Resultados" en las políticas: "Gobierno Digital" y "Seguridad Digital".
Causas	Falta de control y monitoreo en la inactivación de las cuentas de Directorio Activo, una vez se presentan situaciones administrativas o se finaliza el vínculo con la entidad o terminada la relación con terceros.
Efectos	Accesos indebidos por personal no autorizado, generando brechas de seguridad.
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 de Innovación y Tecnología V3; R2 "Lineamientos y políticas de seguridad y privacidad de la información implementados de manera ineficiente" y R3. "Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad, y disponibilidad de los datos", del Subproceso de Seguridad de la Información V2.

Fuente: Elaborado por el equipo auditor

Recomendaciones:

- Fortalecer el proceso de gestión del ciclo de vida de cuentas de usuario e implementar lineamientos y controles automatizados para la desactivación de cuentas en el Directorio Activo y LDAP's de las plataformas MUISCA y SIAT, a través de una interfaz con el Sistema KACTUS, teniendo en cuenta lo referido en el MN-IIT-0072 V5, lineamiento 5.1.18 Derechos de acceso, literal c, donde se establece que la OSI, debe: *"(...) Definir y establecer lineamientos y controles para la desactivación o bloqueo de los privilegios de acceso sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, teniendo en cuenta las siguientes situaciones administrativas: Desvinculación, Licencias, Vacaciones, Traslados o ubicaciones entre dependencias o seccionales, Cambio de cargo o proceso, Sanción disciplinaria, Terminación de contrato de prestación de servicio o contrato con terceras partes o proveedores (...)"*.
- Realizar depuración periódica y auditoría, estableciendo una frecuencia para la revisión de cuentas activas sin uso, con base en: Último inicio de sesión y cambios de contraseña, con una oportunidad sugerida mensual; y, aplicar una política de grupo en el Directorio Activo, para la inactivación automática de cuentas sin uso por más de 30 días, salvo justificación documentada, teniendo en cuenta el literal i) del lineamiento 5.1.18 Derechos de Accesos del MN-IIT-0072 V5, que establece: *"Verificar que todas las aplicaciones y sistemas de información tengan autenticación solo de cuentas administradas por el controlador de dominio y contar con la documentación de la gestión de identidades que se realiza. (...)"*, a cargo de la DGIT.

Hallazgo 9. Deficiencias en la seguridad de los logs de las contraseñas y manejo de usuarios de prueba en producción en las bases de datos de SYGA Siglo XXI.

Responsable: Dirección de Gestión de Innovación y Tecnología, Oficina de Seguridad de la Información.
Corresponsable: Dirección de Gestión de Aduanas.

Verificada la información correspondiente al periodo del 01 de enero de 2024 al 15 de marzo de 2025 se observó que, de un total de 8.530 registros de funcionarios y externos (UTS) en el Sistema SYGA Siglo XXI en 5.262, la contraseña no se encuentra encriptada y 1.800 corresponden a usuarios de prueba. De los 5.262 usuarios: 1.940 se encuentran en "estado = (A) activo" y de estos, 678 no tienen la "fecha hasta" vigente; así mismo, 1.198 usuarios que se encuentran en "estado = (I) inactivo" y 2.127 se encuentran en "estado = (P) primera vez".

De otra parte, en la información suministrada por la Subdirección de Operación Aduanera, se encontró que en la tabla de logs de usuarios de las bases de datos de producción del Sistema SYGA Siglo XXI, la información de la contraseña en algunos casos no está encriptada y se identificaron usuarios de prueba en producción. Estas inconsistencias se evidenciaron en 29 bases de datos, distribuidas de la siguiente manera: Arauca, Armenia, Barranquilla, Bogotá, Bucaramanga, Buenaventura, Cali, Cartagena, Cúcuta, Ibagué, Ipiales, Leticia, Maicao, Manizales, Medellín, Montería, Neiva, Pereira, Popayán, Puerto Asís, Puerto Carreño, Riohacha, San Andrés, Santa Marta, Tumaco, Turbo, Valledupar, Villavicencio y Yopal. (Anexo: Ver archivo "Logs_contraseñas" en la carpeta DGIT-OSI).

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 9. Elementos del hallazgo No. 9.

Criterios	MN-IIT-0072 V5, los controles de la Norma NTC-ISO/IEC 27001:2022 Anexo A y de la Guía GTC-ISO/IEC 27002:2022 y PR-IIT-0455 V3, relacionados con "Gestión de identidad"; MSPI V4.
Dimensiones MIPG V6	Dimensión 3 "Gestión con Valores para Resultados" políticas "Gobierno Digital" y "Seguridad Digital".
Causas	Deficiencias en la seguridad del manejo de la información de los usuarios en el sistema de información SYGA Siglo XXI; falta de control en la asignación de usuarios de prueba en producción; desarrollos que aseguren el cifrado de las contraseñas en todos los casos; y lineamientos para la entrega de las contraseñas que garanticen que sean conocidas sólo por el interesado.
Efectos	Brecha de seguridad para acceder de manera no autorizada a la información del sistema SYGA Siglo XXI.
Riesgos	Exposición a los riesgos R4. "Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información" y R5. "Información usada de manera indebida para beneficio propio o de terceros", del Subproceso Innovación y Tecnología; 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.

Fuente: Elaborado por el equipo auditor.

Recomendaciones:

- Cifrar los campos que almacenen contraseñas en cada una de las bases de datos del sistema de información SYGA Siglo XXI en atención a lo establecido en el MN-IIT-0072 V5, lineamiento 5.4.24 Uso de criptografía, numeral 2, literal a) que establece: "Controlar que la información y/o las aplicaciones que contengan contraseñas de usuario o claves para el control de acceso a los sistemas de información no sea almacenada en texto plano y debe hacer uso de mecanismos criptográficos", a cargo de la DGIT.
- Atender el lineamiento 5.4.31 Separación de los entornos de desarrollo, prueba y producción, literal b, que señala: "Proveer los recursos necesarios para la implementación de controles que permitan la separación de ambientes de pruebas y producción (...)", a cargo de la DGIT.
- Eliminar los usuarios de prueba actualmente existentes en los ambientes de producción de la solución tecnológica SYGA Siglo XXI.
- Revisar la coherencia entre el estado de usuario y la fecha de vigencia, en las bases de datos de la solución tecnológica SYGA Siglo XXI.

Hallazgo 10. Deficiencias en la aplicación de políticas de seguridad de información en las terminales de autogestión (Kioscos)

Responsable: Dirección de Gestión de Innovación y Tecnología.

Corresponsable: Oficina de Seguridad de la Información, Subdirección de Servicio al Ciudadano en Asuntos Tributarios SSCAT, DSA Bogotá - Aeropuerto El Dorado, DSI Barranquilla y DSIA Buenaventura.

a. Se evidenciaron archivos almacenados en las carpetas de "Documentos", "Descargas", "Escritorio" y "Papeleras de reciclaje" de datos sensibles pertenecientes a ciudadanos que

hacen uso de las estaciones de cómputo, tales como: cédulas de ciudadanía, pasaportes, facturas electrónicas, formularios RUT, certificados y otros documentos de Cámara de Comercio en los lugares administrativos: DSA Bogotá - Aeropuerto El Dorado, DSI Barranquilla y DSIA Buenaventura.

b. Se evidenció que la contraseña de acceso a los equipos de auto gestión Kioscos está impresa y adherida a la pared del cubículo o en la base de los monitores, incrementando la posibilidad de afectar la privacidad y seguridad de la información que reposa en estos equipos. DSA Bogotá – Aeropuerto El Dorado y DSIA Buenaventura.

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 10. Elementos del hallazgo No. 10.

Criterios	Resolución 484 de 2013 de la DIAN, Capítulo II, artículo 4 numerales: 1 “Mantener en reserva y hacer un uso adecuado de la información” y 5 “Hacer limpieza del disco del computador”; Capítulo II, artículo 2, numeral 3 “Responsabilidades de los usuarios internos”, literal b “Uso confidencial de la contraseña”; MN-IIT-0072 V5, numeral 5.3.7 “Escritorio y pantalla despejados”, numeral 3, literal f); Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013 y el 1081 de 2015.
Dimensiones MIPG V6	Dimensión 3 “Gestión con Valores para Resultados” en las políticas “Gobierno Digital” y “Seguridad Digital”.
Causas	Incumplimiento o deficiencia en la aplicación de las normas, políticas o procedimientos de seguridad digital.
Efectos	Afectación a la imagen y confianza legítima de la Entidad y los derechos de las personas.
Riesgos	Exposición a los riesgos: R4. “Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información” y R5 “Información usada de manera indebida para beneficio propio o de terceros”, del Subproceso de Innovación y Tecnología V3; R2. “Lineamientos y políticas de seguridad y privacidad de la información implementados de manera ineficiente” y R4 “Activos de información utilizados de manera indebida para beneficio propio y/o de terceros”, del Subproceso de Seguridad de la Información V2.

Fuente: Elaborado por el equipo auditor

Recomendaciones:

- Socializar la política de grupo del Directorio Activo “Limpieza de archivos en terminales de autogestión” con los líderes informáticos en las seccionales.
- Afinar y desplegar la política del Directorio Activo de limpieza automática en las terminales de autogestión – kioscos, para que eliminen archivos temporales y carpetas como “Descargas”, “Documentos” y “Papelería de reciclaje” al finalizar la jornada del punto de atención o implementar perfiles de usuarios temporales o software de congelamiento de discos duro.
- Dar cumplimiento a los lineamientos: 5.3.7 Escritorio y pantalla despejados del MN-IIT-0072 V5, numeral 3, literal f) “Evitar anotar las contraseñas en papeles, evitar colocarlas en el computador o debajo del equipo”; y al Capítulo II, art. 2, num. 3 de la Resolución 484 de 2013, literal b) “Uso confidencial de la contraseña”, que señala: “La contraseña, clave o password de acceso, es de carácter estrictamente confidencial, personal e intransferible”.
- Establecer lineamientos para el uso de los kioscos y divulgarlos a los ciudadanos, publicando en cada uno un aviso en el escritorio del PC u otro medio visible, sobre la

obligación del usuario de cerrar sesión y no almacenar o guardar documentos personales y/o sensibles en el equipo.

Hallazgo 11. Deficiencias en la gestión de cuentas institucionales con inactividad prolongada en servicios como VPN y plataforma de correo electrónico Institucional a nivel nacional.

Responsable: Dirección de Gestión de Innovación y Tecnología.
Corresponsable: Oficina de Seguridad de la Información.

Realizado el cruce entre el reporte de funcionarios de planta con corte a 10/03/2025 remitido por la SGEF vs. el reporte de cuentas de usuarios del Directorio Activo con corte a 06/05/2025 suministrado por la DGIT, se identificó:

- a. Cuentas con accesos por VPN asignadas a (4) usuarios no registrados como funcionarios activos en la planta de personal y sin evidencia de ingreso.
- b. Cuentas con accesos por VPN asignadas a (8) usuarios con más de 180 días calendario desde su último acceso.
- c. Cuentas activas de correo institucional asignadas a (209) usuarios que presentan inactividad por más de 180 días calendario, distribuidas así: funcionarios (18), judicantes (164), CGR(3), ITRC(3), pasantes(3) y POLFA(18).
- d. Cuentas activas de correo institucional asignadas a (251) usuarios no ubicados en planta de personal, de las cuales 38 no han sido utilizadas.
- e. Desactualización frente a la información registrada en el sistema KACTUS y falta de estandarización de la información en las propiedades del correo electrónico de los funcionarios activos, correspondiente al lugar administrativo y área a la que pertenece.

(Ver anexo: Archivos "Acceso VPN" y "Correo institucional" en la carpeta DGIT-OSI).

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 11. Elementos del hallazgo No.11.

Criterios	Numerales "A.5.16 Gestión de Identidad", "A.5.17 Información de Autenticación" y "A.5.18 Derechos de Acceso" de la norma NTC-ISO/IEC 27001:2022; numeral "5.1.18 Derechos de acceso" del MN-IIT-0072 V5.
Dimensiones MIPG V6	Dimensión 3 "Gestión con Valores para Resultados" en las políticas "Gobierno Digital" y "Seguridad digital".
Causas	Falta de control, monitoreo y depuración de las cuentas de accesos por VPN y del correo institucional, con relación a cuentas inactivas y desactualización de la información en los buzones de correo electrónico institucional.
Efectos	Posibilidad de accesos no autorizados a recursos institucionales y la pérdida de trazabilidad y control sobre los accesos institucionales.
Riesgos	Exposición al Riesgo 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

Fuente: Elaborado por el equipo auditor

Recomendaciones:

- Diseñar controles que permitan depurar las cuentas activas asignadas a personas no vinculadas, cuentas duplicadas, cuentas con metadatos incompletos o sin estandarización (área, sede, cargo o rol, etc), en el Directorio Activo, correo electrónico, VPN's, soluciones tecnológicas, entre otros e implementar procedimientos automatizados que permitan generar alertas tempranas que favorezcan la inactivación oportuna de cuentas de acceso, en cumplimiento del lineamiento 3, del literal f), del numeral 5.1.18 Derechos de acceso, a cargo de la DGIT, que señala: *“Mantener actualizado y depurado el listado y los permisos de administración de los diferentes recursos tecnológicos de la entidad. Para tal efecto, se deben hacer por lo menos dos revisiones al año. Adicionalmente, se debe contar con un registro de cuentas con accesos privilegiados”*.

Hallazgo 12. Incumplimiento en la prestación del servicio **“Zona WiFi Gratis para la Gente”**

Responsable: Dirección de Gestión de Innovación y Tecnología.

Corresponsables: DSA Aduanas Bogotá - Aeropuerto El Dorado; DSA y DSI Barranquilla.

La DIAN suscribió Contrato No. 00-207-2024 con el objeto de: *“Prestar el servicio de telecomunicaciones para todas las sedes de las Direcciones de Impuestos y Aduanas Nacionales UAE-DIAN a nivel nacional, incluyendo la infraestructura necesaria para la correcta prestación de este”*, con fecha de inicio de 14 de noviembre de 2024 y fecha de finalización 31 de julio de 2026.

Durante la visita realizada a los puntos de contacto: DSA Bogotá – Aeropuerto El Dorado (CAC), DSI y DSA de Barranquilla, DSIA de Buenaventura, DSI y DSA de Cartagena, se verificó el estado de operación del servicio de conectividad gratuito denominado *“Zona WIFI Gratis para la Gente”* que hace parte de los servicios cubiertos por el mencionado contrato, observando:

a. Incumplimiento en la prestación del servicio de red Wifi de acceso gratuito a los ciudadanos, en la DSI y DSA de Barranquilla y DSA Bogotá - Aeropuerto El Dorado (CAC), debido a que no se encontró disponible en estos lugares administrativos; y por parte de funcionarios, se manifestó desconocimiento de este servicio. No obstante, en respuesta de la DGIT, se indicó que *“El servicio se presta en todos los puntos de contacto informados por la Subdirección de Servicio al Ciudadano en Asuntos Tributarios, y el pago del servicio se está realizando con presupuesto del contrato de telecomunicaciones”*.

Verificados los pagos realizados en mes de abril de 2025, con cargo al referido contrato en la plataforma SECOP II, se estableció que se reportó el pago en la factura IFXC – 431623 de los servicios: ID IFX: 2329992 (DSA Bogotá – Aeropuerto), 2330029 (DSA Barranquilla) y 2330033 (DSI Barranquilla), por los valores que se relacionan a continuación.

Tabla 12. Pagos realizados al servicio de “Wifi Gratis para la Gente”

Enlaces Wifi gratis para la gente	ID IFX	Valor pagado 04/2025 Factura IFXC - 431623
Aeropuerto El Dorado - Muelle Carga	2329992	\$ 235.375
Barranquilla - Aduanas	2330029	\$ 197.716
Barranquilla - Impuestos	2330033	\$ 208.122
TOTAL		\$ 641.214

Fuente: Elaborado por el equipo auditor

Con lo anterior, se incumplen criterios normativos, dimensiones del MIPG V6 y procedimientos institucionales, generando efectos y riesgos, con ocasión a las causas, como se muestra en la siguiente tabla.

Tabla No. 13. Elementos del hallazgo No. 12.

Criterios	Decreto 728 de 2017, Manual de contratación MN-ADF-0013 V4, de la DIAN.
Dimensiones MIPG V6	Dimensión 3 “Gestión con Valores para Resultados” en las políticas “Gobierno Digital” y “Seguridad digital”.
Causas	Incumplimiento de lo establecido en el Decreto 728 de 2017, artículos: 2.2.9.2.2. “Zonas de acceso público a Internet inalámbrico en entidades públicas”, artículos 2.2.9.2.4. “Conexión al servicio de acceso a Internet” y artículo 2.2.9.2.5. “Señalética”; Debilidades en el cumplimiento del Anexo 4, “Cláusulas contractuales: 11.2 Obligaciones especiales del supervisor del contrato, a quien corresponde: 11.2.1. Inspeccionar y verificar la calidad de los servicios contratados, como también el cumplimiento de las especificaciones técnicas de los mismos, 11.2.2. Solicitar al contratista las pruebas de calidad que estime convenientes para establecer y evaluar el correcto funcionamiento de los servicios contratados, 11.2.5. Autorizar, rechazar y/o aprobar todo lo relacionado con la parte funcional, técnico, administrativo, financiero, contable, y jurídica del presente contrato”
Efectos	Posible afectación a la imagen institucional, limitando la utilidad de los informes para la toma de decisiones informadas y un posible incumplimiento del contrato.
Riesgos	Materialización del R1. “Sistemas de información y servicios digitales indisponibles (no programada-fortuita) para las partes interesadas”, del Subproceso de Innovación y Tecnología V3; Exposición al R3 “Incumplimiento total o parcial del contrato”, del Subproceso Compras y Contratos V3.

Fuente: Elaborado por el equipo auditor.

Recomendaciones:

- Dar cumplimiento a las cláusulas 11.2.1, 11.2.2 y 11.2.5 del contrato No. 00-207-2024, la Dimensión 3 “Gestión con valores para resultados” y Dimensión 6 “Seguimiento y evaluación” del MIPG V6 y aplicar lo establecido en el “Manual de Contratación MN-ADF-0013 V4”, de la DIAN.
- Diseñar controles que permitan la verificación del correcto funcionamiento del servicio “Zona Wifi gratis para la gente” establecidas mediante Decreto 728 de 2017; por ejemplo, mediante visitas técnicas presenciales o a través de los líderes informáticos ubicados en las direcciones seccionales de la entidad o a través del uso de herramientas de monitoreo, que permitan visualizar la operación y consumo de los canales de Internet, en cada uno de los puntos contratados a nivel nacional.
- Atender lo dispuesto en el MN-IIT-0072 V5 lineamiento 5.4.22 Segregación de redes, numeral 1, literal i) *Implementar de forma segura la red de “Zona Wifi gratis para la Gente” según el Decreto 728 de 2017*, a cargo de la SITO¹³.

¹³ Subdirección de Infraestructura Tecnología y de Operaciones.

6. EVALUACIÓN DE LOS COMPONENTES DEL SISTEMA DE CONTROL INTERNO

El sistema de control interno está compuesto por varios elementos interrelacionados para garantizar el logro de los objetivos institucionales; a continuación, se presenta la evaluación de los componentes del sistema de control interno en los procesos auditados, así:

6.1 Ambiente de control

Procesos disciplinarios por presuntas faltas disciplinarias

Respecto de actuaciones disciplinarias relacionadas con la gestión de accesos, la Subdirección de Asuntos Disciplinarios informó que, durante el periodo comprendido entre el 01 de enero de 2024 y 15 de marzo de 2025, se adelantaron procesos disciplinarios, uno (1) con “*Auto de archivo*” y dos (2) en “*Indagación previa*”. Adicionalmente, dos quejas fueron trasladadas por competencia a la Agencia ITRC. Los cuales atienden a la reserva de la información.

Régimen de inhabilidades e incompatibilidades y conflicto de interés

En relación con la socialización o divulgación de las situaciones en las cuales se puede incurrir en inhabilidad, incompatibilidad y/o conflicto de interés y cuál ha sido su tratamiento, se realizaron las siguientes actividades:

Campañas informativas sobre el código de integridad, actividades por parte de los gestores de ética e invitación a la segunda Semana para la Transparencia, Ética y Anticorrupción (TEA). (DGIT-OSI).

Sesiones de capacitación en asuntos disciplinarios; inducción durante el periodo de prueba; socialización de la Guía para la gestión de conflictos de interés; socialización de videos alusivos al tema; participación en la Semana TEA. (DSA: Bogotá – Aeropuerto El Dorado, Barranquilla, Cartagena; DSI: Barranquilla, Cartagena; DSIA Buenaventura).

Por parte de las direcciones seccionales auditadas, se informó de la manifestación de dos (2) funcionarios con conflicto de interés en la DSA-Bogotá Aeropuerto El Dorado y uno (1) en la DSA - Barranquilla, las cuales fueron gestionadas.

Actualización de procedimientos y otras normas

El procedimiento de “*Gestión de Accesos PR-IIT-0455 V3*”, fue actualizado el 11 de agosto de 2023; sin embargo, se sugiere realizar revisiones periódicas para validar la vigencia frente a la actualidad y realidad institucional, y dar claridad a algunos lineamientos, tales como:

- Lineamiento 23, numeral 3.2 que señala: “*Es responsabilidad de talento humano, jefes inmediatos y/o supervisores registrar y notificar, la desvinculación definitiva de un funcionario a su cargo y/o la finalización de un contrato o convenio, con el fin de que sean bloqueados todos los accesos a la red corporativa*”. Respecto al momento en que lo debe realizar cada uno de los responsables referenciados y la herramienta de gestión

para el registro, de acuerdo con las competencias.

- Lineamiento 18, numeral 33, que señala “*La Subdirección de Soluciones y Desarrollo realiza seguimiento diario a las fechas de finalización de los contratos de prestación de servicios (...)*”. Respecto del manejo que se debe dar a personal provisto por proveedores, como por ejemplo el suministrado para soporte técnico.

Por otro lado, es importante revisar el “*Manual de Políticas y Lineamientos de seguridad de la información MN-IIT-0072 V5*”, en cuanto a la definición de deberes, funciones y tareas del Centro de Seguridad de la Operación, en el lineamiento 5.1.15, numeral 2, literal c); del SOC en el lineamiento 5.1.14 Redundancia de las instalaciones de procesamiento de información, literal j) del numeral 2; y, del COSI (Centro de Monitoreo de Seguridad de la Información) del lineamiento 5.4.16 Actividades de seguimiento. Así mismo, aclarar las responsabilidades frente al SIEM, entre la DGIT y de la OSI, respecto del análisis de incidentes y alertas de seguridad, producto de la correlación de los logs que deben proporcionar todos los sistemas de información.

De igual manera, armonizar algunos lineamientos establecidos en el MN-IIT-0072 V5, como por ejemplo los relacionados con el numeral 4 “*Los jefes de las dependencias deben (...)*”, del numeral 5.1.18 Derechos de acceso y lo establecido en el PR-IIT-0455 V3, con el fin de unificar criterios y dar claridad a las responsabilidades establecidas.

Adicionalmente, se considera revisar la pertinencia de actualizar la Resolución 484 de 2013, en aspectos como la referencia a los procesos frente a la nueva estructura organizacional y temas tecnológicos que han cambiado desde la fecha de publicación.

Norma Técnica Colombiana NTC 6047

En las visitas realizadas a los puntos de contacto y en el marco de la Norma Técnica Colombiana - NTC 6047 de 2013 “*Accesibilidad al Medio Físico espacios de servicio al ciudadano en la administración pública*” de la Dimensión 3 “*Gestión con Valores para Resultados*” del MIPG V6 - Política de Servicio al Ciudadano, respecto de la disposición de escenarios de relacionamiento, se evaluaron aspectos concernientes a la accesibilidad a espacios físicos de atención presencial al ciudadano, observándose que se ha avanzado en la adecuación de las instalaciones; no obstante, se identificaron oportunidades de mejora en lo referente a “*Señalización*”, la cual debe complementarse con símbolos gráficos para facilitar su comprensión por todas las personas, como el alto relieve y sistema Braille; en cuanto a “*Orientación e Información*” los centros de atención al ciudadano, deben contar como mínimo con señalización de atención a la población con discapacidad auditiva; y, en lo relacionado con “*Sillas Mobiliario*” se requiere mejorar la señalización para adultos mayores, niños, mujeres embarazadas, personas en condición de discapacidad, personas de talla baja y población vulnerable en general.

6.2 Evaluación del Riesgo

La DIAN cuenta con la “Política para la administración de riesgos de la Dirección de Impuestos y de Aduanas Nacionales – UAE DIAN” V3 del 04 de diciembre de 2024, la cual establece las disposiciones para que la entidad gestione de manera efectiva el sistema de

gestión de riesgos y plantea la administración objetiva, integral, participativa y dinámica de los riesgos de: cumplimiento Tributario, Aduanero y Cambiario; estratégicos; operacionales; capital humano; seguridad y salud en el trabajo; ambientales; seguridad de la información; fiscales; integridad; y de los riesgos de lavado de activos, financiación del terrorismo y financiación para la proliferación de armas de destrucción masiva – LAFT/FPADM.

De otra parte, con relación a los informes cuatrimestrales de gestión de riesgos en la vigencia 2024 y primer semestre de 2025, remitidos por los responsables a la OCI en los formatos FT-PEC-2096 “Informe de monitoreo de riesgos” y FT-PEC-2097 “Reporte materialización de riesgos”, se observó lo siguiente:

Tabla 14. Riesgos materializados relacionados con gestión de accesos.

Periodo	Área	Riesgo	Casos	Descripción
2024-01	OSI	Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad, y disponibilidad de los datos.	3	1. Indisponibilidad del módulo de importaciones del sistema siglo XXI. 2. Página falsa que suplanta servicios de la DIAN. 3. Indisponibilidad de la página de SIEX por Internet interno y externo, lo cual ocasiona que no se pueda mostrar la página.
2024-01	DGIT	Sistemas de información y servicios digitales indisponibles (no programada-fortuita) para las partes interesadas	1	1. Caída Pagina SIEX tanto por Internet Interno como por Internet Externo. 2. Indisponibilidad de los servicios aduaneros y tributarios Muisca.
2024-02	OSI	Políticas de seguridad y privacidad de la información incumplidas o no implementadas.	1	1. Incumplimiento de las políticas de privacidad y seguridad de la información, evidenciado en los Kioscos de auto gestión de los Puntos de Contacto, con ocasión de los trámites realizados por los ciudadanos
2024-02	DGIT	Sistemas de información y servicios digitales indisponibles (no programada-fortuita) para las partes interesadas	4	1. El 23/07/2024 se presentó caída de todas las instancias de Bases de Datos del clúster DIAN. 2. Errores de acceso a los servidores informáticos Muisca. 3. El 12/08/2024 se presenta lentitud, intermitencia y errores de acceso y firma de las declaraciones. Formularios 210 y 530. 4. Caída enlace MPLS ¹⁴ que concentra las sedes a nivel nacional, afectando la conectividad.

Fuente: Formatos FT-PEC-2096 y FT-PEC-2097.
Elaboró: Equipo auditor.

En el microsítio “Gestión de Riesgos” se encuentran publicadas matrices de riesgos de corrupción, estratégicos y operacionales; sin embargo, no se observan las correspondientes a los riesgos fiscales enunciados en la “Política para la administración de riesgos de la Dirección de Impuestos y Aduanas Nacionales – UAE DIAN V3”, numeral 1 “Declaración y compromiso de la UAE DIAN frente a la administración de riesgos”, a cargo de la Subdirección de procesos en cuanto a la orientación sobre los mismos.

6.3 Actividades de Control

Las matrices de riesgos de los procesos y subprocesos institucionales tienen diseñados controles para los riesgos de seguridad digital y en el sistema GRC para los riesgos de los activos de información, que están relacionados con la integridad, disponibilidad y confidencialidad de la información; sin embargo, se detectaron las siguientes oportunidades de mejora:

- Se identificó un control en la matriz de riesgos del subproceso de seguridad de la

¹⁴ MPLS es una tecnología de red que permite enviar datos de forma rápida y eficiente.

información para realizar evaluación de vulnerabilidades asociado al R3, a través de la herramienta “*Calilinus*” (*sic*); sin embargo, no se obtuvo evidencia del uso de esta, por lo que se debe proceder a la revisión y validación del control.

- Considerar la inclusión de los controles, en las matrices de riesgos, relacionadas con “*Eliminación de datos en los equipos utilizados en las terminales de autogestión (kioskos)*” y “*Prevenir el registro de información institucional en aplicativos no autorizados por la DGIT*”.
- En la herramienta de protección de bases de datos administrada por la OSI, se recomienda revisar el caso de uso que captura presuntos registros indebidos en las tablas B2 de las bases de datos de la solución tecnológica SYGA Siglo XXI, teniendo en cuenta que, por lo informado y soportado por la DGIT, las actualizaciones reportadas son válidas, cuando se trata de declaraciones anticipadas.
- Los Datacenter sitio 1 y sitio 2, se encuentran ubicados físicamente en la misma ciudad; por lo anterior se recomienda, tener en cuenta factores claves, como riesgos naturales y de orden público, para determinar la distancia física adecuada entre los mismos.

En el anexo 1, se presenta la correlación de riesgos y controles, asociados a los hallazgos identificados en esta auditoría, en donde se detallan los riesgos expuestos y materializados.

6.4 Información y Comunicación

En el desarrollo de la auditoría se evidenciaron oportunidades de mejora en este componente, relacionadas a continuación:

- Falta de actualización de los documentos del “*Listado Maestro*” frente al Mapa de Procesos vigente de la DIAN.
- Se observaron documentos físicos desatendidos en las impresoras, los cuales contienen datos institucionales, cuyo interés corresponde solamente a las partes interesadas, exponiendo la información a la manipulación o uso indebido, sin la adecuada disposición documental, por lo que se sugiere implementar mecanismos de liberación de impresión con clave.
- Falta de paginación en algunos documentos institucionales, tales como: “*Manual de Políticas y Lineamientos de seguridad de la información MN-IIT-0072 V5*”, “*Modelo de seguridad y privacidad de la información OD-IIT-0001 V4*” y “*Manual de Protección de Datos Personales MN-IIT-0062 V3*”.
- Falta de cumplimiento de la estructura de la firma en los correos electrónicos de acuerdo con el “*Manual de marca de la DIAN*”, en cuanto al cargo del remitente.
- Remisión de correos electrónicos desde buzones genéricos que no permiten identificar el remitente, dificultando la comunicación cuando se requiere aclaración o retroalimentación de la información.

- Información entregada en respuesta a solicitudes, en el marco de la auditoría, de forma tardía, incompleta, en formatos de difícil lectura, redundante (registros repetidos), en especial, en lo relacionado con la solicitud de transacciones realizadas en las soluciones tecnológicas, lo que afecta el análisis de la información de manera oportuna.
- Falta de reportes en las soluciones tecnológicas, que permitan la consulta por diferentes criterios, de manera autónoma por parte de los auditores, sin que se dependa de solicitudes a través de PST dirigidos a los responsables de los procesos y subprocesos.

Activos de información

La entidad cuenta con el aplicativo tecnológico de Gobierno, Riesgo y Cumplimiento – GRC en el cual se gestiona, entre otros, el registro, actualización y aprobación de los inventarios de activos de información, que se toma como insumo para el reporte que se publica en la opción de “*Transparencia y acceso a la información pública*” en la sede electrónica de la entidad. Revisado el registro de activos de información, se identificaron “*Aplicativos no corporativos o huérfanos*” que no se encontraban en éste; por tal razón, se recomienda atender el procedimiento *Gestión de activos de información PR-IIT-0366 V6*.

6.5 Actividades de Monitoreo

Revisado el plan de mejoramiento con corte a 15 de marzo de 2025, frente a los temas objeto de la auditoría, no se observaron hallazgos con acciones de mejora o actividades incumplidas; sin embargo, existen ocho (8) hallazgos con acciones de mejora o actividades en proceso, relacionados con la gestión de accesos: seis (6) identificados por la Oficina de Control Interno y dos (2) por la Agencia ITRC, los cuales están siendo objeto de seguimiento, monitoreo y control por los responsables del proceso.

Por otra parte, para la vigencia 2024 no se solicitó retiro de hallazgos del Plan de Mejoramiento Institucional, relacionados con los temas objeto de la auditoría.

7. FOMENTO DE LA CULTURA DEL CONTROL

Se llevó a cabo la sensibilización de “*Fomento a la cultura del control*”, el 15 de julio de 2025, en el que se trataron temas relacionados con: Gestión de accesos, gestión de riesgos, MIPG, MECL, líneas de defensa, Resolución 021 de 2022, mapa de aseguramiento, FURAG y planes de mejoramiento, con una participación de **236** funcionarios con rol “*registrador*” del orden nacional de solicitudes de permisos de accesos a las soluciones tecnológicas en el sistema Soporte TIC y de líderes informáticos de las Direcciones Seccionales.

8. RECOMENDACIONES PARTICIPACIÓN CONCURRENTE DE LA OFICINA DE SEGURIDAD DE LA INFORMACIÓN Y LA AUDITORÍA AGA2025002

La OSI en visita a las Direcciones Seccionales de Impuestos y de Aduanas de Cartagena, impartió charla sobre el Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI y realizó las siguientes recomendaciones.

- Revisar, ajustar y actualizar los activos de información.
- Registrar en el GRC el aplicativo CINSYEXP, como activo de información y reportar el mismo ante la SIC, por manejo de bases de datos con Datos personales.
- Dar cumplimiento al Procedimiento de Gestión de Accesos PR-IIT-0455 V3 y al Instructivo Operaciones para la Gestión de Accesos IN-IIT-0273 V2.
- Mejorar los controles de seguridad en los espacios físicos de las seccionales de Impuestos y de Aduanas de Cartagena.
- Tener en cuenta los lineamientos para las cámaras de grabación y los avisos de privacidad.

9. CONCLUSIONES

La Información constituye actualmente uno de los activos más importantes para planeación, gestión y toma de decisiones en las organizaciones; por tal razón, es necesario fortalecer los controles que garanticen la seguridad de ésta en los atributos de integridad, confidencialidad y disponibilidad.

En virtud de lo anterior y teniendo en cuenta que, uno de los elementos esenciales en esta estructura corresponde a la gestión de accesos, la presente auditoría abordó este aspecto, mediante la ejecución de un objetivo general y siete (7) específicos, permitiendo identificar tanto fortalezas, como retos que se deben atender desde las cuatro líneas de defensa a nivel institucional, en un esquema de gestión por procesos bajo el modelo estratégico de “*Alineación Total*” implementado por la entidad, dando lugar a 12 hallazgos, dos (2) con presunta incidencia disciplinaria y uno (1) con incidencia penal.

Es importante resaltar que la entidad cuenta con políticas, procedimientos, instructivos, cartillas y manuales, que dan orientaciones sobre la gestión de accesos a los diferentes macroprocesos, procesos y subprocesos institucionales.

Como resultado de los objetivos específicos del 1 al 5, desarrollados en la auditoría se identificaron falencias que deben ser atendidas, con el fin controlar la exposición y/o materialización de riesgos, relacionados con: falta de coherencia entre el Anexo “*Roles de las soluciones tecnológicas*” y los reportes “*Roles Activos Usuarios DIAN*”; deficiencias en la gestión de roles informáticos; uso de un aplicativo no autorizado por la entidad; suplantación de usuarios en el sistema RUT; uso de aplicativos no corporativos o huérfanos para suplir funcionalidades no cubiertas por los institucionales y brechas de seguridad en algunos de estos; deficiencias en la seguridad de las contraseñas y uso de usuarios de prueba en ambientes producción; deficiencias en la seguridad de la información en las terminales de autogestión; deficiencias en la gestión de cuentas institucionales con inactividad prolongada en servicios de VPN y plataforma de correo electrónico; e incumplimiento en la prestación del servicio “*Zona WiFi Gratis para la Gente*” en algunos de los puntos de contacto.

En cuanto a la evaluación de los componentes del Sistema de Control Interno, enmarcado en el objetivo 6, se observan oportunidades de mejora, entre otras, en lo relacionado con la claridad que se debe dar a algunos incisos del procedimiento “*Gestión de Accesos PR-IIT-0455 V3*”; la armonización de este con el “*Manual de Políticas y Lineamientos de Seguridad de la Información MN-IIT-0072 V5*”; la necesidad de actualización de la Resolución 484 de

2013; actualización de los procedimientos y matrices de riesgos con el actual Mapa de Procesos; el aprovechamiento de la herramienta de protección de bases de datos en las soluciones tecnológicas; la necesidad de la apropiación de MN-IIT-0072 V5 por parte de todos los funcionarios, para fortalecer la seguridad de la entidad y evitar estar inmersos en posibles sanciones de tipo disciplinario, fiscal o penal; y el cumplimiento a cabalidad de los lineamientos del mismo.

Dada la materialización de riesgos, y conforme a los resultados de correlación entre riesgos y controles presentados en el Anexo 1, se recomienda actualizar las matrices de riesgos institucionales, la cual debe orientarse a identificar, evaluar y gestionar los riesgos y sus respectivos controles, con el fin de mitigar la probabilidad de ocurrencia de eventos adversos que puedan afectar el cumplimiento de los objetivos institucionales; así mismo, analizar la procedencia de remisión a los órganos competentes.

Con respecto al objetivo 7, se realizó sensibilización en “*Fomento de la cultura del Control*”, con una participación de **236** funcionarios, a nivel nacional, en donde se fortalecieron conocimientos relacionados con la gestión de accesos y el control interno.


10. RECOMENDACIONES



Sin perjuicio de las recomendaciones realizadas en cada uno de los hallazgos y oportunidades de mejora, se considera atender los lineamientos y normatividad vigente en la DIAN en materia de gestión de accesos, en especial los relacionados con el “*Manual de Políticas y Lineamientos de Seguridad de la Información MN-IIT-0072 V5*” y el “*Procedimiento de Gestión de Accesos PR-IIT-0455 V3*”; así como también, fortalecer la apropiación y aplicación del “*Código de Integridad de la DIAN CG-TAH-0002 V3*” y la revisión permanente de las matrices de riesgos contemplando controles que aseguren el efectivo tratamiento, a fin de evitar la exposición o materialización de estos.



ENRIQUE CASTIBLANCO BEDOYA
Jefe Oficina de Control de interno

Proyectó: Equipo Auditor.
Yamile Fresno Forero 
Edgar Javier Ríos Molina 
Sandra del Pilar Chuquirín Badillo – Líder 

Juan Felipe Solórzano García – Apoyo Análisis de datos 

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

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
Subproceso Innovación y Tecnología V3	R1. "Sistemas de información y servicios digitales indisponibles (no programada-fortuita) para las partes interesadas"	Hallazgo No. 12 Incumplimiento en la prestación del servicio "Zona WiFi Gratis para la Gente".	C3: Monitorear el funcionamiento de la plataforma tecnológica, a través del instructivo IN-IIT-0241 Monitoreo de plataforma.	M	El control C3 es insuficiente, respecto al funcionamiento y monitoreo del servicio WIFI gratis en los puntos de contacto y no se evidenció reportada por la herramienta Orion.
	R3. "Plataforma tecnológica inadecuada para soportar los servicios tecnológicos"	Hallazgo No. 4 Deficiencias en la gestión de aplicativos no corporativos.	C30: Revisar y aprobar el plan de proyecto y monitorear su ejecución de acuerdo con el procedimiento PR-IIT-0153 Gestión de proyectos de tecnología	E	El control C30 evidencia falencias en la gobernabilidad y control de los aplicativos no corporativos a nivel nacional en la entidad.
	R4. "Información afectada en su integridad y/o confidencialidad y/o disponibilidad por incidentes de seguridad de la información"	Hallazgo No.1 Deficiencias en la coherencia entre el Anexo "Roles de las soluciones tecnológicas según procedimientos y procesos" y los reportes "Roles Activos Usuarios DIAN".	C7: Otorgar y controlar los accesos internos y externos mediante el cumplimiento de procedimiento PR-IIT-0455 V3 Gestión de accesos.	E	Deficiencias en la ejecución del control C7 debido a la falta de coherencia en la información publicada del Anexo "Roles de las soluciones tecnológicas según procedimientos y procesos" y los reportes "Roles Activos Usuarios DIAN".
		Hallazgo No.2 Deficiencias en la gestión de roles informáticos en las soluciones tecnológicas institucionales.	C7: Otorgar y controlar los accesos internos y externos mediante el cumplimiento de procedimiento PR-IIT-0455 V3 Gestión de accesos.	E	Deficiencias en la ejecución del control C7 debido a las falencias en la gestión y administración de roles informáticos en las soluciones tecnológicas institucionales.
		Hallazgo No.3 Deficiencias en la depuración de roles en sistemas corporativos que no figuran en los reportes "Roles Activos Usuarios DIAN"	C7: Otorgar y controlar los accesos internos y externos mediante el cumplimiento de procedimiento PR-IIT-0455 V3 Gestión de accesos.	E	Deficiencias en la ejecución del control C7 en cuanto la depuración de roles de sistemas corporativos que no figuran en los reportes publicados de Diannet de "Roles Activos Usuarios"
		Hallazgo No. 6 Falencias en la gestión de accesos y suplantación de usuarios en el Sistema RUT (D)	C7: Otorgar y controlar los accesos internos y externos mediante el cumplimiento de procedimiento PR-IIT-0455 V3 Gestión de accesos.	M	La ejecución del control C7 no es suficiente para la gestión y administración de accesos de las soluciones tecnológicas institucionales, evidenciando suplantación de usuarios en el Sistema RUT.
		Hallazgo No. 7 Debilidades en la gestión de roles asignados en periodos de situaciones administrativas superiores a 15 días calendario. (P)	C7: Otorgar y controlar los accesos internos y externos mediante el cumplimiento de procedimiento PR-IIT-0455 V3 Gestión de accesos.	M	El control C7 no es efectivo en la gestión de roles asignados en periodos de situaciones administrativas superiores a 15 días calendario.
		Hallazgo No. 8 Cuentas activas sin uso vinculadas a funcionarios con situaciones administrativas o retirados de la Entidad o terceros con relación terminada	C35: Aplicar los controles de seguridad NTC 27001 incorporados en los procedimientos "PR-IIT-0455 V3 Gestión de accesos", "PR-IIT-0453 Desarrollo de soluciones tecnológicas", al igual que los instructivos "IN-IIT-0245 Requerimiento de información electrónica", "IN-IIT-0249 Requerimiento de licencias de software", "IN-IIT-0242 Requerimiento de directorio en la red y el Manual de Seguridad de la Información".	E	Se observo deficiencias en el control C35 en la gestión y administración de cuentas activas sin uso vinculadas a funcionarios con situaciones administrativas o retirados de la Entidad o terceros con relación terminada
		Hallazgo No. 9 Deficiencias en la seguridad de los logs de las contraseñas y manejo de usuarios de prueba en producción en las bases de datos de SYGA SXXI.	C35: Aplicar los controles de seguridad NTC 27001 incorporados en los procedimientos "PR-IIT-0455 V3 Gestión de accesos", "PR-IIT-0453 Desarrollo de soluciones tecnológicas", al igual que los instructivos "IN-IIT-0245 Requerimiento de información electrónica", "IN-IIT-0249 Requerimiento de licencias de software", "IN-IIT-0242 Requerimiento de directorio en la red y el Manual de Seguridad de la Información".	E	Deficiencias en la ejecución del C35 respecto a la seguridad de los logs de las contraseñas y manejo de usuarios de prueba en producción en las bases de datos de SYGA SXXI
		Hallazgo No. 10 Deficiencias en la aplicación de políticas de seguridad de información en las terminales de autogestión (Kioscos)	C7: Otorgar y controlar los accesos a la plataforma tecnológica a través del procedimiento "PR-IIT-0453 Gestión de accesos" y el instructivo "IN-IIT-0242 Requerimiento de directorio en la red".	E	Se observo deficiencias en el C7 en cuanto la aplicación de políticas de seguridad de información en las terminales de autogestión (Kioscos)
Hallazgo No. 11 Deficiencias en la gestión de cuentas institucionales con inactividad prolongada en servicios como VPN (Red Privada Virtual) y plataforma de correo como VPN (Red Privada Virtual) y plataforma de correo electrónico Institucional a nivel nacional.	C7: Otorgar y controlar los accesos a la plataforma tecnológica a través del procedimiento "PR-IIT-0453 Gestión de accesos" y el instructivo "IN-IIT-0242	E	Deficiencias en el C7 en la gestión y administración de cuentas institucionales con inactividad prolongada en servicios como VPN (Red Privada Virtual) y plataforma de correo electrónico Institucional a nivel nacional.		

Matriz	Riesgo	Hallazgo	Controles de los procedimientos y matriz de riesgos	E/M	Observaciones frente a los controles
		electrónico Institucional a nivel nacional.	Requerimiento de directorio en la red".		
	R5. "Información usada de manera indebida para beneficio propio o de terceros"	Hallazgo No.3 Deficiencias en la depuración de roles en sistemas corporativos que no figuran en los reportes "Roles Activos Usuarios DIAN"	C39: Otorgar y controlar los accesos a la plataforma tecnológica a través del procedimiento "PR-IIT-0455 V3 Gestión de accesos" y el instructivo "IN-IIT-0242 Requerimiento de directorio en la red".	E	Falencias en el C39 evidenciadas en las deficiencias en la depuración de roles en sistemas corporativos que no figuran en los reportes "Roles Activos Usuarios DIAN"
		Hallazgo No. 7 Debilidades en la gestión de roles asignados en periodos de situaciones administrativas superiores a 15 días calendario. (P)	C41: Participar en las campañas de sensibilización a usuarios sobre la adopción de las políticas de seguridad de la información (MN-IIT-0072 V5 Manual de seguridad de la información).	E	La ejecución del control C41 es insuficiente para la gestión y administración de roles asignados en periodos de situaciones administrativas superiores a 15 días calendario.
		Hallazgo No. 9 Deficiencias en la seguridad de los logs de las contraseñas y manejo de usuarios de prueba en producción en las bases de datos de SYGA SXXI.	C44: Participar en las campañas de sensibilización a usuarios sobre la adopción de las políticas de seguridad de la información (MN-IIT-0072 V5 Manual de seguridad de la información).	E	Falencias en el C44 debido a las deficiencias en la seguridad de los logs de las contraseñas y manejo de usuarios de prueba en producción en las bases de datos de SYGA SXXI.
		Hallazgo No. 10 Deficiencias en la aplicación de políticas de seguridad de información en las terminales de autogestión (Kioscos)	C44: Participar en las campañas de sensibilización a usuarios sobre la adopción de las políticas de seguridad de la información (MN-IIT-0072 V5 Manual de seguridad de la información).	E	Deficiencias en la ejecución del C44 respecto a la aplicación de políticas de seguridad de información en las terminales de autogestión (Kioscos)
Subproceso de Seguridad de la información V2	R2. "Lineamientos y políticas de seguridad y privacidad de la información implementados de manera ineficiente"	Hallazgo No. 8 Cuentas activas sin uso vinculadas a funcionarios con situaciones administrativas o retirados de la Entidad o terceros con relación terminada.	C1: Realizar campañas de sensibilización a nivel nacional.	E	Falta de controles para la gestión y administración de Cuentas activas sin uso vinculadas a funcionarios con situaciones administrativas o retirados de la Entidad o terceros con relación terminada.
		Hallazgo No. 10 Deficiencias en la aplicación de políticas de seguridad de información en las terminales de autogestión (Kioscos)	C4: Realizar sesiones de sensibilización a la alta y media dirección, relacionados con tema de Seguridad de la Información.	E	Falta de controles que complementen el C4 para ejecutar la aplicación de políticas de seguridad de información en las terminales de autogestión (Kioscos)
	R3 "Medidas de seguridad y privacidad de la Información inadecuadas que amenazan la integridad, confidencialidad y disponibilidad de los datos"	Hallazgo No.1 Deficiencias en la coherencia entre el Anexo "Roles de las soluciones tecnológicas según procedimientos y procesos" y los reportes "Roles Activos Usuarios DIAN".	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.	E	Falta de aplicación del C6 para corregir las deficiencias en la coherencia entre el Anexo "Roles de las soluciones tecnológicas según procedimientos y procesos" y los reportes "Roles Activos Usuarios DIAN".
		Hallazgo No.3 Deficiencias en la depuración de roles en sistemas corporativos que no figuran en los reportes "Roles Activos Usuarios DIAN"	C7: Realizar evaluaciones de vulnerabilidades.	E	Falta de controles que complementen el C7 para corregir las deficiencias en la depuración de roles en sistemas corporativos que no figuran en los reportes "Roles Activos Usuarios DIAN". No se evidenció el uso de la herramienta "Callilinus" ni los informes de vulnerabilidades a los que se hace referencia.
		Hallazgo No. 4 Deficiencias en la gestión de aplicativos no corporativos.	C7: Realizar evaluaciones de vulnerabilidades.	E	El control C7 evidencia falencias en la evaluación de las vulnerabilidades y control de los aplicativos no corporativos a nivel nacional en la entidad. No se evidenció el uso de la herramienta "Callilinus" ni los informes de vulnerabilidades a los que se hace referencia.
		Hallazgo No. 5 Uso de aplicativo público no institucional Portal SAR (D)	C7: Realizar evaluaciones de vulnerabilidades.	M	Falta de controles que complementen el C7 para corregir las deficiencias en la depuración de roles en sistemas corporativos que no figuran en los reportes "Roles Activos Usuarios DIAN". No se evidenció el uso de la herramienta "Callilinus" ni los informes de vulnerabilidades a los que se hace referencia.
		Hallazgo No. 6 Falencias en la gestión de accesos y suplantación de usuarios en el Sistema RUT (D)	C7: Realizar evaluaciones de vulnerabilidades. C9: Solicitar la activación, inactivación de roles o modificación del anexo de roles o las credenciales de acceso	M	Falta de controles que complementen el C7 para corregir las deficiencias en la depuración de roles en sistemas corporativos que no figuran en los reportes "Roles Activos Usuarios DIAN". No se evidenció el uso de la herramienta "Callilinus" ni los informes de vulnerabilidades a los que se hace referencia. La ejecución del control C9 no es suficiente para la gestión y administración de accesos de las soluciones tecnológicas institucionales, evidenciando suplantaciones de usuarios en el Sistema RUT.

Matriz	Riesgo	Hallazgo	Controles de los procedimientos y matriz de riesgos	E/M	Observaciones frente a los controles
		Hallazgo No. 8 Cuentas activas sin uso vinculadas a funcionarios con situaciones administrativas o retirados de la Entidad o terceros con relación terminada	C8: Realizar revisión de los roles asignados al equipo de trabajo.	E	Se observó deficiencias en el C8 para la administración de Cuentas activas sin uso vinculadas a funcionarios con situaciones administrativas o retirados de la Entidad o terceros con relación terminada.
		Hallazgo No. 9 Deficiencias en la seguridad de los logs de las contraseñas y manejo de usuarios de prueba en producción en las bases de datos de SYGA SXXI.	C7: Realizar evaluaciones de vulnerabilidad.	E	Deficiencias en la ejecución del C7 respecto a la seguridad de los logs de las contraseñas y manejo de usuarios de prueba en producción en las bases de datos de SYGA SXXI. No se evidenció el uso de la herramienta "Callinus" ni los informes de vulnerabilidades a los que se hace referencia.
	R4 "Activos de información utilizados de manera indebida para beneficio propio y/o de terceros."	Hallazgo No. 10 Deficiencias en la aplicación de políticas de seguridad de información en las terminales de autogestión (Kioscos)	No se identificaron controles	E	En la matriz de riesgos del subproceso, no se identificaron controles frente a las deficiencias en la aplicación de políticas de seguridad de información en las terminales de autogestión (Kioscos)
Riesgos estratégicos de la DIAN	R4. "Pérdida de prestigio institucional"	Hallazgo No. 5 Uso de aplicativo público no institucional Portal SAR (D)	C7: TG1 Desarrollar y mantener la tecnología de la información y las telecomunicaciones para optimizar la gestión institucional y la Estrategia de Gobierno en Línea, en función de un mejor servicio al ciudadano.	E	Deficiencias en el control C7 lo que incurre en la pérdida de prestigio institucional debido al uso de información institucional en aplicativos no corporativos.
Riesgos de corrupción DIAN 2025	Información usada de manera indebida para beneficio propio o de terceros	Hallazgo No. 5 Uso de aplicativo público no institucional Portal SAR (D)	C39: Otorgar y controlar los accesos a la plataforma tecnológica a través del procedimiento "PR-IIT-0455 V3 Gestión de accesos" y el instructivo "IN-IIT-0242 Requerimiento de directorio en la red".	E	Se observó falencias en el control C39 por la posible utilización de Información de manera indebida para beneficio propio o de terceros
	Activos de información utilizados de manera indebida para beneficio propio y/o de terceros.	Hallazgo No. 5 Uso de aplicativo público no institucional Portal SAR (D)	No se identificaron controles	E	En la matriz de riesgos del subproceso, no se identificaron controles frente al uso de aplicativos no corporativos con información institucional.
Fiscalización y Liquidación V4	R8. "Información afectada en su integridad y/o confidencialidad y/o disponibilidad"	Hallazgo No. 5 Uso de aplicativo público no institucional Portal SAR (D)	C39: Diligenciar y firmar acuerdos de confidencialidad Manual de protección de datos personales	E	Deficiencias en el control C39 debido al uso de información institucional en aplicativos no corporativos.
Subproceso Compras y Contratos V3	R3 "Incumplimiento total o parcial del contrato"	Hallazgo No. 12 Incumplimiento en la prestación del servicio "Zona WiFi Gratis para la Gente".	C17: Aplicar el procedimiento PR-ADF-0433, PR-ADF-0434 y cartilla CT-ADF-0109 Cartilla de Supervisión o Interventoría	E	El control C17 presenta falencias en el cumplimiento total o parcial del contrato de prestación del servicio "Zona WiFi Gratis para la Gente" en puntos de contacto.

E= Exposición; M=Materialización.