Función Pública

INFORME DE SEGUIMIENTO IMPLEMENTACION LINEAMIENTOS GOBIERNO DIGITAL

Oficina de Control Interno

Versión 01

Abril 2026

Objetivo

Evaluar por parte de la Oficina de Control Interno el estado actual de implementación del habilitador transversal de “Servicios Ciudadanos Digitales”, acorde con los lineamientos y elementos que conforman su estructura en la Política de Gobierno Digital establecidos en el Decreto 767 de 2022.

De otro lado, verificar el estado actual de las recomendaciones generales derivadas del informe de seguimiento a la Implementación de Gobierno Digital de la vigencia 2025.

Es importante mencionar que las observaciones registradas en el presente informe de seguimiento coadyuvan a fortalecer el ambiente de control del sistema de información actual.

Alcance

Para esta vigencia se verificarán dos escenarios así:

a. Estado actual de los lineamientos que componen el habilitador de Servicios Ciudadanos Digitales, el cual según el Manual de Gobierno Digital - MGD, “busca desarrollar mediante soluciones tecnológicas, las capacidades para mejorar la interacción con la ciudadanía y organizar su derecho a utilización de medios digitales ante la administración pública.”. Este habilitador busca que todas las entidades públicas implementen lo dispuesto en el Decreto 1413 de 2017 (incorporado en el título 17, parte 2, libro 2 del Decreto 1078 de 2015), que establece los lineamientos para la prestación de los servicios ciudadanos digitales y para permitir el acceso a la administración pública a través de medios electrónicos. En dicho Decreto los servicios digitales se clasifican en los siguientes servicios básicos y su naturaleza acorde con el Decreto 1413 de 2017:

- **Autenticación Digital:** Este servicio tiene como objetivo verificar los atributos digitales de una persona cuando se adelanten trámites y servicios a través de medios digitales, afirmando que dicha persona es quien dice ser. El servicio permite generar un ambiente que habilita a los ciudadanos su acceso a los trámites y servicios de entidades públicas y privadas por medios electrónicos, con plenas garantías de confianza y seguridad.

- **Carpeta Ciudadana**: “Es aquel que permite el almacenamiento y conservación electrónica de mensajes de datos en la nube para las personas naturales o jurídicas, en donde éstas pueden recibir, custodiar y compartir de manera segura y confiable la

información generada en su relación con el Estado a nivel de trámites y servicios. En ningún caso la carpeta ciudadana hará las veces de sistema de gestión de documentos electrónicos de archivo."

- **Interoperabilidad**: Es aquella que brinda las capacidades necesarias para garantizar el adecuado flujo de información y de interacción entre los sistemas de información de las entidades del Estado, permitiendo el intercambio, la integración y la compartición de la información, con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad.

Se destaca que estos servicios son de obligatorio uso y adopción, así como servicios especiales, que son adicionales a los servicios básicos, como el desarrollo de aplicaciones o soluciones informáticas para la prestación de los servicios ciudadanos digitales básicos.

Acorde a lo anterior, para el presente seguimiento se evaluará el estado de implementación de los servicios mencionados y que sean aplicables directa o indirectamente a la operatividad de la Entidad.

b. Estado actual de las recomendaciones generales derivadas del informe de seguimiento a la Implementación de Gobierno Digital de la vigencia 2025, relacionadas con el habilitador de Seguridad y Privacidad de la Información.

1. Resultados del seguimiento

1.1. Habilitador Servicios Ciudadanos Digitales – SCD

Para la verificación a este ítem, se tomó como marco de seguimiento, la Guía de Lineamientos de los Servicios Ciudadanos Digitales - SCD de septiembre 2020, desarrollada por el MinTIC, presentándose el siguiente resultado:

Gobierno y control de gestión

- ✓ Responsabilidad: El control técnico operativo, se mantiene a través de la Coordinación de Servicios de Información - GSI de la OTIC, quien mantiene el control periódico de la gestión sobre los SCD. Es así como la gestión directa se efectúa a través del grupo de interoperabilidad conformado por dos ingenieros de planta temporal y el Coordinador del GSI. Este grupo genera un informe periódico de gestión, donde se evidencian las acciones realizadas y dando su respectivo alcance en la planeación institucional.

- ✓ Estrategia: la implementación del servicio de interoperabilidad se encuentra estratégicamente incluida en el PETI (Plan Estratégico de TI), en la gestión de información actual, donde se especifica que la Oficina de Tecnologías de la Información y las Comunicaciones ha venido implementando servicios de interoperabilidad bajo la plataforma XROAD (Capa de interoperabilidad de código abierto y distribuida que permite el intercambio de datos seguro, estandarizado y automático entre sistemas de información.) y estándares de Lenguaje Común de Información, según los lineamientos establecidos por MINTIC; cumpliendo con los tres ambientes exigidos (Pruebas, Preproducción y Producción) y debidamente actualizados y certificados por MINTIC, entre los cuales se encuentran los procesos de interoperabilidad de los sistemas de información (SIGEP). También, se relaciona como tendencia tecnológica propuesta que se deberá tener en cuenta para futuros ejercicios de prospectiva de TI, incluyéndola dentro de Proyección de las necesidades de TI para la presente vigencia.

- ✓ Reportes de gestión: Periódicamente el grupo de interoperabilidad efectúa un informe el cual permite evidenciar las acciones realizadas por el grupo, para el proceso de interoperabilidad, dando alcance a la planeación institucional. En él, se presentan las tareas del grupo enfocándose a la gestión de los servicios para mantener e implementar los procesos de interoperabilidad de los sistemas de información con las entidades con las cuales el DAFP tiene convenios de intercambio de información.(Ruta evidencia: Por cada vigencia en Yaksa/10031GSI/DOCUMENTOS_APOYO/INTEROPERABILIDAD /DOCUMENTOS/INFORMES).

  Por otro lado, en el módulo de planeación institucional del SGI, se encuentra el entregable estratégico “Sistemas de información misionales de Función Pública actualizados e interoperando”, cuya meta es “Garantizar los sistemas de información misionales de Función Pública actualizados e interoperando” y programación bimensual. Al respecto se evidencia la debida gestión y la trazabilidad respectiva.

Otro aspecto importante enmarcado en los reportes de gestión, es la autoevaluación del nivel de madurez de interoperabilidad que se reporta anualmente y que fue efectuada a finales de la vigencia 2025 (Ruta: \\yaksa\10031GSI\2025\DOCUMENTOS_APOYO\INTEROPERABILIDAD\DOCUMENTOS\MADUREZ) con el acompañamiento del grupo de lenguaje común de información de MinTIC. En esta evaluación la Entidad mediante un link generado por este Ministerio, registra en un archivo Excel la autoevaluación del cumplimiento a los lineamientos expuestos en el marco de interoperabilidad. Los resultados a nivel general se muestran a continuación, teniendo en cuenta los siguientes niveles de calificación para establecer el estado actual del intercambio de información en el que se encuentra cada entidad:

Nivel	Nombre	Descripción
1	AUSENTE	La entidad no ha empezado a implementar los lineamientos del Marco de Interoperabilidad del Estado y carece de las capacidades necesarias para implementarlo.
2	INICIAL	La entidad ha iniciado su proceso de implementación de los lineamientos del Marco de Interoperabilidad.
3	INTERMEDIO	La entidad ha venido trabajando en la implementación de los lineamientos del Marco de Interoperabilidad en algunos de sus servicios de intercambio de información
4	CONSOLIDADO	La entidad ha logrado que la implementación de los lineamientos del Marco de Interoperabilidad del Estado sea un tema conocido a nivel institucional sin embargo no ha logrado involucrar a todos los interesados
5	INSTITUCIONALIZADO	La entidad ha logrado implementar de forma adecuada los lineamientos del Marco de Interoperabilidad.

Fuente: Diagnóstico modelo de madurez interoperabilidad noviembre 2025

Dominio	Lineamiento	Criterio	Nivel actual	Resultado
Dominio Organizacional	LI.IOP.OG.04	Liderazgo del Marco de Interoperabilidad	3	3,3
	LI.IOP.OG.05	Cultura organizacional	3	
	LI.IOP.OG.01 LI.IOP.OG.02 LI.IOP.OG.03	Adecuación de procesos	4	
Dominio político legal	LI.IOP.LG.01 LI.IOP.LG.02	Normatividad para el intercambio de información	5	5
	LI.IOP.LG.03	Manejo de la información confidencial y personal	5	
Dominio semántico	LI.IOP.SM.01 LI.IOP.SM.04 LI.IOP.SM.06 LI.IOP.SM.03	Lenguaje común de intercambio de información	5	5
	LI.IOP.SM.02 LI.IOP.SM.05	Documentación de los servicios de intercambio	5	
Dominio técnico	LI.IOP.TE.01	Uso de servicios ciudadanos digitales	5	5
	LI.IOP.TE.07	Diseño funcional de los servicios web	5	
	LI.IOP.TE.07	Diseño técnico de los servicios	5	
	LI.IOP.TE.07	Pruebas de los servicios web	5	
	LI.IOP.TE.07	Despliegue de los servicios web	5	
	LI.IOP.TE.02	Infraestructura tecnológica para el intercambio de información	5	

Fuente: Diagnóstico modelo de madurez interoperabilidad noviembre 2025

Como se puede observar, tres (3) de los cuatro (4) dominios evaluados obtuvieron una calificación de cinco (5) “INSTITUCIONALIZADO”, demostrando que la entidad ha logrado implementar de forma adecuada los lineamientos del Marco de Interoperabilidad. Solamente para el dominio organizacional logro una calificación de 3,3 (INTERMEDIO), debido a que:

- ✓ Bajo el criterio ‘Liderazgo del Marco de Interoperabilidad’, existe un único responsable de intercambio de información, pero no está formalizado dicho liderazgo al interior de la entidad.
- ✓ La entidad capacita al recurso humano en temas de interoperabilidad y hace campañas con todas las áreas de la entidad para involucrarlos en los temas de interoperabilidad.
- ✓ La entidad tiene documentados sus procesos, están actualizados, pero no tienen necesidades de intercambio de información identificadas.

Acorde a lo anterior, en el mismo formato del modelo de madurez se determinaron las siguientes actividades:

- ✓ Formalizar el nombramiento del responsable y líder de interoperabilidad.
- ✓ Documentar el procedimiento detallado de interoperabilidad, según el Marco.
- ✓ Establecer Plan de Capacitación.

Sobre estas actividades no se evidencia registro de trazabilidad y gestión de las mismas.

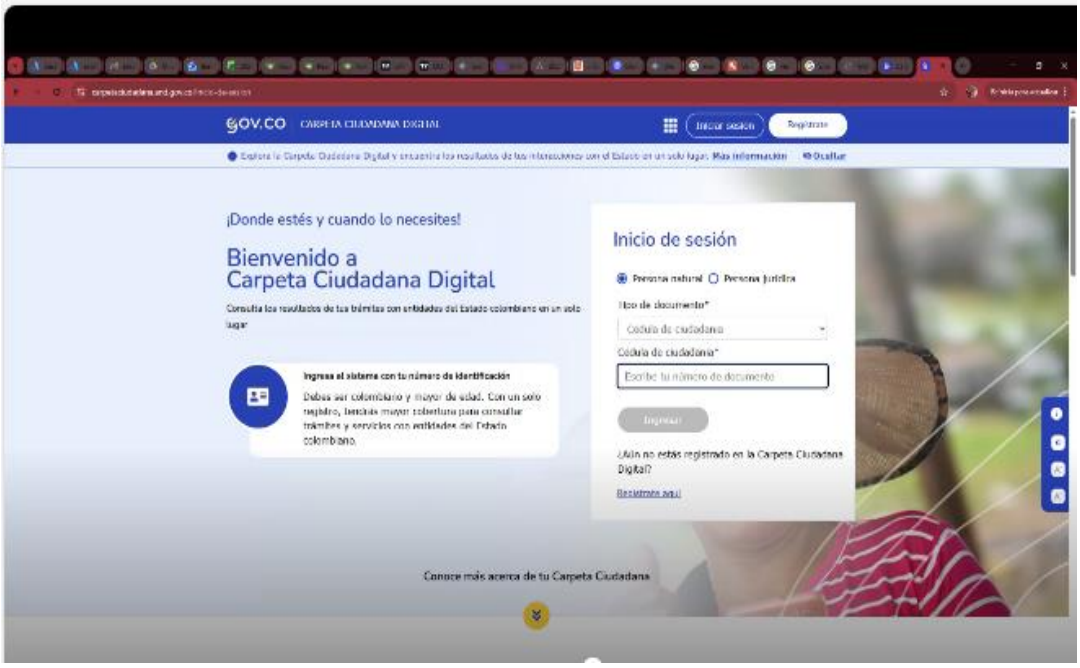
1.2. Autenticación Digital

Generalidades: El Servicio de Autenticación Digital tiene un valor estratégico que permite ofrecer a las personas un único conjunto de mecanismos de autenticación para acceder de un modo seguro y confiable a los servicios del Estado, y a su vez que las entidades puedan confiar que quien accede a un servicio en línea es quien afirma ser, de acuerdo con el nivel de riesgo del servicio. Para ello la Autenticación Digital permite:

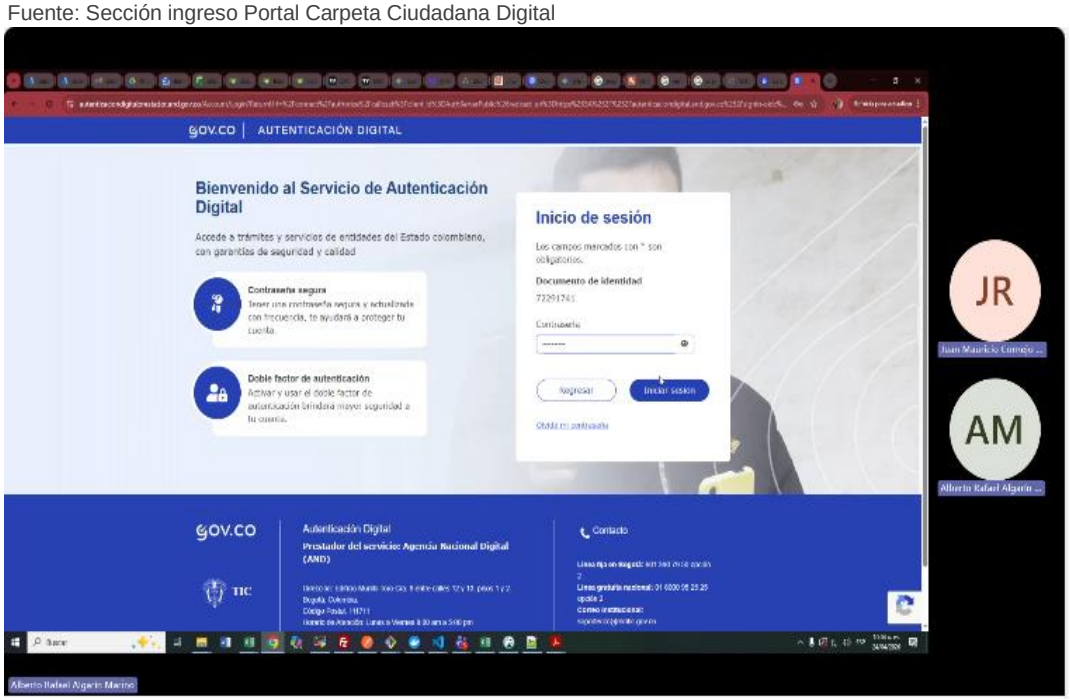
- Definir los lineamientos para que se les asegure a los ciudadanos el derecho de acceso a la administración pública por medios electrónicos en condiciones de calidad.
- Ofrecer un servicio a las entidades públicas y privadas que permita validar la identidad de los usuarios por medios digitales, mitigando los riesgos de suplantación de identidad, asegurando un nivel de seguridad apropiado para cada servicio o trámite a realizar por medios electrónicos.
- Garantizar autenticidad e integridad a los mensajes de datos dándoles admisibilidad y fuerza probatoria, de acuerdo con el nivel de garantía requerido por la entidad para un servicio específico.
- Proveer los mecanismos necesarios para que los usuarios puedan firmar mensajes de datos y así garantizar la validez jurídica de sus actuaciones con el Estado.
- Mitigar los riesgos de seguridad a los que se ven expuestos los trámites y servicios en línea.

Gestión actual

El DAFP ha venido trabando este habilitador mediante el cumplimiento de un hito del convenio con la Agencia Nacional Digital - AND, quien como entidad adscrita al MinTIC y bajo los lineamientos de Gobierno Digital funge para este caso como *articulador* dentro de los SCD, siendo responsable directo en el proceso de autenticación digital (Registro, inscripción y emisión). Al respecto, se puede evidenciar este servicio en el acceso a Carpeta Ciudadana Digital mediante el DNS “AND.gov.co”, donde al iniciar la sesión, se establece el primer grado de autenticación mediante tipo de documento y número de identificación del usuario (Ver primera imagen a continuación); luego, con un primer factor de clave y contraseña segura y un segundo nivel opcional mediante autenticación de doble factor (Ver segunda imagen).



Fuente: Sección ingreso Portal Carpeta Ciudadana Digital



Fuente: Sección autenticación Portal Carpeta Ciudadana Digital

1.3. Carpeta ciudadana

Generalidades: Es el servicio que les permite a las personas naturales o jurídicas, acceder y gestionar digitalmente el conjunto de datos almacenados o custodiados por la Administración Pública, de forma segura y confiable.

Este servicio se enmarca en lo definido en la Política de Gobierno Digital y en el cumplimiento de la normatividad vigente. En este escenario, el uso del servicio ciudadano digital de carpeta ciudadana es obligatorio para las entidades públicas, y optativo para las personas naturales y jurídicas.

En el servicio de Carpeta Ciudadana Digital se definen los actores de los Servicios Ciudadanos Digitales involucrados en el desarrollo de este servicio y los elementos que interactúan para el envío y recepción de la información necesaria para un correcto cumplimiento de los objetivos establecidos.

A continuación, se describen los roles relacionados con el Servicio de Carpeta Ciudadana Digital y que se encuentran establecidos en los lineamientos de la Política de Gobierno Digital:

- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC): Encargado del desarrollo de la normatividad, lineamientos y requerimientos técnicos necesarios para que el servicio de Carpeta Ciudadana Digital se desarrolle de forma efectiva.
- Articulador (AND): En cumplimiento de la prestación del servicio de Carpeta Ciudadana Digital, debe entre otros:

  a. Integrar el servicio de Autenticación digital para que el usuario logre la autorización de ingreso a su carpeta.
  b. Integrar el servicio de Interoperabilidad para lograr el intercambio de datos entre entidades del Estado.
  c. Generar la estructuración de los datos acorde a los requerimientos establecidos para los servicios de Carpeta Ciudadana Digital.
  d. Diseñar el componente sobre el cual va a funcionar el servicio de Carpeta Ciudadana Digital.
  e. Administrar el componente destinado para prestar el servicio de Carpeta Ciudadana Digital.
  f. Gestionar la operación propia, derivada de la prestación del servicio y los datos recolectados de esta, para generar reportes, estadísticas e informes.

g. Brindar acompañamiento a las entidades en cuanto al proceso de provisión de la Carpeta Ciudadana Digital, si es requerido de manera especial, así como dentro del acompañamiento general a la implementación de los servicios ciudadanos digitales base.
h. Administrar la Información procedente de la prestación del servicio.
i. Garantizar las condiciones de seguridad y privacidad requeridas por el servicio, para garantizar aspectos como la integridad, la confidencialidad y la disponibilidad de la información, así como los niveles de acceso a la misma.

- Usuarios: representa a la persona natural, nacional o extranjera titular de cédula de extranjería, o la persona jurídica, de naturaleza pública o privada, que hace uso de los Servicios Ciudadanos Digitales.

- Portal Único del Estado GOV.CO: teniendo en cuenta que el Portal Único del Estado es una herramienta de integración y punto de acceso digital del ciudadano, será el medio a través del cual el usuario pueda ingresar para hacer uso del servicio de la Carpeta Ciudadana Digital.

- Servicio de Autenticación Digital: desde la perspectiva del servicio de Carpeta Ciudadana Digital, el servicio de Autenticación Digital es el encargado de proveer el mecanismo de autenticación para que el usuario obtenga las credenciales necesarias para lograr ingresar a su Carpeta.

- *Servicio de Interoperabilidad*: el servicio de Interoperabilidad es fundamental para una correcta prestación del servicio de Carpeta Ciudadana Digital, teniendo en cuenta que de esta integración dependerá el impacto que obtenga el ciudadano de la Carpeta, así como la utilidad de los datos que se logren exponer al usuario; por otro lado, también es el habilitador para la comunicación entre el usuario y la Administración Pública en cuanto a las solicitudes de actualización de sus datos.

- *Entidad*: es el actor encargado de suministrar los datos e información que posea del usuario para ser expuesta a través de la carpeta, de manera tal que deberá habilitar los servicios de información requeridos, bien sea desde sus sedes electrónicas o de sus sistemas de información. Así pues, es necesario para la correcta prestación del servicio de Carpeta:

  a. Que cumpla con los requerimientos establecidos para la habilitación del servicio de Interoperabilidad.

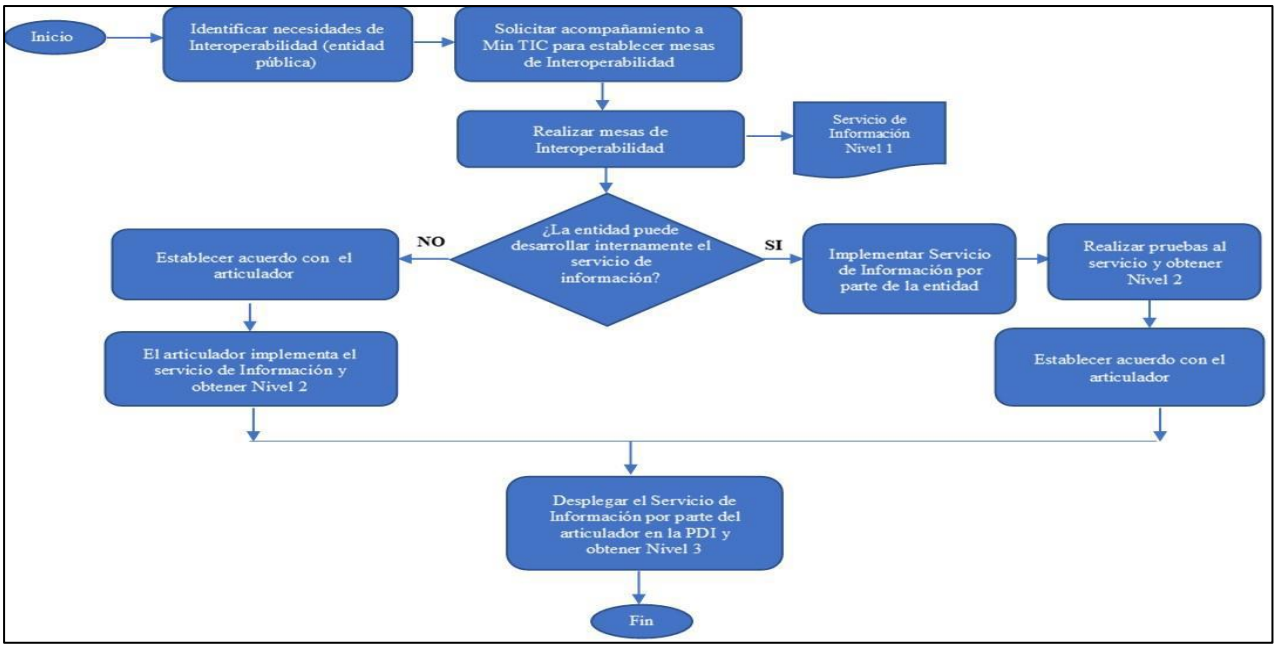
b. Cumplir las directrices y lineamientos establecidos en el marco de interoperabilidad y del lenguaje común de intercambio de información, formulados por MinTIC.

Gestión actual

Actualmente, el DAFP en su rol de "entidad" ha habilitado al SIGEP como sistema de información requerido, exponiendo la información relacionada con la Hoja de Vida consumida en la consulta de hojas de vida en el portal GOV.co - Carpeta ciudadana, donde a través del sector "Trabajo, empleo, pensión", se puede consultar dicha hoja por usuario autenticado.

1.4. Interoperabilidad

Generalidades: Acorde con los lineamientos de los SCD inmerso en la guía de MinTIC respectiva, las entidades deben realizar las actividades de alistamiento para la interoperabilidad que se ilustran en el siguiente esquema:



Fuente: Anexo 1 Guía de lineamientos de SCD – Política de Gobierno Digital

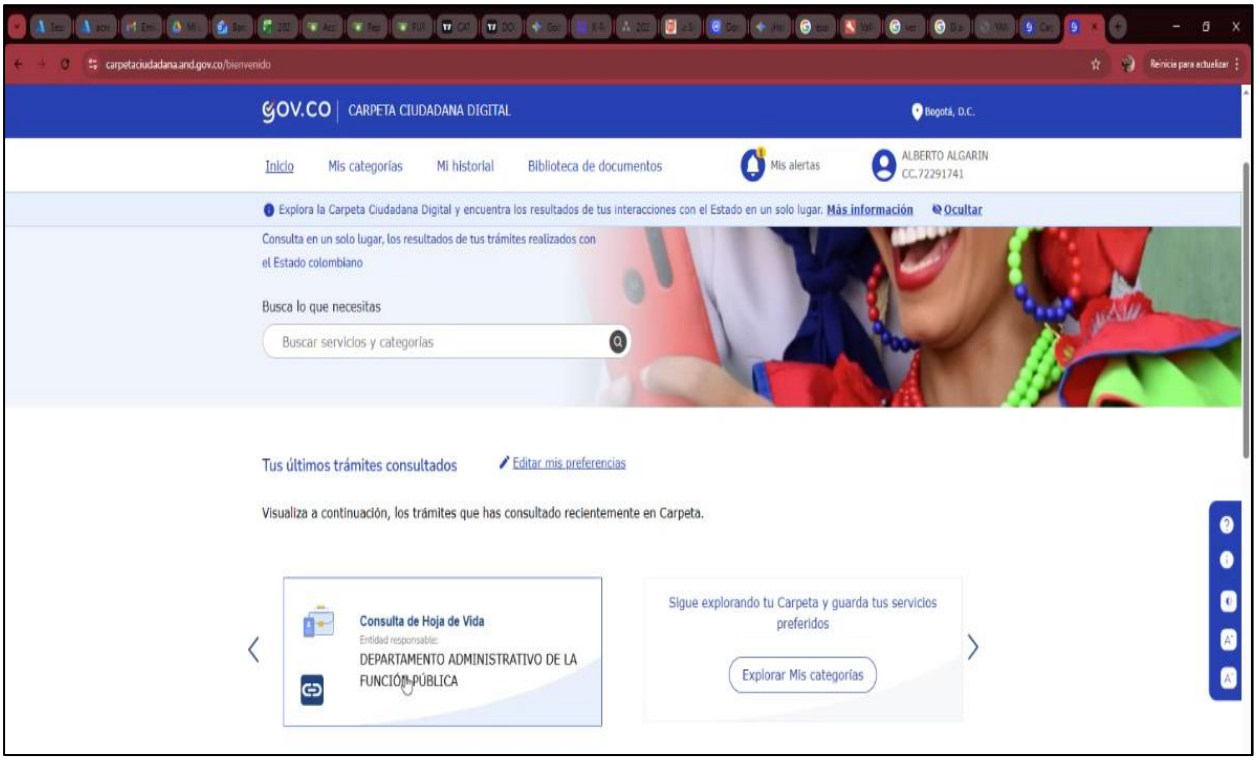
La gestión sobre estas actividades, se evidencian en los diferentes frentes de madurez de la implementación de cada entidad vigencia a vigencia, en la carpeta compartida Yaksa del GSI (10031).

Gestion Actual

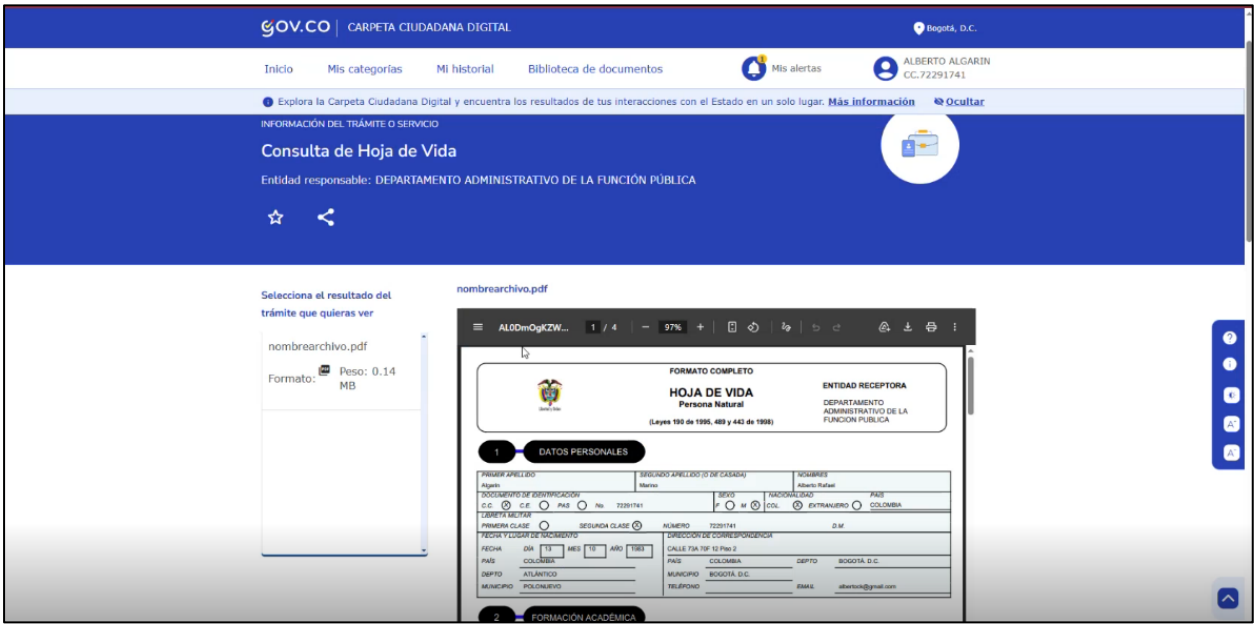
A nivel general, se evidencia el acervo de las actividades de alistamiento mencionadas en la figura anterior por cada entidad con la que el DAFP tiene establecida interoperabilidad, tanto en ambiente productivo, como en desarrollo. Esta documentación por entidad se encuentra en el servidor de carpetas compartidas Yaksa, en documentos de apoyo / interoperabilidad.

Actualmente la Entidad, con relación a este modelo de servicio, viene gestionando los siguientes frentes en ambiente ***productivo***:

- **Consulta de hojas de vida SIGEP - CCD**: vista que se enlaza con el modelo de carpeta ciudadana del portal GOV.CO, donde a través del sector “Trabajo, empleo, pensión”, se puede consultar la hoja de vida, en la cual se puede ver la información respectiva desde SIGEPII, como se ve a modo de ejemplo en la siguiente imagen, además, de poder ser descargada por el usuario en el formato respectivo.



Fuente: Portal GOV.co – consulta Hoja de Vida



Fuente: Portal GOV.co – consulta Hoja de Vida

- **Rama Judicial – Consejo Superior de la Judicatura (CSDJ) - EFINOMINA**

  La interoperabilidad con rama judicial sigue vigente y en continuo consumo. Se sigue brindando el soporte para el consumo de servicio de hoja de vida SIGEP.

  Los soportes de gestión se tienen en la ruta: \\yaksa.dafp.local\10031GSI\2025\DOCUMENTOS_APOYO\INTEROPERABILIDAD\CSDJ

- **Departamento Administrativo del Servicio Civil Distrital (DASCD)**

  Se mantiene la disponibilidad de los servicios de QA, preproducción y producción.

  Actualmente se tiene en QA y Preproducción el desarrollo de consulta, registro y modificación de bienes y rentas desde el SIDEAP al SIGEP.

  Productivamente se tiene el servicio de consulta, registro y modificación de hojas de vida.

  Soportes en la ruta: \\yaksa.dafp.local\10031GSI\2026\DOCUMENTOS_APOYO\INTEROPERABILIDAD\DASCD

\\yaksa.dafp.local\10031GSI\2025\DOCUMENTOS_APOYO\INTEROPERABILIDAD\DASCD
\\yaksa.dafp.local\10031GSI\2024\DOCUMENTOS_APOYO\INTEROPERABILIDAD\DASCD

- **Departamento Administrativo Nacional de Estadística – DANE**

  Entidad en ambiente productivo desde la vigencia 2023 con el consumo del servicio del indicador de ODS (Objetivo de Desarrollo Sostenible) liderado por la DEP de Función Pública. Este servicio tiene el propósito de permitir al DANE, en cumplimiento de los mandatos constitucionales, revisar la adecuada y efectiva participación de las mujeres en todos los niveles de las ramas y demás órganos del poder público.

  Soportes en la ruta:
  \\yaksa.dafp.local\10031GSI\2023\DOCUMENTOS_APOYO\INTEROPERABILIDAD\DANE
  \\yaksa.dafp.local\10031GSI\2024\DOCUMENTOS_APOYO\INTEROPERABILIDAD\DANE

- **Superintendencia de Notariado y Registro - SNR**

  Entidad en ambiente productivo desde la vigencia 2023 con el consumo del servicio de Hoja de Vida del SIGEP de parte de Función pública.

  Soportes en la ruta:
  \\yaksa.dafp.local\10031GSI\2023\DOCUMENTOS_APOYO\INTEROPERABILIDAD\SNR
  \\yaksa.dafp.local\10031GSI\2022\DOCUMENTO_APOYO\INTEROPERABILIDAD\SNR

Con respecto a las entidades que se encuentran en proceso de habilitación para interoperar se encuentran las siguientes:

- **Registraduría Nacional del Estado Civil - RNEC**

  Estado actual: En este periodo no se avanza con esta interoperabilidad, ya que se está esperando la modificación de SIGEP, para que llame el servicio de calidad de Interoperabilidad y lograr mostrar resultados a la RNEC para que sean proporcionadas las credenciales productivas para lograr instalar en producción la Interoperabilidad.

  Soportes en la ruta:
  \\yaksa.dafp.local\10031GSI\2024\DOCUMENTOS_APOYO\INTEROPERABILIDAD\RNEC
  \\yaksa.dafp.local\10031GSI\2025\DOCUMENTOS_APOYO\INTEROPERABILIDAD\RNEC

- **Agencia Nacional de Tierras - ANT**

  Estado actual: Pendiente dé respuesta sobre el convenio interadministrativo, para el intercambio de información y socialización del avance de su desarrollo. En el informe de interoperabilidad de marzo 2026 se especifica la gestión histórica:

  "2025-12-26, se envía el documento del convenio interadministrativo para el intercambio de información.
  2026-01-26, se solicita retroalimentación para obtener respuesta del documento definitivo del convenio interadministrativo, se envía diccionario de datos.
  2026-03-13, se informa que hubo cambio de IPs (Protocolo de Internet) por cambio de proveedor de internet, por lo cual del lado de ANT es necesario realizar modificaciones en la configuración de nuestras nuevas IPs.
  2026-03-20, después de la configuración de las nuevas IPs, la ANT confirma consumo exitoso a nuestro servicio por medio de XRoad."

  Soportes de gestión rutas:
  \\yaksa.dafp.local\10031GSI\2025-2026\DOCUMENTOS_APOYO \INTEROPERABILIDAD \ANT

- **Contraloría General de la República - CGR**

  Estado actual:

  2026-01-26, se entregan los diccionarios de datos de los dos servicios solicitados.
  2026-03-13, se socializa nuevas IPs de los servidores de interoperabilidad, para que del lado de la CGR realicen el cambio.
  2026-03-16, se tiene sesión para consumo previa configuración de las IPs, en donde se confirma correcta respuesta del servicio, se acuerdan los lineamientos técnicos, documentales y procedimentales para avanzar con el paso a producción.

  Soportes de gestión rutas:

  \\yaksa.dafp.local\10031GSI\2025\DOCUMENTOS_APOYO\INTEROPERABILIDAD\CGR
  \\yaksa.dafp.local\10031GSI\2026\DOCUMENTOS_APOYO\INTEROPERABILIDAD\CGR

\\yaksa.dafp.local\10031GSI\2024\DOCUMENTOS_APOYO\INTEROPERABILIDAD\CGR
\\yaksa.dafp.local\10031GSI\2023\DOCUMENTOS_APOYO\INTEROPERABILIDAD\CGR
\\yaksa.dafp.local\10031GSI\2022\DOCUMENTO_APOYO\INTEROPERABILIDAD\CGR

- **Registro de Deudores Alimentarios Morosos – REDAM**

  Se cuenta con acceso a los ambientes de calidad, preproducción y producción. Queda pendiente realizar el desarrollo interno para que desde SIGEP, puedan consumir el servicio de REDAM.

  Gestión histórica:

  2026-01-27, se realiza seguimiento de configuración de las IPs nuestras, para validar consumo en ambiente de calidad.
  2026-03-06, se tiene sesión para validar permisos de QA, se logra conexión.
  2026-03-16, se tiene sesión para validar permisos de producción, se logra conexión.

  Soportes de gestión rutas:

  \\yaksa.dafp.local\10031GSI\2025\DOCUMENTOS_APOYO\INTEROPERABILIDAD\REDAM
  \\yaksa.dafp.local\10031GSI\2026\DOCUMENTOS_APOYO\INTEROPERABILIDAD\REDAM

- **Departamento Administrativo de la Presidencia de la República– DAPRE**

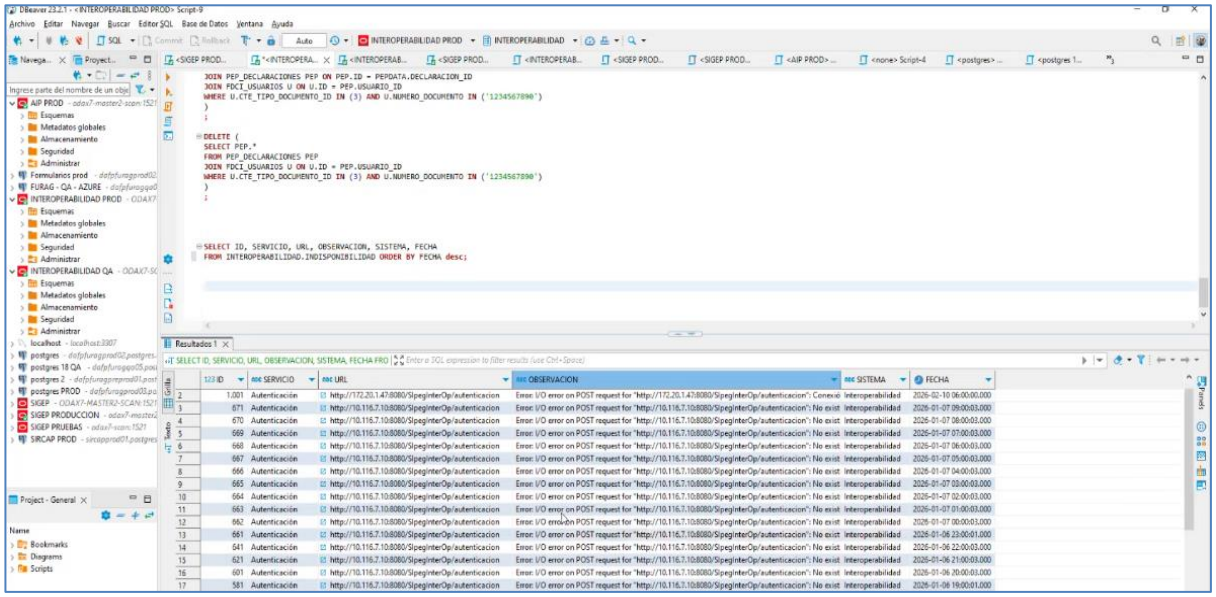
  Se encuentra en proceso de aprobación de la información a compartir por parte de la DEP. Se evidencia correos cruzados al respecto. No se tiene convenio interadministrativo aún.

  Soportes de gestión rutas:
  \\yaksa.dafp.local\10031GSI\2026\DOCUMENTOS_APOYO\INTEROPERABILIDAD\DAPRE

Operación de la plataforma

Según la guía de lineamientos de SCD de Gobierno digital, en la prestación del servicio de interoperabilidad, las autoridades deben considerar algunos procesos de administración, en especial, los relacionados con la gestión de la capacidad, gestión de la continuidad del servicio y gestión de la disponibilidad. A continuación, se presenta el estado actual de cada escenario:

- Gestión de la continuidad del servicio / disponibilidad: Al respecto, los tiempos de indisponibilidad (Cuando falla un consumo en el servicio) se están registrando automáticamente en el sistema y queda almacenada su trazabilidad y registro en una tabla de la base de datos, como se puede observar a continuación:



Fuente: Vista tabla interoperabilidad.indisponibilidad 24-04-2026

No obstante, no se está generando un indicador periódico de indisponibilidad de la tabla mencionada, el cual con la avenencia del coordinador de interoperabilidad se podría extractar de manera periódica y se incluiría como información estadística en el informe de gestión de los servicios productivos y en curso.

Con relación la continuidad de los servicios, si bien la Entidad tiene los planes de contingencia y continuidad de los sistemas misionales, no se videncia un plan para el ambiente de interoperabilidad el cual segure que el intercambio de datos entre sistemas críticos persista durante emergencias o fallos.

- Gestión de la Capacidad: Permite planificar la capacidad de procesamiento necesaria para la prestación de las capacidades de la plataforma de interoperabilidad. Al respecto, la capacidad sugerida que recomendó la AND para la instalación de la infraestructura sobre los ambientes productivos de XROAD de interoperabilidad, fue totalmente acatada por el DAFP, de acuerdo

al convenio interadministrativo 231 de 2019. Hasta el momento no se han presentado temas de encolamiento o rendimiento en tiempos de respuesta.

Las especificaciones deseadas establecidas por la AND, se evidencian en el documento "Especificaciones del servidor de seguridad x-ROAD", ubicado en la ruta: \\yaksa.dafp.local\10031GSI\2019\DOCUMENTO_APOYO\PROYECTOS\INTEROPERABILIDAD\AND\AUTENTICACION. Las especificaciones deseadas fueron:

- Sistema operativo Ubuntu 18.04 de 64 bits
- 2 CPU Intel o AMD o compatible de doble núcleo de 64 bits. El soporte del conjunto de instrucciones AES es altamente recomendado.
- 16 GB RAM
- 20 GB de espacio libre en disco duro (partición del Sistema operativo). 20-40 GB de espacio libre en disco /var/
- Alta disponibilidad

1.2. Seguimiento a recomendaciones específicas a la implementación del habilitador de seguridad y privacidad de la información del informe de seguimiento vigencia 2025

Generación del documento del Plan Estratégico de Seguridad de la Información - PESI acorde a la plantilla suministrada en el modelo de gobierno digital

Se evidencia en la ruta: \\Yaksa\10030otic\2025\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\PLAN_ESTRATEGICO_SEGURIDAD, el documento del PESI denominado "Plan_estrategico_seguridad_informacion_2025_completo", totalmente actualizado con la plantilla sugerida por el producto tipo de Gobierno Digital.

Al respecto, solo queda recomendar mantener siempre este modelo del PESI para las siguientes vigencias. Generando el documento completo (Word) según la plantilla y el plan en Excel publicado en la sección de transparencia de la página Web del DAFP, con el apoyo de la OAP.

De otro lado, como se había recomendado, se incorporaron las actividades relacionadas en el PESI, así como las de los demás productos tipo del habilitador, en la planeación institucional

centralizada en el SGI, permitiendo así una visión integral y coordinada de los compromisos estratégicos, su nivel de gestión y su trazabilidad en el tiempo. (Soportes en la ruta: \\yaksa.dafp.local\10030OTIC\2026\DOCUMENTOS_APOYO\SEGURIDAD\REPORTE_SGI). Sobre este aspecto es Importante, mantener su consecución como se ha venido desarrollando para cada vigencia.

Segregación de los roles del Oficial de Seguridad de la Información (CISO) con el Especialista de Seguridad de la Información de la OTIC

Como se había observado el año pasado, el DAFP por temas coyunturales había unificado dichos roles en un solo profesional, lo cual va en contravención a lo estipulado en el Manual de Políticas de Seguridad de la Información y en la norma ISO 27001 en su sección A.6. Organización de la Seguridad de la Información, donde se especifica que estos roles deben mantener independencia y autonomía, así como una debida segregación de funciones. A la fecha, esta situación permanece en la misma condición.

Por lo anterior, se reitera a la Administración tomar las medidas pertinentes sobre el asunto.

Complementación e inclusión de numerales en la estructura del documento de la Política General de Seguridad de la información - PGSI de acuerdo a los lineamientos de la plantilla dada por el modelo de Gobierno Digital

Verificando el documento borrador de la PGSI, que se mantiene en construcción para esta vigencia, se pudo evidenciar en la actualización el ajuste y complementación de los elementos pendientes que se habían evidenciado en el seguimiento de la vigencia pasada así:

Titulo	Estado 2025	Cumplimiento 2026
Compromiso de la alta Dirección	Cumple. Numerales: 2. Compromisos y responsabilidades y 3. Cumplimiento. ***Tener en cuenta para una siguiente versión si se puede indicar expresamente la asignación de recursos suficientes (tecnológicos y talento humano calificado), en los compromisos y responsabilidades de la Alta Gerencia.***	Ajustado el tema de asignación de recursos acorde a lo recomendado (Numeral 11 de la Política)
Organización de la seguridad de la	***Cumple parcialmente***. Numeral 2.1 Roles y Responsabilidades. ***No se evidencia las***	Ya se incluyeron las responsabilidades del Comité de

información (roles y responsabilidades)	***responsabilidades del Comité de Gestión y Desempeño, Grupo de Gestión Humana, Oficina Asesora de Comunicaciones y Grupo de gestión Contractual*** .	Gestión y Desempeño, las demás siguen pendientes. **Nueva recomendación**: *Incluir las responsabilidades de los roles del Grupo de Gestión Humana, Oficina Asesora de Comunicaciones y Grupo de gestión Contractual*
Sanciones	No cumple. "***Se debe definir como procederá la entidad en caso de que alguno de los integrantes de la entidad incumpla con las políticas o lineamientos de seguridad de la información de la entidad (se pueden incluir o mencionar los lineamientos relacionados con este tema).***"	Se incluyó al respecto el proceder de la entidad frente al incumplimiento de las políticas. (Numeral 12)
Seguimiento, medición, análisis y evaluación del SGSI	No cumple. ***"Se debe indicar como la entidad realizará seguimiento a la implementación del SGSI, si establecerá indicadores, a través de comités, revisiones por la dirección."***	En el PESI 2026 se incluyeron los siguientes Hitos: 1. Realizar análisis periódico de indicadores de gestión y desempeño del Sistema de Gestión de Seguridad de la Información 2. Realizar diagnósticos de cumplimiento frente a requisitos normativos y estándares aplicables **Nueva recomendación:** *Verificando que estos hitos se pueden estandarizar en la gestión de cada vigencia, incluir un capítulo dentro del documento de la PGSI relacionando el seguimiento y medición con los hitos mencionados*
Aprobación y revisiones a la política	No cumple. ***"Se debe definir la periodicidad en que la política general de seguridad de la información será revisada, actualizada y aprobada por la entidad, adicionalmente deben indicarse***	Aún no se ha incluido esta información en la PSGI. *Se recomienda con el apoyo de la OAP, incluir un numeral en la*

	las situaciones por las cuáles se harían revisiones o actualizaciones .	*Política relacionada con la definición mencionada en la recomendación inicial.*

Con relación a lo anterior, una vez se complementen los elementos pendientes se sugiere que, en el Comité Institucional de Gestión y Desempeño, sea presentada y aprobada la nueva versión de la PGSI.

Todos los soportes de esta gestión se evidenciaron en la ruta: \\Yaksa\10030otic\2026\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS 2026-03-10_Politica_general_seguridad_informacion

Análisis e inclusión de ítems en el Manual de Políticas de Seguridad de acuerdo a los lineamientos de la plantilla dada por el modelo de Gobierno Digital

Revisando el manual oficial de Políticas de Seguridad de la Información aprobado en noviembre de 2025, se pudo evidenciar que se efectuaron los ajustes recomendados, conteniendo así todos los elementos exigidos por la plantilla del producto tipo del Gobierno digital acorde a lo recomendado en el informe de la vigencia 2024, a excepción del título denominado “Sensibilización y comunicación en seguridad de la información” , el cual debe tener los aspectos normativos relacionados con Sensibilización y comunicación y Capacitaciones en seguridad a los funcionarios de la entidad.

Por lo anterior, se recomienda para la siguiente versión del manual incluir dicho numeral y la correspondiente normatividad con el apoyo de la OAP y la OAC.

Complementación de la información contenida en el formato de inventario de activos de información de Función Pública, con lo establecido en el producto tipo de gobierno digital en la matriz de inventario y clasificación de activos de información

El formato de inventario de activos fue completando con la información requerida acorde con la plantilla del producto tipo correspondiente. Tal y como se pudo evidenciar en el formato ubicado en la carpeta : \\Yaksa\10030otic\2025\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\. Además, este formato fue socializado a la OAP, con el fin de revisar este formato, el cual fue enviado al GGD y a OTIC, para su gestión pertinente.

Ajuste y completez de la matriz de amenazas en la gestión de riesgos actual con la información requerida en la plantilla del producto tipo a nivel de todos los activos de información identificados

Se evidencia la matriz de riesgos de seguridad de la información actual, estructurada acorde con la información de la plantilla de producto tipo de GD (Ruta: \\Yaksa\10030otic\2025\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\PLAN_TRATAMIENTO_RIESGOS_SEGURIDAD). En esta plantilla, se evidencian los riesgos identificados en la sábana de riesgos del SGI y ya se encuentran implementados e identificados los siguientes atributos que no fueron evidenciados en el seguimiento de la vigencia 2025: proceso, tipo de activo, la vulnerabilidad (Causa raíz), la descripción del riesgo, el control o controles asociados y su descripción, los atributos de cada control, fechas de implementación y seguimiento de las acciones.

Al respecto, es importante tener en cuenta que los nuevos riesgos de seguridad de la información que se vayan identificando y analizando en el proceso de Tecnologías de la Información, sean registrados en este formato. Así como la integración de todos los que correspondan a los demás procesos de la entidad bajo este mismo tipo (Seguridad digital"), bajo la coordinación de la OAP.

Conclusiones y recomendaciones

1. Se evidenció a nivel general adecuados controles en cuanto a:

   - ✓ Seguimiento al desarrollo de las actividades de mantenimiento e implementación de los procesos de interoperabilidad de los sistemas de información a través del registro de avance de los proyectos en la planeación institucional del SGI y a la gestión propia del Grupo de Interoperabilidad.
   - ✓ Presentación de informes periódicos de gestión sobre los servicios en ambiente productivo y en curso por parte del grupo de interoperabilidad.
   - ✓ Monitoreo y diagnóstico periódico del estado de madurez de Gobierno Digital para Interoperabilidad, a través de la herramienta establecida por MinTIC que permite a las entidades evaluar su progreso en el intercambio de información.
   - ✓ Mantenimiento y continuidad en la consecución de la actualización, documentación, aprobación y divulgación de la totalidad de los productos tipo que conforman el habilitador de seguridad y privacidad de la información, y prioritariamente a los elementos que conforman la estrategia, asegurando así el cumplimento a lo estipulado en el manual de gobierno digital y a lo establecido en la Decreto 612 de 2018 y la resolución 500 de 2021 establecida por MinTIC. Este resultado, refleja la debida gestión efectuada por la CISO y en gran parte a las recomendaciones generadas por la OCI en los informes de seguimiento de vigencias anteriores.

2. Se recomienda que las actividades de mejora que fueron identificadas como resultado de la aplicación de la herramienta de diagnóstico del estado de madurez de interoperabilidad, la cual fue aplicada a finales de la vigencia pasada, sean incluidas en los informes periódicos de gestión de interoperabilidad. Esto con el fin de dar continuidad, registro, seguimiento y oportunidad a su implementación en pro de la mejora continua y con el objetivo de lograr la implementación adecuada de los lineamientos del marco de interoperabilidad.

3. Con base en la tabla de indisponibilidad del servicio de interoperabilidad que se mantiene automáticamente en el base de datos (XRoad) , generar de manera mensual un indicador que permita **medir el tiempo o la frecuencia con la que los sistemas de información no pueden intercambiar datos** entre sí, permitiendo evaluar la estabilidad de la conexión entre entidades. Este indicador se puede incluir en los informes de gestión generados por el Grupo de Interoperabilidad de la OTIC.

4. Efectuar la implementación de las recomendaciones pendientes que hacen parte de la documentación del habilitador de Seguridad y Privacidad de la Información, mencionadas en el numeral 1.2 de este informe. Esto con el fin de lograr el 100% de cumplimiento sobre los lineamientos del producto tipo de Gobierno Digital.

Jorge Iván De Castro Barón

Firmado digitalmente por Jorge Iván De Castro Barón
Fecha: 2026.04.30 12:09:16 -05'00'

Jorge Iván De Castro Barón
Jefe de Control Interno

Elaboró: Juan Mauricio Cornejo R. - Contratista Oficina de Control Interno
Revisó y aprobó: Jorge Iván de Castro Barón - Jefe Oficina Control Interno

Función Pública

INFORME DE SEGUIMIENTO IMPLEMENTACION LINEAMIENTOS GOBIERNO DIGITAL

Versión 1
Proceso de Evaluación Independiente
Mayo 2025