Función Pública

INFORME DE SEGUIMIENTO IMPLEMENTACION LINEAMIENTOS GOBIERNO DIGITAL

Oficina de Control Interno

Versión 01

Mayo 2025

Glosario

Política de Gobierno Digital: La Política de Gobierno Digital es la política del Gobierno Nacional que propende por la transformación digital pública. Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC. Hace parte del Modelo Integrado de Planeación y Gestión - MIPG y se integra con las políticas de Gestión y Desempeño Institucional.
Gobernanza: Este elemento se basa el relacionamiento entre el orden nacional y territorial, y el nivel central y descentralizado. Asimismo, involucra a los grupos de interés en la toma de decisiones, la definición de los focos estratégicos de acción y la distribución de los recursos disponibles. Innovación Pública Digital: La Política de Gobierno Digital propenderá por la generación de valor público a través de la introducción de soluciones novedosas y creativas que hagan uso de las TIC y de metodologías de innovación, para resolver problemáticas públicas desde una perspectiva centrada en los ciudadanos.
Estándar: Es el conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Un estándar se construye a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular, implican uniformidad y normalización y es de obligatorio cumplimiento.
Lineamientos: Directriz o disposición establecida por MinTIC, que debe ser implementada por las entidades públicas para el desarrollo de la Política de Gobierno Digital y se desarrolla a través de estándares, guías, recomendaciones o buenas prácticas.
Habilitador: Son elementos fundamentales que permiten el desarrollo de los componentes de la política de gobierno digital.
Confidencialidad: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
Integridad: Propiedad de la información que busca preservar su exactitud y completitud.
Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

Sistema de Gestión de Seguridad de la Información: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

CISO (Chief Information Security Officer): Oficial de seguridad de la información.

Objetivo

Evaluar por parte de la Oficina de Control Interno el estado actual de implementación del habilitador transversal de “Seguridad y Privacidad de la Información”, acorde con los productos tipo y elementos que conforman la estructura de la Política de Gobierno Digital establecidos en el Decreto 767 de 2022. 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 el presente año se verificará el estado actual de los lineamientos que componen el habilitador de Seguridad y Privacidad de la Información, el cual según el Manual de Gobierno Digital - MGD, “busca desarrollar capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de datos.”.

Fuente: Manual de Gobierno Digital (https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/)

Acorde a lo anterior, para el presente seguimiento se evaluará el estado de implementación de los siguientes elementos que componen la hoja de ruta del habilitador, donde se despliegan los productos tipo que lo componen:

Fuente: Hoja de ruta habilitador Seguridad y privacidad de la información – Manual Gobierno Digital

1. Antecedentes

- **Responsabilidad seguridad y privacidad de la información:** La Entidad unificó para la vigencia 2025 los roles del Oficial de seguridad – CISO que pertenecía a la Oficina Asesora de Planeación, con el especialista en seguridad de la información de la OTIC, quedando este rol a cargo de la OTIC. Lo anterior, debido a que para esta vigencia la Entidad no tenía establecido el rol del Oficial como en vigencias anteriores.
- **Recurso humano**: No se tiene este recurso en esta vigencia para mantener los habilitadores de gobierno digital, como se había tenido en vigencias anteriores. La OTIC hasta donde su recurso lo permite se está haciendo cargo directamente de algunos habilitadores.
- **Planeación gestión**: La OTIC desarrollo en la presente vigencia un plan para la implementación de la Política de Gobierno Digital, mediante el establecimiento de una hoja de ruta para el desarrollo de las actividades priorizadas para el 2025 acorde a los recursos

disponibles, de tal forma que se continúe con el desarrollo de lineamientos establecidos en el manual de la Política de Gobierno Digital establecidos por MinTIC. La Hoja de ruta se despliega a continuación tal y como se especificó en el documento denominado “2025-04-15_Plan_implementacion_gobierno_digital_fp.pdf”, versión 1 de abril del presente año (Ruta: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS_APOYO\GOBIERNO_DIGITAL\PLAN):

Tabla 1 Hoja de Ruta

Habilitador	Actividad	Fecha
Habilitador de Seguridad y Privacidad de la Información	Política de Seguridad y Privacidad de la Información	Agosto-2025
	Plan de Tratamiento de Riesgo	Noviembre-2025
	Plan de Seguridad y Privacidad de la Información	Noviembre-2025
	Diagnóstico de Seguridad y Privacidad de la Información	Octubre-2025

Fuente: Numeral 1.1.1. “2025-04-15_Plan_implementacion_gobierno_digital_fp.pdf”

En la planeación institucional registrada en el SGI, se encuentra el entregable correspondiente a la Política de Seguridad y Privacidad de la Información, como se muestra a continuación, con sus metas, fechas y responsables , entre otras.

Entregable	Responsable	Actividades	Fechas
Política de Seguridad y Privacidad de la Información en Función Pública implementada	CISO / Profesional de seguridad	Realizar jornadas de sensibilización en seguridad de la información para Función Pública.	Enero a diciembre 2025
		Actualizar la documentación asociada a la política de seguridad de la información	Enero a diciembre 2025

Para este entregable, se evidencia la debida gestión corroborada en el registro de avance de las actividades correspondientes, tal es el caso de las jornadas de sensibilización que se han venido efectuando hasta la fecha (Soportes ruta: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS_APOYO\SEGURIDAD\REPORTE_SGI).

Como complemento a lo anterior, la CISO/Especialista de seguridad mantiene un control de dichos entregables a través de un archivo Excel donde se tiene también el detalle de gestión sobre lo que está en la planeación institucional (El archivo se mantiene en la ruta mencionada en el párrafo anterior).

Para las otras 3 actividades del plan, no se tiene registro y control a través de la Planeación Institucional. Sin embargo, se mantiene un control mediante archivo de Excel, en el cual como se pudo observar para las actividades del plan de tratamiento de riesgos y del Plan estratégico de Seguridad y Privacidad de la Información, se tiene el debido registro y control de cada actividad. Dicho archivo contiene la siguiente información:

- Plan
- Actividades
- Meta
- Reporte
- Ruta de evidencia
- Nombre de archivo
- Fecha inicio
- Fecha fin

Se aclara por parte de la OTIC que estas actividades del plan se programaron para el segundo semestre, debido a que dependiendo del estado del soporte e infraestructura que se tenga en el segundo semestre, por cuanto la nube privada por ejemplo se vence contrato a finales de

junio y si se tiene el presupuesto, se daría continuidad a estas actividades, de lo contrario habría un riesgo por cuanto no se contaría con el soporte e infraestructura necesaria.

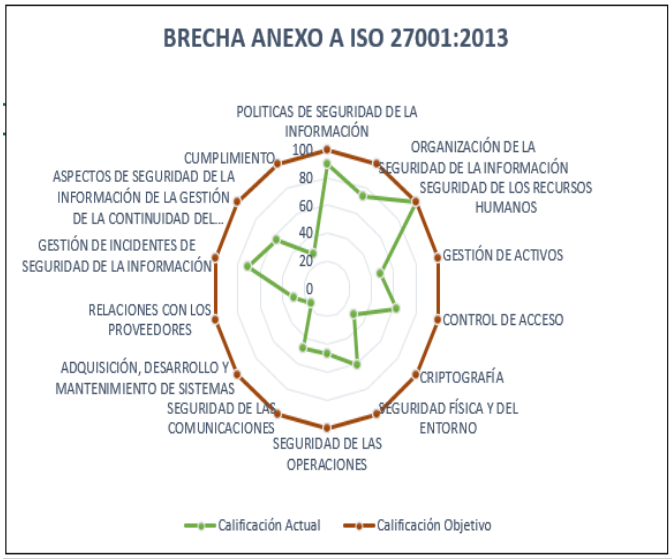
2. Resultados del seguimiento

2.1. Evaluación autodiagnóstico de seguridad de la información

Para gestionar este producto tipo, la OTIC ha venido aplicando el instrumento sugerido por MINTIC, el cual busca brindar un grado de avance exacto en la implementación de los lineamientos y controles exigidos por el Modelo de Seguridad y Privacidad de la Información de la Entidad.

Al respecto, se evidencia en la ruta: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS, los resultados de la aplicación del instrumento en el segundo semestre de la vigencia 2024 y los resultados parciales sobre los cuales se está adelantando el levantamiento de información en el primer semestre de la vigencia actual. A continuación, se muestran los resultados a nivel general para 2024:

Evaluación de Efectividad de controles		
DOMINIO	Calificación Actual	Calificación Objetivo
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	74	100
SEGURIDAD DE LOS RECURSOS HUMANOS	100	100
GESTIÓN DE ACTIVOS	48	100
CONTROL DE ACCESO	63	100
CRIPTOGRAFÍA	30	100
SEGURIDAD FÍSICA Y DEL ENTORNO	61	100
SEGURIDAD DE LAS OPERACIONES	47	100
SEGURIDAD DE LAS COMUNICACIONES	48	100
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	17	100
RELACIONES CON LOS PROVEEDORES	30	100
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	71	100
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	57	100
CUMPLIMIENTO	27,5	100



Fuente: Herramienta Autodiagnóstico MSPI segundo semestre 2024.

En este cuadro se observó para la vigencia 2024, un promedio de evaluación de los controles en 55/100. Actualmente, bajo el mismo instrumento, la OTIC, está empezando a efectuar la actualización respectiva a nivel de lo que a tecnología se requiere y a nivel administrativo se está analizando que dependencias deben intervenir en el suministro de la información requerida. Se espera obtener un reporte parcial para el primer semestre de este año.

2.2. Plan Estratégico de Seguridad de la Información (PESI)

Definición: Este plan es un documento de índole estratégico, que tiene como objetivo permitir a las entidades diseñar, planificar y ejecutar sus proyectos de seguridad de la información y así poder implementar el Modelo de Seguridad en un mediano/largo plazo, teniendo en cuenta insumos de diagnóstico que le permitan identificar su estado actual. El PESI permite cumplir con los requisitos establecidos en la estrategia de seguridad digital de la entidad, de acuerdo con lo determinado en el artículo 5 de la resolución 500 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”, el Decreto 612 de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”, el Manual de Gobierno Digital – MINTIC y el Modelo de Seguridad y Privacidad de la Información – MINTIC

Verificando inicialmente el acto administrativo de aprobación del PESI, se pudo evidenciar en el acta 001 – 2025 Comité Institucional de Gestión y Desempeño del Departamento Administrativo de la Función Pública, su debida presentación y aprobación. (Ruta: \\yaksa.dafp.local\10020OAP\2025\TRD\ACTA\ACTAS_COMITE_INSTITUCIONAL_GESTION_DESEMPENO)

Para esta vigencia se evidencia la publicación del plan mencionado, en la página web de Función Pública, como se muestra a continuación:

Plan Estratégico de Seguridad de la Información, Ciberseguridad y Privacidad de Datos

Versión 01 - Enero 2025

Objetivo: Mantener Implementado los lineamientos a nivel de seguridad de la información en la entidad, que esté protegida frente a las amenazas cibernéticas cumplir con los estándares y normas establecidas de seguridad y privacidad de la información.

No.	Actividades	Meta	Hitos	Fecha inicio	Fecha fin	Responsable
1	Documentar y actualizar la información de seguridad de la información alineada a los objetivos estratégicos de Función Pública.	Documentación actualizada del sistema de seguridad de la información.	1. Actualizar la política general de seguridad de la información enfocando: * Mejoramiento ciberseguridad * Protección de datos personales * Protección contra malware y ransomware	2025-02-01	2025-11-30	Oficina de Tecnologías de la Información y las Comunicaciones
2	Diseñar, aplicar y comunicar un programa de concientización en seguridad de la información para Función Pública	Programa de concientización en seguridad de la información para Función Pública aplicado	1. Definir la temática sobre seguridad de la información 2. Socializacion a través de capacitaciones	2025-02-01	33/11/2025	Oficina de Tecnologías de la Información y las Comunicaciones
3	Documentar y actualizar los procedimientos, políticas, estrategias de aseguramiento de datos de la Función Pública.	Procedimientos, políticas, estrategias de aseguramiento de datos de la Función Pública documentados y actualizados.	1. Actualizar la declaración de aplicabilidad 2.Actualizar los activos de información de Función Pública 3. Desarrollar los lineamientos de la política de control de acceso 4. Actualizar el procedimiento para la gestión de incidentes	2025-02-01	31/11/2025	Oficina de Tecnologías de la Información y las Comunicaciones
4	Aplicar la mejora continua al Sistema de Gestión de Seguridad de la Información	Mejora continua al Sistema de Gestión de Seguridad de la Información aplicada	1. Realizar análisis de los riesgos actuales para la seguridad de la información 2. Realizar el procedimiento actualizado de respuesta ante incidentes de seguridad y ciberataques	2025-02-01	2025-11-30	Oficina de Tecnologías de la Información y las Comunicaciones

Fuente: Menú de trasparencia, página WEB Función Pública: https://www1.funcionpublica.gov.co/planeacion-sectorial-institucional

Efectuando el seguimiento a cada una de las actividades se pudo evidenciar el control mencionado en el numeral 1 de este informe, mediante archivo de Excel, en el cual como se pudo observar para las actividades del Plan estratégico de Seguridad y Privacidad de la Información, se tiene el debido registro y control de cada actividad. En el momento se estan efectuado algunas revisiones y actualizaciones a las actividades del plan que se encuentran planificadas entre febrero y noviembre de la presente vigencia, como se muestra a continuación:

	B	C	D	E	F
	Plan	Actividades	Meta		REPORTE
1	Plan Estratégico de Seguridad de la Información, Ciberseguridad y Privacidad de Datos	Documentar y actualizar la información de seguridad de la información alineada a los objetivos estratégicos de Función Pública.	Documentación actualizada del sistema de seguridad de la información.	1. Actualizar la política general de seguridad de la información enfocando: * Mejoramiento ciberseguridad * Protección de datos personales * Protección contra malware y ransomware	Se esta actualizando mejoramiento de Ciberseguridad
2	Plan Estratégico de Seguridad de la Información, Ciberseguridad y Privacidad de Datos	Diseñar, aplicar y comunicar un programa de concientización en seguridad de la información para Función Pública	Programa de concientización en seguridad de la información para Función Pública aplicado	1. Definir la temática sobre seguridad de la información 2. Socializacion a través de capacitaciones	Primera capacitación, jueves 13 marzo fortinet
3	Plan Estratégico de Seguridad de la Información, Ciberseguridad y Privacidad de Datos	Documentar y actualizar los procedimientos, políticas, estrategias de aseguramiento de datos de la Función Pública.	Procedimientos, políticas, estrategias de aseguramiento de datos de la Función Pública documentados y actualizados.	1. Actualizar la declaración de aplicabilidad 2.Actualizar los activos de información de Función Pública 3. Desarrollar los lineamientos de la política de control de acceso 4. Actualizar el procedimiento para la gestión de incidentes	se esta revisando los activos de OTIC
4	Plan Estratégico de Seguridad de la Información, Ciberseguridad y Privacidad de Datos	Aplicar la mejora continua al Sistema de Gestión de Seguridad de la Información	Mejora continua al Sistema de Gestión de Seguridad de la Información aplicada	1. Realizar análisis de los riesgos actuales para la seguridad de la información 2. Realizar el procedimiento actualizado de respuesta ante incidentes de seguridad y ciberataques	

Fuente: Archivo de control planes seguridad de la información

Finalmente, acorde a lo que propone el modelo, no se evidencian todas las secciones mínimas recomendadas que todas las entidades deberían tener en cuenta para estructurar un PESI adecuadamente. Es decir, no se evidencia un documento estructurado con los siguientes elementos:

- ✓ **Alcance**: Definir cuáles serán los límites del PESI a establecerse, si cubrirá todos los procesos o inicialmente será bajo alcance de unos en específico.
- ✓ **Documentos de referencia**: Indicar que documentos constituyen la base para la construcción del PESI (pueden ser leyes, decretos, resoluciones, modelos o estándares).
- ✓ **Estado Actual de la entidad respecto al sistema de gestión de seguridad de la información**: En esta sección, se debe indicar y documentar de la forma más estratégica posible el estado actual de la entidad respecto a la implementación de los lineamientos de seguridad de la información requeridos por el MSPI. Esto permitirá a la entidad establecer la línea base de donde se encuentra la entidad y así proyectar hacía que punto desea llegar con base a las actividades definidas dentro del PESI.
- ✓ **Descripción de las estrategias específicas (ejes):** describir el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021.

- ✓ **Portafolio de proyectos / actividades:** Para cada estrategia específica, (LA ENTIDAD) debe definir los proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI).
- ✓ **Análisis presupuestal:** Con base a los proyectos definidos en el cronograma de actividades, se debe generar el presupuesto aproximado por cada vigencia según los proyectos establecidos y presentarlo a la Alta Dirección para las consideraciones y viabilidad pertinentes.

2.3. Política general de seguridad de la información

Objeto de la política: establecer los lineamientos definidos por la Alta Dirección de la Entidad para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información, las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas.

En el seguimiento, se pudo evidenciar la Política general de seguridad de la información publicada en el Sistema Integrado de Planeación y Gestión (SIPG), en el proceso de Tecnologías de la Información, versión 01 de octubre/2024. (Ruta: https://www1.funcionpublica.gov.co/documents/34645357/34703081/politica-general-seguridad-informacion-v1.pdf/415dc2a2-cc14-475c-b109-91aa5400c94b?t=1728482670613).

Verificando el grado de cumplimiento de la política actual publicada frente a lo requerido en la plantilla del producto tipo del habilitador, se encontró lo siguiente:

Elemento	Observación OCI
Objetivo	Cumple
Definiciones/Glosario	Cumple
Política general	Cumple con los componentes a tener en cuenta para su redacción. Numeral 1.

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.***
Alcance del sistema de gestión de seguridad de la información	Cumple.
Aplicabilidad	Cumple. Inmersa en el alcance de la política
Organización de la seguridad de la información (roles y responsabilidades)	***Cumple parcialmente***. Numeral 2.1 Roles y Responsabilidades. ***No se evidencia las responsabilidades del Comité de Gestión y Desempeño, 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).***"
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."***
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 las situaciones por las cuáles se harían revisiones o actualizaciones o que ameriten actualizar dicha política general."***

2.4. Manual de políticas de seguridad de la información

Definición: Este manual, tiene la finalidad de establecer los lineamientos relacionados con la seguridad de la información abordando temáticas específicas, como complemento a lo definido en la "Política General de Seguridad de la Información de la Entidad" con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos del Departamento Administrativo de la Función Pública.

Verificando este producto tipo, se evidencia que aún no ha sido implementado en la Entidad. Este producto acorde con la plantilla definida en el modelo de gobierno digital, debe contener la siguiente información:

- Objetivo
- Alcance
- Definiciones
- Políticas
    - ✓ Políticas de seguridad de los recursos humanos
    - ✓ Políticas de gestión de activos
    - ✓ Políticas de control de acceso lógico
    - ✓ Criptografía
    - ✓ Políticas de seguridad física y del entorno
    - ✓ Políticas de seguridad en las operaciones
    - ✓ Políticas de seguridad de las comunicaciones
    - ✓ Políticas de adquisición, desarrollo y mantenimiento de sistemas
    - ✓ Políticas de relaciones con los proveedores
    - ✓ Políticas de gestión de incidentes
    - ✓ Políticas de cumplimiento
    - ✓ Escritorio limpio:
    - ✓ Uso adecuado de internet
    - ✓ Uso adecuado de correo electrónico
    - ✓ Uso de usuarios y contraseñas
- Sensibilización y comunicación en seguridad de la información
- Sensibilización y comunicación
- Capacitaciones en seguridad
- Aprobación y revisión de las políticas
- Sanciones

Al respecto, es importante mencionar que el Departamento tiene un acercamiento a este manual, en las Políticas Específicas de Seguridad de la Información versión 8 del Proceso de Tecnologías de la Información. En las cuales se especifican varias de las políticas incluidas en el manual.

2.5. Inventario de activos de seguridad de la información

Definición: El inventario y clasificación de activos hace parte de las actividades más relevantes e importantes del Modelo de Seguridad y Privacidad de la Información y está compuesto por las siguientes fases:

- ***Identificación y Tipificación de los Activos de Información***: Corresponde a la etapa en donde la Dependencia como propietario y custodio de la información, identifica y clasifica la información producida, de acuerdo con: Activos de información puros, de Tecnologías de la Información, de Talento humano y Servicios.
- ***Clasificación de los activos de Información***: Corresponde a la etapa en donde la Dependencia propietario y custodio de la información califica los activos de información de acuerdo con lo establecido en el Artículo 6º de la Ley 1712 de 2014: Información Pública, Clasificada o Reservada.
- ***Revisión y Aprobación***: Corresponde a la Etapa en donde se valida la clasificación y valoración dada a los activos de información, para la presentación y aprobación por el Comité respectivo.
- ***Publicación de los Activos de Información***: Corresponde a la etapa de publicación de la información en la página web de la entidad, Link de transparencia y acceso a la Información Pública, Portal de Datos Abiertos del estado colombiano o el sitio que lo modifique o sustituya.

Efectuando la verificación, se evidenció que la OTIC a través del CISO/Especialista de Seguridad, está adelantando en la vigencia la actualización con el apoyo de la OAP, un formato de Inventario de activos de información de la entidad, para activos de TI, basándose en la

generada en la vigencia 2024 (Ruta evidencia: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS). Este formato contiene a nivel general la siguiente información:

- ✓ Identificación y categorización del activo
- ✓ Clasificación del activo
- ✓ Características del activo
- ✓ Ubicación del activo o lugar de consulta
- ✓ Ciclo de vida del activo
- ✓ Responsabilidades de acceso, custodia y soporte al activo de información
- ✓ Calificación del activo
- ✓ Valoración del activo

Si bien, este formato posee la mayoría de elementos de información establecidos por MInTIC en el manual de gobierno digital (Matriz de inventario y clasificación de activos de información), no posee la totalidad de la información requerida, la cual está sustentada por las Leyes 594 de 2000, 1712 DE 2014 y 1581 de 2012, Decretos 103 de 2015 y 1080 de 2015 y norma SO 27001.

Por otro lado, como cierta información contenida en el formato actual aplicado está clasificada como de carácter privada o sensible, la OTIC está filtrando que información se puede publicar en la página web de Función Pública. A su vez, debido a que la información allí contenida es de carácter institucional y no solo tecnológica, con el apoyo de la OAP se levantará la información de las respectivas dependencias en su registro y actualización.

Como complemento, se evidencia también el inventario de activos de TI, archivo “2024-07-04_Inventario_activos_dafp.xls” (Ruta: \\yaksa.dafp.local\10030OTIC\2024\DOCUMENTOS_APOYO\SEGURIDAD\NOTIFICACIONES_SOC), generado por la OTIC, donde se identifican los activos que componen los Routers, Firewalls, Sistemas operativos Windows y Unix y la Web.

2.6. Gestión de riesgos de seguridad de la información

Definición: Posterior a la definición de la matriz de activos de seguridad de la información, donde se identifican, califican y valoran los activos mencionados, se realiza un análisis de riesgos que los pueden afectar. En esta matriz se identificarán cuáles son las vulnerabilidades (o debilidades) en seguridad que puede tener cada activo o grupo de activos y también se identificarán cuáles son las posibles amenazas que podrían aprovechar nuestras debilidades para afectar la seguridad de los activos.

En la actualidad, la OTIC diseño una matriz de amenazas, acorde con los activos de información que pueden ser vulnerables a riesgos de seguridad de la información a nivel tecnológico, dicha matriz se encuentra en la ruta: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS_APOYO\SEGURIDAD\COMPROMISOS\PLAN_TRATAMIENTO_RIESGOS_SEGURIDAD, y posee la siguiente información:

- ✓ Activo Afectado
- ✓ Amenaza
- ✓ Probabilidad
- ✓ Impacto
- ✓ Nivel de Riesgo
- ✓ Acciones de Mitigación
- ✓ Acción
- ✓ Responsable
- ✓ Objetivo
- ✓ Ruta evidencia

La matriz mencionada se encuentra en proceso de actualización por parte de los especialistas al interior de la OTIC, acorde con el activo de información que corresponda. La gestión sobre esta matriz está registrada como entregable en la planeación institucional relacionado con la política

de gobierno digital, donde se trata una actividad sobre la gestión de la matriz de análisis de amenazas con el fin de identificar, evaluar y gestionar los riesgos.

Al respecto, si bien se tiene un matriz adelantada y con información significativa, y se controla su gestión a través del entregable en la planeación institucional, no se evidencia:

- ✓ La completitud de la información requerida en la plantilla del modelo de gobierno digital, como: 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, entre otras.
- ✓ La transversalidad con todos los procesos de la cadena de valor de Función Pública a nivel de los riesgos de seguridad de la información.

Conclusiones y recomendaciones

Generales

1. A nivel general se pudieron evidenciar adecuados controles de gestión en cuanto al desarrollo de las actividades de actualización y documentación del habilitador de seguridad y privacidad de la información.

2. A pesar de la existencia del control actual sobre las actividades propuestas a través de archivos Excel que mantiene la Oficial de seguridad, es importante que se incorporen las relacionadas en el PESI, así como las de los demás productos tipo del habilitador, en la planeación institucional centralizada en el SGI, esto permite una visión integral y coordinada de los compromisos estratégicos, su nivel de gestión y su trazabilidad en el tiempo.

3. Si bien para esta vigencia la administración del Departamento por temas coyunturales unifico los roles del Oficial de Seguridad de la Información con el Especialista de Seguridad de la

Información, se debe tener en cuenta que esta medida debe ser temporal, por lo cual recomendamos lo antes posible independizar los roles mencionados, por cuanto estos deben mantener independencia y autonomía, así como una debida segregación de funciones como lo especifica la norma ISO 27001 en su sección A.6. Organización de la Seguridad de la Información. En esencia, el rol del CISO requiere una comprensión profunda de los principios y estrategias de ciberseguridad, las regulaciones relevantes para el desarrollo y supervisión de políticas de seguridad, las prácticas de gestión de riesgos e independiente de las áreas de tecnología, mientras el Especialista de Seguridad de la Oficina de Tecnología trabaja en la implementación y gestión técnica de las medidas de seguridad, implementando y manteniendo la seguridad de la red, los sistemas y los datos, monitoreando la red y los sistemas en busca de actividades sospechosas, investigando y respondiendo a incidentes de seguridad, evaluando y mejorando las medidas de seguridad, entre otras.

4. Se debe mantener la consecución en la actualización, documentación, aprobación y divulgación de la totalidad de los productos tipo que conforman el habilitador, y prioritariamente a los elementos que conforman la estrategia de seguridad y privacidad de la información, 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. Se recuerda que el no acatar los aspectos normativos establecidos por MinTIC, podría acarrear sanciones administrativas, según lo establecido en la Ley 1341 de 2009 y otras leyes relacionadas. Estas sanciones pueden incluir multas, suspensión o revocación de licencias, o incluso investigaciones administrativas. El incumplimiento de las resoluciones del MinTIC puede afectar la operación de las empresas y organizaciones del sector de las Tecnologías de la Información y las Comunicaciones (TIC).

5. El Departamento Administrativo de la Función Pública debe propender por mantener el recurso financiero y humano necesario para continuar con la implementación de la Política de Gobierno Digital con el fin de avanzar en la modernización de su gestión, mejorar la eficiencia y fortalecer la relación Estado-ciudadano.

Especificas

1. Mantener la gestión en la actualización del instrumento de evaluación del modelo de seguridad y privacidad de la información, como lo ha venido haciendo la OTIC, con el fin de consolidar todas las calificaciones y el nivel de avance de la entidad en todos los aspectos del MSPI (Controles, PHVA y Madurez). Incluir, además, esta gestión en los entregables de la planeación institucional concentrada en el SGI.

2. Con respecto al PESI, acorde a lo establecido en el producto tipo, se debe generar un documento tal y como está especificado en la plantilla suministrada en modelo de gobierno digital, la cual contiene las secciones mínimas recomendadas que todas las entidades deberían tener en cuenta para estructurar un PESI adecuadamente. El detalle de lo mencionado se visualiza en el numeral 2.2 de este informe.

3. Con relación a la Política General de Seguridad de la Información, se recomienda para la próxima actualización, tener en cuenta los numerales que deben ser complementados o incluidos acorde con la estructura del documento establecida en los lineamientos de la plantilla dada por el modelo. Ver el detalle en el numeral 2.3 de este informe.

4. Para el manual de políticas de seguridad de la información, se recomienda analizar los puntos que debe contener acorde al modelo (Ver numeral 2.4 de este informe) y los relacionados en las Políticas Específicas de Seguridad de la Información versión 8 del Proceso de Tecnologías de la Información, publicadas en el SIPG. Esto con el fin de unificar la información y poder implementar dicho manual.

5. Se debe analizar la posibilidad de complementar 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, la cual debe contener el universo completo de los activos de información de cada proceso de la

cadena de valor, por lo cual con el apoyo de la OAP y la OTIC cada proceso debe involucrarse en su diligenciamiento a pesar que este en cabeza del oficial de seguridad de la información.

Se recuerda que la matriz es un instrumento desarrollado por MINTIC que busca brindar un esquema completo para la estructuración del Inventario de Activos de Información de cada Entidad, donde puedan realizar una identificación, clasificación y valoración de cada uno, para así identificar cuáles son los activos más críticos para **CADA PROCESO DE LA ENTIDAD**. El instrumento ofrece una estructura que permite dar cumplimiento a otras normativas como protección de datos personales y lineamientos del archivo general de la nación, sin embargo, tener en cuenta que la **Entidad si desea puede ajustar el formato manejando únicamente lo relacionado con Seguridad Digital**.

6. Con respecto a la Gestión de riesgos de seguridad de la información, se recomienda complementar la matriz de amenazas actual con la información requerida en la plantilla del producto tipo, involucrando todos los activos de información respectivos a nivel Entidad, por lo cual una vez los procesos hayan realizado la identificación, clasificación y valoración de los activos, deberán realizar un análisis de los posibles riesgos que los puedan afectar. El modelo de Gobierno Digital recomienda que se podría construir una matriz de activos y una de riesgos por cada proceso de la entidad o una unificada.

   Complementando lo anterior, se recuerda que la gestión de riesgos de seguridad se realiza siguiendo lo establecido en la Guía de Administración de Riesgos del Departamento Administrativo de la Función Pública, y que los riesgos identificados deben estar contenidos en la sábana de riesgos institucionales de la entidad que se mantiene en el SGI.

Jorge Iván De Castro Barón

Firmado digitalmente por Jorge Iván De Castro Barón
Fecha: 2025.05.30 10:00:02 -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