Función Pública

INFORME DE SEGUIMIENTO A LA IMPLEMETACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - MSPI

Evaluación Independiente

OFICINA CONTROL INTERNO

Versión 01

Junio de 2026

Objetivo

Verificar y evaluar por parte de la Oficina de Control Interno el estado actual de gestión sobre el Modelo de seguridad y Privacidad de Información - MSPI, de acuerdo con lo establecido en la Resolución 0500 de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). La cual tiene por objeto "establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital".

Es importante mencionar que las observaciones registradas en el presente informe de seguimiento coadyuvan a fortalecer el ambiente de control de la seguridad de la información al interior de la entidad.

Alcance

Se verificará el estado actual de cumplimiento de las fases que componen el MSPI, establecidas en el documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información MinTIC, versión 5 del 21 de abril de 2025, las cuales se relacionan a continuación, además de las recomendaciones resultado del seguimiento efectuado por la OCI en la vigencia 2026 inmersas en cada fase:

- ✓ Diagnóstico: Permite a las entidades establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un "Diagnóstico" utilizando el "instrumento de evaluación MSPI" con el que se identifica de forma específica los controles implementados, se mide el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información y se obtienen insumos fundamentales para la fase de planificación.

- ✓ Fase 1 Planificación : Permite que la entidad proceda con la elaboración del Plan de Seguridad y Privacidad de la Información, con el objetivo de que la entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI.

- ✓ Fase 2 Operación: Relativa a la implementación de los procesos de seguridad de la información: gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles. Fomentando la cultura de seguridad y definición de criterios

de cumplimiento y mecanismos de control para procesos y servicios externos relevantes, asegurando su alineación con el SGSI.

- ✓ Fase 3 Evaluación de desempeño: se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 “Protección de datos personales” y Ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”.

- ✓ Fase 4 Mejoramiento Continuo: Se consolidan los resultados obtenidos de la fase de evaluación de desempeño y se diseña el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

1. Resultados del seguimiento

1.1. Diagnóstico

Lineamiento: “Identificar a través de la herramienta de autodiagnóstico (instrumento de evaluación MSPI) el estado actual de la entidad respecto a la Seguridad y Privacidad de la Información”.

Propósito: “Identificar el nivel de madurez de Seguridad y Privacidad de la información en el que se encuentra la entidad, como punto de partida para la implementación del MSPI”.

Estado Actual:

A la fecha de acuerdo a los formatos remitidos por MinTIC bajo la norma ISO 27000:2023 se aplicó la herramienta, evidenciándose el diagnóstico completo.

En la ruta \\yaksa.dafp.local\10030OTIC\2026\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\Plan Estratégico de Seguridad de la Información, se evidencia el documento de autodiagnóstico diligenciado con fecha 30 de marzo de 2026 (“2026-03-30_Diagnostico_seguridad_privacidad_informacion.docx (V01)”), Donde se expone como conclusión general que “La entidad tiene un gobierno de seguridad "Gestionado", pero tecnológicamente vulnerable. La prioridad debe ser automatizar controles técnicos y fortalecer la capacidad de prevención para equilibrar la excelente capacidad de respuesta detectada.

Se deben realizar mesas de trabajo con cada una de las áreas involucradas (Recursos Humanos , Administrativa y toda la OTIC con sus grupos internos) para verificar y a aumentar el porcentaje para seguir en la otra fase.”

Únicamente se encuentra pendiente, la socialización con las áreas involucradas y la ejecución de mesas de trabajo para incrementar los porcentajes y avanzar a la siguiente fase.

Recomendación:

Se debe propender por efectuar la debida socialización de los resultados del autodiagnóstico a las dependencias y/o profesionales involucrados en el desarrollo de estrategias que coadyuven a fortalecer la gestión en Seguridad de la Información al interior de la entidad, así como la ejecución de las mesas de trabajo respectivas.

1.2. Fase 1 Planificación

1.2.1. Definición del alcance del MSPI

Lineamiento: “Determinar con claridad los límites, el alcance y la aplicabilidad del MSPI en el marco del modelo de operación por procesos de la entidad. Esta definición debe especificar a qué procesos, recursos humanos, financieros, técnicos y tecnológicos se aplicará la implementación del modelo. Se recomienda iniciar con los procesos misionales, dado su impacto estratégico y su nivel de exposición a riesgos de seguridad y privacidad de la información”.

Propósito: “Identificar qué activos de información, software, hardware, roles, sistemas de información, áreas seguras (generada o utilizada en los procesos de la entidad) será protegida mediante la adopción del MSPI.”

Estado Actual: El alcance fue definido y se encuentra formalmente establecido en el Plan Estratégico de Seguridad de la Información – PESI 2026 (2026-01-12_Plan_estrategico_seguridad_Informacion_pesi_dafp.docx). Este alcance se orienta a la “Aplicación transversal a todos los procesos, sistemas de información, áreas funcionales y dependencias de la entidad', incluyendo datos personales, institucionales y de carácter público, en concordancia con la política institucional de seguridad y los marcos normativos vigentes”. Ver sección 2 “Alcance”.

El PESI mencionado se evidenció en la ruta : \\yaksa.dafp.local\10030OTIC\2026\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\Plan Estratégico de Seguridad de la Información.

Por otro lado, en el Plan de Acción Anual OTIC 2026 (PAA) (2026-01-13__Matriz_plan_accion_anual_2026_otic_diligenciado_otic.xlsx - Entregable E3 (PEI-088)), se evidencia registro del entregable PEI-088 'Políticas de Seguridad y Privacidad de la información en Función Pública implementada' con actividades de actualización documental, matriz de activos y sensibilización, formalizando el alcance operativo en el SGI institucional.

Al respecto, se encuentra pendiente la aprobación formal del alcance en el CIGD (Comité Institucional de Gestión y desempeño).

Recomendación:

El PESI generado para la vigencia 2026 donde se involucra el alcance del MSPI, debe quedar registrado en el Sistema Integrado de Planeación y Gestión – SIGP, y una vez aprobado por el CIGD ser publicado en la página Web de FP en la sección de transparencia/Planeación y seguimiento sectorial e institucional (Contar para ello con el apoyo y aprobación de la OAP). A su vez, el alcance inmerso en el PESI debe ser presentado y aprobado en el CIGD.

1.2.2. Liderazgo

1.2.2.1. Liderazgo y compromiso

Lineamiento: “Las entidades deben asignar, mediante acto administrativo, al Comité Institucional de Gestión y Desempeño - CIGD (o su equivalente) las funciones relacionadas con la seguridad y privacidad de la información, asegurando la adopción, implementación y mejora continua del MSPI. En este comité debe incluirse como miembro permanente al responsable de seguridad de la información, con el fin de garantizar su implementación efectiva y el cumplimiento de acciones claves del MSPI”

Propósito: “Garantizar el liderazgo y el compromiso del CIGD o quien haga sus veces para conseguir los objetivos definidos para la implementación del MSPI”.

Estado Actual:

Se observa la resolución 1236 de 2017 del DAFP por la cual se crea y conforma el CIGD, evidenciándose lo siguiente con respecto al lineamiento:

✓ En el Artículo 2. *Conformación del Comité Institucional de Gestión y Desempeño*, especifica que el Comité estará conformado por:

1. El Subdirector de Función Pública, quien lo presidirá
2. Un representante de la Dirección General
3. El Secretario General
4. El Director de Gestión del Conocimiento
5. El Director Jurídico
6. El Director de Empleo Público
7. El Director de Desarrollo Organizacional
8. El Director de Gestión y Desempeño Institucional
9. El Director de Participación, Transparencia y Servicio al Ciudadano
10. El Jefe de la Oficina Asesora de Planeación, quien actuará como Secretario del Comité
11. El Jefe de la Oficina Asesora de Comunicaciones
12. El Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones
13. El Coordinador del Grupo de Gestión Contractual
14. El Coordinador del Grupo de Gestión Humana
15. El Coordinador del Grupo de Gestión Financiera
16. El Coordinador del Grupo de Gestión Administrativa
17. El Coordinador del Grupo de Gestión Documental
18. El Coordinador del Grupo de Servicio al Ciudadano Institucional

En este artículo aún no se establece la inclusión como miembro permanente al responsable de seguridad de la información, con el fin de garantizar la implementación efectiva y el cumplimiento de acciones claves del MSPI, tal como se había evidenciado la vigencia pasada.

No obstante, se tienen algunos elementos que coadyuvan al propósito mencionado, así:

- En el PESI 2026 se definen cinco ejes estratégicos incluyendo 'Liderazgo de Seguridad de la Información', con productos esperados relacionados con: El desarrollo, implementación y formalización de la política de seguridad de la información, y la definición de los roles y responsabilidades en seguridad de la Información formalizados dentro de las políticas de seguridad.
- El PAA 2026 (entregable E1-A2) registra la implementación de la primera fase del MSPI y presupuesto asignado.
- El Decálogo de Seguridad (marzo 2026) referencia explícitamente al 'Oficial de Seguridad de la Información' como responsable del aseguramiento institucional, con

canales de reporte definidos. (Archivo: 2026-03-20_Decatalogo_seguridad.pptx - Slide 4 Oficial de Seguridad).

- El PAA 2026 también confirma continuidad del proyecto de inversión 20230000000140 (C_TI-3-2) para mejorar la estrategia de seguridad 2024-2027. (Archivo: 2025-11-27_Matriz_plan_accion_anual_2026_otic.xlsx - E1-A2 (MSPI) y C_TI-3-2).
- En el artículo 3 *funciones del Comité Institucional de Gestión y Desempeño*, en el numeral 6 se especifica la función de "Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información".

Pendiente:

• Actualización de la Resolución 1236 de 2017 (CIGD (Comité Institucional de Gestión y desempeño)) para incluir al Oficial de Seguridad como miembro permanente.

• Aprobación del PESI v02 y la Política General de Seguridad de la Información v03 en el CIGD.

Recomendación:

Como se recomendó en el informe de seguimiento de la vigencia pasada, se debe actualizar la Resolución 1236 de 2017 de creación del CIGD, incluyendo en el artículo 2 como miembro al Oficial de SI, para que por medio de él se garantice la implementación efectiva del MSPI y las acciones clave como:

- Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Garantizar la adopción de los requisitos del MSPI en los procesos de la entidad.
- Comunicar en la entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo, entre otros) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI (al menos dos veces por año y en las que el Nominador deberá estar presente).

1.2.2.2. Política de seguridad y privacidad de la información

Lineamiento: "Se debe establecer en la política de seguridad y privacidad de la información los lineamientos y compromisos que se adoptaran para asegurar la confidencialidad, integridad y disponibilidad de la información."

Propósito: “La política establece la base respecto al comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad. Orientar y apoyar por parte de la alta dirección de la entidad a través del comité de gestión institucional, la gestión de la seguridad de la información de acuerdo con la misión de la entidad, normatividad y reglamentación pertinente”

Estado Actual:

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 la mayoría de los elementos pendientes que se habían evidenciado en el seguimiento de la vigencia pasada como se muestra a continuación:

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 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*** .	Ya se incluyeron las responsabilidades del Comité de 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***	Se incluyó al respecto el proceder de la entidad frente al incumplimiento de las políticas. (Numeral 12)

	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.”***	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 las situaciones por las cuáles se harían revisiones o actualizaciones .***	Aún no se ha incluido esta información en la PSGI. *Se recomienda con el apoyo de la OAP, incluir un numeral en la Política relacionada con la definición mencionada en la recomendación inicial.*

Fuente: Seguimiento Implementación Gobierno digital (Abril / 2026)

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.

Recomendación:

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.

1.2.2.3. Roles y Responsabilidades

Lineamiento:

“Articular roles y responsabilidades con las áreas de la entidad para la adopción del MSPI, asegurando el monitoreo, reporte y aprobación ante el comité institucional. Los líderes de proceso deberán gestionar los riesgos de seguridad y privacidad de la información. Designar un responsable del MSPI con un equipo de apoyo, dependiente de un área estratégica distinta a la de Tecnología. Si no existe el cargo, deberá delegarse por acto administrativo e integrarse con voz y voto al comité de gestión institucional de gestión y desempeño y con voz al comité de control interno. Si no hay personal de planta, varias entidades podrán compartir un responsable de seguridad mediante contrato de servicios, justificando la falta de recursos, conforme al artículo 5 de la Resolución 500 sobre Estrategia de Seguridad Digital”.

Propósito:

”Es fundamental que los funcionarios y contratistas conozcan sus responsabilidades, comprendan el impacto de sus acciones en la seguridad de la información y entiendan cómo contribuyen a la implementación efectiva del MSPI.”

Estado Actual:

En la actualidad, no se tiene una clara definición de roles y responsabilidades para adoptar el MSPI. Como se había observado el año pasado, el DAFP por temas coyunturales había unificado dichos roles en un solo profesional desde la vigencia 2024, 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.

Recomendación:

La Entidad debe:

- ✓ Independizar los roles del CISO y el Especialista de SI, 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. y el Manual de Políticas de Seguridad de la Información del DAFP.
- ✓ Una vez se tenga esta segregación de funciones. designar como mínimo en el corto plazo al CISO o al recurso humano que estimen conveniente como responsable del MSPI, el cual tenga la facultad de monitorear, reportar y participar en la aprobación de los componentes esenciales que conforman el modelo ante el CIGD.

1.2.3. Planeación

1.2.3.1. Identificación de activos de información e infraestructura critica cibernética

Lineamiento:

"Las entidades deben definir y aplicar un proceso de identificación y clasificación de los activos de información, que permita:

- ✓ Identificar los activos de información que agregan valor al proceso y requieren protección, según el alcance y los procesos cubiertos por el MSPI.
- ✓ Clasificar los activos de información de acuerdo con los tres principios de seguridad de la información: Integridad, confidencialidad y disponibilidad
- ✓ Actualizar el inventario y la clasificación de los activos por los propietarios y custodios de los activos de forma periódica o toda vez que exista un cambio en el proceso.
- ✓ Realizar la identificación y el inventario de infraestructura crítica y servicios esenciales de la entidad."

Propósito:

"Estructurar una metodología que permita identificar y clasificar los activos de información."

Estado Actual:

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Actualmente, el inventario de activos V03 (abril 2026) cubre los activos de la OTIC con clasificación de acuerdo a la Ley 1712/2014, la Ley 1581/2012, la valoración CID (Confidencialidad, Integridad y Disponibilidad) y criticidad interna/externa. (Archivo: 2026-04-15_Formato_inventario_activos.xlsx (V03 - actualización 2025-05-20))

De otro lado, el PESI V02 incluye en su portafolio (eje Gestión de Riesgos) el proyecto de 'Identificación y clasificación de activos' con la Matriz de Activos como producto esperado. Y el PAA 2026 registra la actividad E3-A2 'Actualización de la matriz de activos de información' con responsable y periodicidad semestral.

Pendiente: Generar y formalizar el procedimiento metodológico de actualización periódica del inventario con responsables y tiempos definidos.

Recomendaciones:

- Acorde con el lineamiento, solo faltaría la generación de un procedimiento detallado que contenga los insumos, la hoja de ruta para actualizar el inventario de activos de información, responsables y los tiempos estimados de revisión y actualización. Esto, propendiendo por mantener la continuidad y oportunidad de la gestión en el tiempo.

- Actualizar los responsables de las actividades programadas en la matriz del PAA (2026-01-13__Matriz_plan_accion_anual_2026_otic_diligenciado_otic.xlsx), debido a que figura una Funcionaria que ya no labora en la entidad.

1.2.3.2. Valoración de los riesgos de seguridad de la información

Lineamiento: “Las entidades deben definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita entre otros:

- ✓ Identificar los riesgos que causen la pérdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la entidad dentro del alcance del MSPI.
- ✓ Identificar los propietarios de los riesgos.
- ✓ Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia.
- ✓ Determinar el apetito de riesgos definido por la entidad.
- ✓ Establecer criterios de aceptación de los riesgos.
- ✓ Valorar los riesgos que afecten la confidencialidad, integridad y disponibilidad de la información dentro del alcance del MSPI.
- ✓ Priorización de los riesgos analizados para su tratamiento.

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

- ✓ Se debe asegurar que las valoraciones repetidas de los riesgos de seguridad y privacidad de la información produzcan resultados consistentes, válidos y comparables.
- ✓ Se deben considerar los nuevos riesgos asociados a los dominios incluidos en la ISO/IEC 27001:2022, tales como amenazas avanzadas, entornos de nube, y riesgos en la cadena de suministro digital."

Estado Actual:

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.dafp.local\10030OTIC\2026\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\Plan de Tratamiento de Riesgos de Seguridad). En esta plantilla (2026-05-01_Matriz_riesgos_seguridad.xlsx (versión mayo 2026)), 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.

En la matriz mencionada se evidencian los riesgos identificados en la sábana de riesgos del SGI para el proceso de "Tecnologías de la Información" y uno del proceso "Diseño y desarrollo de las políticas para la gobernabilidad y la gobernanza de las administraciones públicas". No obstante, los siguientes riesgos de "seguridad digital" registrados en la sábana de riesgos del SGI, y con estado "Aprobado" no han sido gestionados a través del instrumento de análisis:

# Riesgo	Proceso	Descripción del Riesgo
52	Comunicación estratégica	Posibilidad de afectación reputacional por quejas de grupos de valor debido a pérdida de integridad de la información cuando personal no autorizado realiza publicaciones en las redes o modifica contenido
60	Gestión Administrativa	Posibilidad de afectación reputacional por sanción del ente de control (superintendencia de industria y comercio), debido a la pérdida de confidencialidad de los datos personales del registro de visitantes y grabaciones de video del circuito cerrado de televisión
71	Fortalecimiento y desarrollo de la gestión y desempeño de las administraciones publicas	Posibilidad de afectación reputacional y económica por pérdida de información en los aplicativos SUIT y SIRCAP debido a la inadecuada gestión de los permisos de acceso y fallas en el soporte técnico del aplicativo
72	Diseño y desarrollo de las políticas para la gobernabilidad y la gobernanza de las	Posibilidad de afectación reputacional por divulgación no autorizada de información reservada o clasificada almacenada en los repositorios institucionales o sistemas de información debido a la inadecuada gestión de los permisos de acceso. - DEP

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

	administraciones publicas	
95	Fortalecimiento y desarrollo de la gestión y desempeño de las administraciones públicas	Posibilidad de afectación reputacional por divulgación no autorizada de información reservada o clasificada almacenada en los repositorios institucionales o sistemas de información debido a la inadecuada gestión de los permisos de acceso. DGC
98	Diseño y desarrollo de las políticas para la gobernabilidad y la gobernanza de las administraciones publicas	Posibilidad de afectación reputacional por divulgación no autorizada de información reservada o clasificada almacenada en los repositorios institucionales o sistemas de información debido a inadecuada gestión de los permisos de acceso
99	Fortalecimiento y desarrollo de la gestión y desempeño de las administraciones publicas	Posibilidad de afectación reputacional por quejas de los grupos de valor debido a la no disponibilidad de la información gestionada por el proceso, en el archivo en físico o digital administrado y almacenado por el grupo de apoyo a la gestión meritocrática.
112	Control Disciplinario Interno	Posibilidad de afectación reputacional por violación de la reserva, disponibilidad, confidencialidad o integridad en la información, debido a la ausencia o débil parametrización de permisos de acceso en los repositorios documentales o de la documentación generada por el Proceso.

Fuente: Reporte “Informe Gestión Riesgos” SGI (15-06-2026)

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 el análisis e 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.

De otra parte:

- Se verificó la Guía metodológica institucional para la gestión integral del riesgo de la entidad /Versión 7 – septiembre 2025) publicada en la página web de función pública y se pudo evidenciar el capítulo V, donde el Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC), como líder de la política de gobierno digital, define los lineamientos y metodologías aplicables para la gestión de riesgos de seguridad de la información, lo que permite incrementar la confianza de las partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en las entidades. En este capítulo se desarrollan los pasos necesarios para la identificación y tratamiento de los riesgos asociados a la Disponibilidad, Integridad y Confidencialidad de los activos de información que permiten cumplir con la misión y alcanzar la Visión en las diferentes entidades.

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

- El PESI V02 incluye el proyecto “Identificar, valorar y clasificar los riesgos asociados a los activos de información” con la Matriz de Riesgos de Seguridad Digital como producto esperado, articulando así la valoración con la estrategia institucional.

Recomendación:

Como se había recomendado en el seguimiento de la vigencia 2025, se debe incluir en la matriz de riesgos de SI el universo de riesgos de seguridad digital mencionados en este numeral y que se encuentran vigentes en estado aprobado en el mapa de riesgos institucional, independiente del proceso a que correspondan; así mismo, a futuro considerar los nuevos riesgos asociados a posibles amenazas sobre cada uno de los activos de información identificados y a los dominios incluidos en la ISO/IEC 27001:2022, tales como amenazas avanzadas, entornos de nube, y riesgos en la cadena de suministro digital, siempre y cuando apliquen al MSPI de la entidad.

1.2.3.3. Plan de tratamiento de los riesgos de seguridad de la información

Lineamiento: “Las entidades deben definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita:

- ✓ Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos.
- ✓ Elaborar una declaración de aplicabilidad que contenga: los controles adoptados por la entidad, su estado de implementación y la justificación de posible exclusión de acuerdo con los riesgos identificados y las capacidades técnicas y humanas con las que cuenta.
- ✓ Definir un plan de tratamiento de riesgos que contenga, fechas, acciones de tratamientos de riesgos a tratar y responsables con el objetivo de realizar trazabilidad.
- ✓ Los dueños de los riesgos que deben ser los dueños de los procesos afectados por estos riesgos, o las personas designadas por ellos. Deben realizar la aprobación formal del plan de tratamiento de riesgos y la aprobación debe llevarse a la revisión por dirección en el Comité Institucional y de Desempeño, o quien haga sus veces.”

Propósito:” Estructurar una metodología que permita definir las acciones que debe seguir la entidad para poder gestionar los riesgos de seguridad y privacidad de la información”.

Estado Actual:

Al interior de la entidad se evidencia el “Plan de Tratamiento de Riesgos de Seguridad – PTRS 2026 Versión 1 - enero 2026”, el cual tiene por objetivo: “Identificar, evaluar y mitigar

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

los riesgos asociados a la seguridad de la información y a los activos de la entidad, garantizando la confidencialidad, integridad y disponibilidad de la información, de conformidad con la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del MinTIC, con el fin de minimizar el impacto de eventos adversos en la operación institucional.”; en dicho plan se tienen especificadas las siguientes actividades:

Actividades	Meta	Hitos
Documentar y actualizar la información de seguridad y privacidad de la información, alineada con los objetivos estratégicos de Función Pública, en cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital y el Sistema de Gestión Institucional (SGI)	1. Realizar seguimiento a la implementación de los controles del MSPI	1. Análisis de la normativa vigente, lineamientos MinTIC y requisitos del MSPI aplicables. *Aprobación formal por comité de Gestión 2. Implementación de la primera fase del Modelo de Seguridad y Privacidad de la Información - MSPI
Diseñar, implementar y comunicar un programa de concientización en seguridad de la información para Función Pública.	Ejecutar el Plan de Concienciación en Seguridad y Privacidad, fortaleciendo la cultura de seguridad, promover el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) y mitigar riesgos asociados al manejo de la información institucional	1. Identificación de necesidades de concientización 2. Definir las temáticas prioritarias a abordar. 3.Socializar los lineamientos y buenas prácticas en seguridad de la información a través de jornadas de capacitación.
Actualizar la Matriz de Activos de Información institucional, garantizando la identificación, clasificación y valoración adecuada de los activos, conforme a los lineamientos del MSPI	Matriz de Activos de Información actualizada, validada, que refleje el estado real de los activos de información de la entidad, su clasificación, responsables y controles asociados, como insumo para la gestión de riesgos de seguridad de la información	1. Identificación de activos de información 2. Clasificación de los activos de información según criterios de(confidencialidad, integridad y disponibilidad.) 3. Definición de propietarios y custodios de cada activo de información. 4. Análisis del impacto y criticidad de los activos frente a la operación institucional. 5. Relación de controles existentes o requeridos para la protección de los activos. 6. Actualización de la matriz

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Implementar y fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, conforme a los lineamientos del MSPI	Revisar la Política y el Manual de Políticas de Seguridad y Privacidad de la Información y actualizar en caso de ser necesario.	Revisar y actualizar, cuando aplique, la Política y el Manual de Políticas de Seguridad y Privacidad de la Información, garantizando su alineación con el MSPI y la normatividad vigente.
Documentar y mantener actualizados los procedimientos, políticas y estrategias de aseguramiento de datos de la Función Pública, asegurando su conformidad con el Modelo de Seguridad y Privacidad de la Información (MSPI) y normatividad vigente	Procedimientos, políticas y estrategias de aseguramiento de datos de la Función Pública elaborados, documentados, actualizados y validados técnicamente, que soportan la implementación y operación del Sistema de Gestión de Seguridad de la Información	1.Desarrollar y formalizar los lineamientos de la Política de Control de Acceso 2.Actualizar el procedimiento de gestión de incidentes de seguridad 3.Documentar y mantener actualizado el catálogo de servicios de seguridad de la información
Implementar acciones de mejora continua en el Sistema de Gestión de Seguridad de la Información, basadas en el análisis de resultados, hallazgos de auditorías, incidentes presentados y cambios en el contexto organizacional.	Acciones de mejora continua implementadas en el Sistema de Gestión de Seguridad de la Información, con seguimiento a su eficacia y resultados documentados.	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

Fuente: Plan de Tratamiento de Riesgos de Seguridad 2026 Versión 1 - enero 2026

El plan mencionado se evidencia en la ruta: \\yaksa.dafp.local\10030OTIC\2026\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\PLAN_TRATAMIENTO_RIESGOS_SEGURIDAD.

Por otro lado, mediante la metodología aplicada en el SGI para la definición, registro, calificación, seguimiento y tratamiento de riesgos, se está supliendo este lineamiento, lo cual se puede evidenciar en los informes de gestión de riesgos generados en el SGI, donde se puede evidenciar por riesgo la siguiente información:

- ✓ Código
- ✓ Materializado
- ✓ Proceso
- ✓ Dependencia
- ✓ Estado
- ✓ Riesgo
- ✓ Tipo

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

- ✓ Clasificación
- ✓ Impacto
- ✓ Causa inmediata
- ✓ Causa raíz
- ✓ Activos
- ✓ Probabilidad inherente
- ✓ Impacto inherente
- ✓ Zona inherente
- ✓ Probabilidad residual
- ✓ Impacto residual
- ✓ Zona residual
- ✓ Tratamiento
- ✓ Periodicidad
- ✓ No. Controles
- ✓ Controles
- ✓ Responsables controles
- ✓ No. Acciones
- ✓ Acciones
- ✓ Responsables acciones
- ✓ Fecha materialización
- ✓ Acontecimiento materialización

En este control se evidencia el cumplimiento al lineamiento en cuanto a la trazabilidad de la gestión enfocando la responsabilidad, cumplimiento (fechas) y acciones de gestión que los dueños de los riesgos deben ejercer, además que los mismos son los dueños de cada proceso afectado, como lo determina el lineamiento, y son los que efectúan su tratamiento.

Pendientes:

- No se evidencia el acta formal del CIGD aprobando el PTRS 2026.
- El enlace del PTRS 2026 inmerso en el link del menú de transparencia https://www1.funcionpublica.gov.co/planeacion-sectorial-institucional de la página web de FP, dirige al PESI 2026.

Recomendación:

- Gestionar la aprobación del PTRS 2026 por parte el CIDG, la cual debe soportarse en el acta respectiva del Comité.
- Ajustar el enlace en la sección de transparencia de la página Web de FP, con el correspondiente al PTRS 2026.

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

1.2.4. Soporte

1.2.4.1. Recursos

Lineamiento: “Las entidades deben asegurar los recursos financieros, humanos y técnicos necesarios para adoptar, implementar y mantener el MSPI como un proceso transversal conforme al alcance definido.”

Propósito: “Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del MSPI.”

Estado Actual:

Recurso humano: Se tiene tan solo un recurso humano gestionando algunos elementos del MSPI, el cual como se ha venido exponiendo comparte el rol de CISO y Especialista de SI.

Recurso Financiero: en los proyectos de inversión de la presente vigencia, publicados en la página Web de la entidad (https://www1.funcionpublica.gov.co/proyectos-de-inversion), se encuentra aún el denominado “20230000000140 – Mejoramiento de las tecnologías de la información y las comunicaciones a nivel institucional para dar cumplimiento a las políticas de gobierno digital y transformación digital Bogotá”, en el que se puede observar dentro de la FICHA ACTUALIZADA DEL PROYECTO PLATAFORMA INTEGRADA DE INVERSIÓN PÚBLICA, PIIP, en la cadena de valor, el producto “Servicio de actualización del Sistema de Gestión - Dar continuidad a la implementación de la política de Gobierno Digital”, y en él la actividad “Mejorar la implementación de la estrategia de seguridad y privacidad de la información acorde a la normatividad vigente” con un costo total: $2.482.114.094,00, con su correspondiente distribución por vigencia como se muestra en la siguiente imagen:

FICHA ACTUALIZADA DEL PROYECTO PLATAFORMA INTEGRADA DE INVERSIÓN PÚBLICA, PIIP

ID MGA:594141	CÓDIGO BPIN: 202300000000140	FECHA REPORTE: 08-01-2025 09:10:07
NOMBRE DEL PROYECTO: Mejoramiento de las tecnologías de la información y las comunicaciones a nivel institucional para dar cumplimiento a las políticas de Gobierno Digital y transformación Digital Bogotá		

CADENA DE VALOR			
Costo total: 4.910.409.279,00		2027	98.073.077,00
Servicio de actualización del Sistema de Gestión - Dar continuidad a la implementación de la política de Gobierno Digital **Unidad de medida de producto:** Número de sistemas **Etapa:** Inversión **Costo total:** 4.910.409.279,00	**Actividad:** Mejorar la implementación de la estrategia de seguridad y privacidad de la información acorde a la normatividad vigente **Costo total:** 2.482.114.094,00	2024	0,00
		2025	595.052.500,00
		2026	835.835.625,00
		2027	1.051.225.969,00

Fuente: Ficha actualizada del proyecto plataforma integrada de inversión pública, PIIP, 08-01-2025

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Con respecto a la actualización del PETI de acuerdo con los recursos necesarios para realizar la gestión adecuada de los riesgos de seguridad de la información identificados y el plan de seguridad y privacidad de la información, como lo especifica una de las salidas del lineamiento, se evidenció en el Documento Técnico del Plan Estratégico de Tecnología de la Información – PETI 2026 (Versión 1 – enero 2026) que dentro de los motivadores estratégicos se tiene en la estrategia institucional al plan de seguridad y privacidad de la información y en la matriz DOFA dentro de la situación actual se presenta como fortaleza la política de seguridad y privacidad de la información y los planes de tratamiento de riesgos actualizados.

También, en la proyección de necesidades de TI para la vigencia 2026 incluidas en el PETI 2026, que apalancan cada uno de los productos a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones para el producto "*Mejorar la implementación de la estrategia de seguridad y privacidad de la información acorde a la normatividad vigente*", se registran los siguientes requerimientos:

- "Con el fin de continuar la implementación del habilitador de Seguridad y Privacidad de la Información, es necesario disponer para la vigencia 2024 -2027 de personal especializado en seguridad de la información para actualizar el diagnóstico con los nuevos lineamientos y normatividad existente, actualizar los planes asociados a seguridad e implementar controles, para robustecer los aspectos técnicos de seguridad de la información e incrementar el nivel de cumplimiento del habilitador de Seguridad y Privacidad de la Información establecido en la Política de Gobierno Digital. Mediante la adopción de este modelo se busca el aprovechamiento estratégico de las TIC como herramienta en el fortalecimiento de la seguridad de la información de la entidad, privacidad de los datos de los ciudadanos y funcionarios de la Función Pública, todo esto, soportado por la legislación colombiana"

- "Con el fin de continuar la implementación del habilitador de Seguridad y Privacidad de la Información, se requiere contar con un Oficial de Seguridad de la Información que permita garantizar la adecuada protección y conservación de los activos de información de Función Pública. Así mismo, es necesario dar continuidad a la realización de ejercicios de seguridad la actualización de políticas, normas y procedimientos relacionados con la seguridad digital, la actualización del diagnóstico conforme a los nuevos lineamientos y normatividad vigente, así como la actualización de los planes asociados a seguridad e implementación de controles".

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Recomendación:

Como se expone en la proyección de necesidades de TI, relacionadas en el PETI 2026, la entidad debe disponer para esta vigencia de:

- ✓ “Personal especializado en seguridad de la información para actualizar el diagnóstico con los nuevos lineamientos y normatividad existente, actualizar los planes asociados a seguridad e implementar controles, para robustecer los aspectos técnicos de seguridad de la información e incrementar el nivel de cumplimiento del habilitador de Seguridad y Privacidad de la Información establecido en la Política de Gobierno Digital. Mediante la adopción de este modelo se busca el aprovechamiento estratégico de las TIC como herramienta en el fortalecimiento de la seguridad de la información de la entidad, privacidad de los datos de los ciudadanos y funcionarios de la Función Pública, todo esto, soportado por la legislación colombiana”

- ✓ “Un Oficial de Seguridad de la Información que permita garantizar la adecuada protección y conservación de los activos de información de Función Pública. Así mismo, es necesario dar continuidad a la realización de ejercicios de seguridad la actualización de políticas, normas y procedimientos relacionados con la seguridad digital, la actualización del diagnóstico conforme a los nuevos lineamientos y normatividad vigente, así como la actualización de los planes asociados a seguridad e implementación de controles”.

1.2.4.2. Competencia, toma de conciencia y comunicación

Lineamiento: Las entidades deben definir un plan de comunicación, capacitación, sensibilización y concientización para:

- ✓ Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del MSPI.
- ✓ Involucrar al 100% de los colaboradores de la entidad en la implementación y gestión del MSPI.
- ✓ Concientizar a los colaboradores y partes interesadas en la importancia de la protección de la información.
- ✓ Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información.
- ✓ Tener un enfoque práctico en la respuesta a incidentes, especialmente en técnicas de phishing, ingeniería social y ciberhigiene, para fortalecer la capacidad de respuesta ante ataques dirigidos.

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

- ✓ Cuando proceda, tomar las acciones para adquirir y/o fortalecer la competencia de los responsables del MSPI.
- ✓ Evaluar la eficacia de las acciones de concientización y sensibilización realizadas."

Propósito: "Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos los funcionarios conozcan la política, su rol en el MSPI y las implicaciones de no aplicar las reglas de seguridad y privacidad."

Estado Actual:

Verificando los diferentes frentes de capacitación y sensibilización en SI, se encontró la siguiente gestión:

- ✓ El PESI V02 2026 incluye la actividad de "Diseñar, implementar y comunicar un programa de concientización en seguridad de la información para Función Pública", con la meta de "Ejecutar el Plan de Concienciación en Seguridad y Privacidad, fortaleciendo la cultura de seguridad, promover el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) y mitigar riesgos asociados al manejo de la información institucional", basándose en los siguientes hitos bajo la responsabilidad del CISO:

  - Identificar las necesidades de concientización
  - Definir las temáticas prioritarias a abordar.
  - Socializar los lineamientos y buenas prácticas en seguridad de la información a través de jornadas de capacitación.

- ✓ El PAA 2026 registra la actividad E3-A3 'Realizar jornadas de sensibilización en seguridad de la información para Función Pública' asignando como responsable al CISO y con una periodicidad definida

- ✓ El Decálogo de Seguridad (marzo 2026) es el ejemplo de una acción de concientización ejecutada, comunicando a todos los servidores los 10 pilares de seguridad digital del DAFP con canales de reporte definidos. Al respecto, en el decálogo aparece como contacto de reporte el correo interno del responsable de seguridad que ya no labora en el Departamento.

- ✓ La OTIC estableció un cronograma anual de capacitación en Ciberseguridad para la vigencia 2026 con las siguientes actividades:

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Periodo	Tema Central (Sugerido)	Objetivo de Aprendizaje
1: Enero - Marzo	Detectando el "Phishing"	Identificar correos, SMS y llamadas fraudulentas para evitar el robo de credenciales explicar sobre el evento ocurrido en diciembre 2025.
2: Abril - Junio	Gestión de Identidad y Contraseñas	Implementar el uso de gestores de contraseñas y la importancia del MFA (Autenticación de Dos Pasos).
3: Julio - Septiembre	Seguridad en el Trabajo Híbrido	Protección de redes domésticas, uso de VPN y seguridad física de dispositivos fuera de la oficina.
4: Octubre - Diciembre	Ingeniería Social e IA	Reconocer tácticas modernas como Deepfakes y estafas basadas en Inteligencia Artificial.

Fuente: Cronograma anual de capacitación ciberseguridad (OTIC 2026)

- ✓ En el mes de marzo acorde al cronograma anterior, se efectuó una campaña de sensibilización a servidores y contratistas aplicando un ejercicio sobre el tema de ingeniería social y detección de Phising. Se evidencian los debidos soportes (\\yaksa.dafp.local\10030OTIC\2026\DOCUMENTOS_APOYO\SEGURIDAD\CAPACITACIONES).

- ✓ Finalmente, como control, en la planeación institucional registrada en el SGI se puede observar el entregable denominado “Políticas de Seguridad y Privacidad de la información en Función Pública implementada”, donde se evidencia la actividad “3. Realizar jornadas de sensibilización en seguridad de la información para Función Pública”.

Pendientes:

- Como se observó en la vigencia pasada, no se evidencia gestión por parte de la entidad en cuanto a capacitación y/o formación interna brindada al responsable actual para la implementación y gestión del MSPI. Así como, la evaluación de eficacia de las acciones realizadas.
- No se evidencia la debida evaluación de las campañas de capacitación y/o sensibilización donde se mida la eficacia de las mismas.

Recomendación:

La Entidad debe:

- Fortalecer los planes de capacitación y formación en el SGSI y MSPI involucrando al responsable actual de la implementación del Modelo y a su vez robustecer los esquemas actuales de concientización, educación y comunicación con respecto a la

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

seguridad y privacidad de la información, en la que todos los funcionarios conozcan la política, su rol en el MSPI y las implicaciones de no aplicar las reglas de seguridad y privacidad, como lo establece el propósito de este lineamiento.

- Evaluar la eficacia de las acciones de concientización y sensibilización realizadas y mantener su debido registro.

1.2.4.3. Información documentada

Lineamiento:

"El modelo de seguridad y privacidad de la información de la entidad debe incluir:

- ✓ Información documentada de los lineamientos establecidos.
- ✓ Documentos que la entidad considere necesarios para la eficacia del SGSI.
- ✓ Reglas claras para crear y actualizar documentos: identificación, formato, soporte, y control de versiones.
- ✓ La información documentada debe estar disponible y ser adecuada para su uso, donde y cuando se necesite además de estar adecuadamente protegida"

Propósito:

"Mantener una documentación adecuada para que pueda ser consultada en cualquier momento por las partes interesadas y le permita conocer los detalles del sistema de gestión de seguridad de la información."

Estado Actual:

Acorde con el seguimiento a la implementación de Gobierno Digital efectuada en el mes de abril, los documentos que actualmente soportan algunos componentes de MSPI como la política general de seguridad de la información, la Política específica de Seguridad de la información, gestión de incidentes de seguridad de la información, indicadores y el Formato de Registro de Incidente de Seguridad de la Información, se encuentran publicados y disponibles internamente en el SIGP en el proceso de Gestión de tecnologías de la información.

La demás documentación relacionada con el Plan de tratamiento de riesgos, el Plan seguridad y privacidad de la información 2025, el Plan Estratégico de tecnologías de la información -PETI- 2025 Sectorial y el Plan Estratégico de tecnologías de la información -PETI- 2025 Institucional, se encuentran publicados en la página web del Departamento para el público en general (Link de acceso: https://www1.funcionpublica.gov.co/planeacion-sectorial-institucional).

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Finalmente, los soportes de la herramienta de autodiagnóstico aplicada, el archivo de inventario de activos de información y la matriz de riesgos de seguridad de la información se encuentran almacenados en el servidor de carpetas compartidas YAKSA bajo la ruta : \yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS_APOYO \SEGURIDAD\.
Nota: Los escenarios de almacenamiento y publicación de los documentos y soportes mencionados poseen adecuado grado de seguridad de acceso manteniéndolos debidamente protegidos.

Recomendación:

- Analizar con el apoyo de la OAP, el establecimiento de un sitio que permita mantener toda la documentación actualizada (versionamiento final) del MSPI en un solo sitio a nivel de backend, que garantice su disponibilidad, uso y protección como lo indica el lineamiento.

- Integrar en el acervo documental los nuevos documentos que se están generando a raíz de este seguimiento como el alcance del MSPI y los Actos administrativos derivados del CIGD que competan directamente con aprobaciones o presentaciones de artefactos del MSPI.

1.3. Fase 2: Operación

1.3.1. Control y planeación operacional

Lineamiento:

“Las entidades deben realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos y el plan de Seguridad y Privacidad de la Información, esta información debe estar documentada para cada proceso según lo planificado, los planes de tratamiento deben ser definidos y aprobados por los líderes de proceso, Los proyectos o controles de seguridad que no pueden implementarse en el corto plazo o mediano plazo se deben escalar al CIGD para toma de decisiones y asignación de recursos. Las acciones que la entidad considere relevantes deben ser aprobadas por el CIGD. De igual manera, deben reforzar los mecanismos de monitoreo continuo, incluyendo la implementación de sistemas de alerta temprana que permitan a las entidades detectar y responder a incidentes en tiempo real, garantizando la resiliencia frente a ciberataques. “

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Propósito: “Implementar los planes y controles para lograr los objetivos del MSPI”

Estado Actual:

Actualmente, como ya se había mencionado, se tiene definido el Plan estratégico de Seguridad de la Información Ciberseguridad y Privacidad de Datos – PESI 2026 v02 y el Plan de Tratamiento de Riesgos de Seguridad 2026 Versión 1 - enero 2026, sobre los cuales se tienen los debidos controles de gestión y trazabilidad de gestión interna como se especificó en el numeral 1.2.3.3. de este informe.

Así mismo, acorde a las recomendaciones del informe de seguimiento de Gobierno Digital generado por la OCI en esta vigencia, el Especialista de SI, actualizo en esta vigencia el plan estratégico de seguridad de la información – PESI, con los estándares recomendados en el habilitador de seguridad de la información. Ese documento se pudo evidenciar en la ruta : \\yaksa.dafp.local\10030OTIC\2026\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\Plan Estratégico de Seguridad de la Información, bajo el nombre “2026-01-12_Plan_estrategico_seguridad_Informacion_pesi_dafp.doc”. En este borrador se observaron los componentes recomendados en la plantilla suministrada por MinTIC. Esta versión se encuentra en proceso de presentación al CIGD para su aprobación.

En el PESI mencionado, según el lineamiento no se había definido en la vigencia 2026 en la estrategia de implementación de controles de seguridad, el detalle del plan asociado, conteniendo como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto. En la actualidad fue ajustado y se evidencia la estrategia de implementación de controles con portafolio de proyectos por eje (liderazgo, riesgos, concientización, controles, incidentes), productos esperados, responsables y alineación normativa. Incluye el detalle requerido por el lineamiento.

Recomendaciones:

- Presentar el borrador del PESI actualizado para aprobación por parte del CIGD, almacenándolo en el repositorio respectivo y efectuando su debida publicación en la página Web del Departamento, con el apoyo de la OTIC.

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

- También, tener en cuenta que los proyectos o controles de seguridad que no pueden implementarse en el corto plazo o mediano plazo se deben escalar al CIGD para toma de decisiones y asignación de recursos.

- Finalmente, mantener como se ha venido efectuando, la trazabilidad y evidencia de la implementación y gestión de los controles de seguridad y privacidad de la información, que brinda la sábana de gestión de riesgos del SGI.

1.3.2. Definición de indicadores de gestión

Lineamiento: "La entidad debe definir indicadores que le permitan medir la evolución y avance en el nivel de madurez de la seguridad de la información."

Propósito:

"Establecer indicadores para medir la gestión y madurez de la entidad en la implementación del modelo de seguridad y privacidad de la información"

Estado actual:

Si bien: el PESI V02 establece métricas de línea base (69% controles ISO, 67% PHVA, puntuaciones NIST por función); la matriz de Riesgos 2026 incluye un seguimiento semestral por control y el PAA 2026 registra el entregable E4-A2 'Realizar seguimiento al proceso a través del control de indicadores y riesgos', no se evidencian fichas técnicas formales de indicadores de madurez del MSPI incluidas en el tablero de control del plan de acción (Decreto 612/2018). Además, los indicadores A.8.11 y A.8.32 definidos en la vigencia 2025 no fueron verificados, aprobados y publicados por la OAP; estos indicadores no permiten medir el estado actual de la gestión general y madurez evolutiva de la implementación del MSPI al interior de la entidad, coadyuvan a medir algunos controles tecnológicos, pero no todo el universo del plan.

Recomendación:

Como se especificó en el seguimiento de la vigencia 2025, se debe generar una Hoja de vida del (los) indicador(es), que permita(n) medir el estado actual de la gestión general y madurez evolutiva de la implementación del MSPI al interior de la entidad, el (los) cual(es) debe(n) incluirse en el tablero de control del plan de acción, tal como lo ordena el Decreto

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

612 de 2018. Para la definición de los indicadores se puede utilizar como guía los lineamientos de Indicadores de Gestión de Seguridad de la Información

1.4. Fase 3: Evaluación de desempeño

1.4.1. Seguimiento, medición, análisis y evaluación

Lineamiento:

“Las entidades deben conocer sus avances en la implementación del modelo de Gobierno Digital, estableciendo tiempos y recursos para su monitoreo y reporte ante el Comité de Gestión y Desempeño, conforme al MIPG”.

Propósito: “Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.”

Estado actual:

Actualmente en el PTRS 2026 se establecen informes técnicos periódicos de la plataforma CheckPoint para Ciberseguridad, así como en los entregables de la planeación institucional implementados en el Departamento a través del SGI, se puede monitorear el avance en la implementación de los artefactos y controles. A su vez en el PESI V02 se definen mecanismos de 'seguimiento, evaluación y mejora continua de los controles'.

Si bien los elementos anteriormente mencionados coadyuvan al seguimiento, medición y análisis del modelo, no se está reportando al CIGD un informe integral con la evaluación y medición de la efectividad de las acciones implementadas para la adopción del modelo, según pide el lineamiento.

Recomendación:

Desarrollar y mantener un Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos de Seguridad de la Información, de los indicadores y de los artefactos que exige la implementación del MSPI y que sea del pleno conocimiento por parte del CIGD.

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

1.4.2. Auditoría Interna

Lineamiento: “Realizar mínimo una auditoría interna al año con el fin de obtener información sobre el cumplimiento del MSPI “

Propósito: “Identificar no conformidades, desviaciones y oportunidades de mejora del MSPI”

Estado actual:

Actualmente y desde la vigencia pasada la OCI ha venido efectuado el seguimiento general a la implementación del MSPI, incluyéndolo dentro del Plan anual de auditorías y seguimientos. Lo anterior con el fin de brindar un insumo de mejora continua sobre la adopción, implementación y mantenimiento del MSPI.

Los informes respectivos se encuentran publicados en la página Web de FP, en la sección de trasparencia (https://www1.funcionpublica.gov.co/informes-y-seguimientos-oficina-de-control-interno)

Recomendación:

Mantener la continuidad en la programación y ejecución anual del seguimiento a la consecución del MSPI, tal y como se ha venido ejecutando.

Como resultado de dicha gestión, generar las posibles No conformidades, hallazgos u oportunidades de mejora en pro del mejoramiento continuo de la Entidad.

1.4.3. Revisión por la Dirección

Lineamiento: “La Política y el Manual de Seguridad y Privacidad deben ser revisados y aprobados por el Comité de Gestión y Desempeño o por decisión del nominador, considerando los cambios en las necesidades de las partes interesadas.”

Propósito: “Revisar el MSPI de la entidad, por parte de la alta dirección (CIGD), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia.”

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Estado actual:

Acorde a lo visto en puntos anteriores de este seguimiento, los elementos como las políticas de seguridad de la información, manuales y demás componentes de gestión del MSPI, se han venido presentando al CIGD para su respectiva aprobación.

Si bien en el mes de enero de la vigencia 2026, se presentaron ante el CIGD los planes institucionales de la OTIC (PETI, PTRSP, PESI y PECN), con estructura de actividades, metas, fechas y responsables, lo que constituye una evidencia inicial de aprobación por la dirección sobre la planeación de seguridad. NO se evidencia al igual que en la vigencia pasada una revisión general periódica del MSPI por parte del CIGD, la cual permita determinar la conveniencia, adecuación y eficacia del Modelo.

Recomendación:

- Estructurar y mantener un informe general del avance y gestión surtida en la implementación y evolución de todos los lineamientos aplicables del MSPI, el cual sea presentado al CIGD para que le permita a esta instancia determinar la conveniencia, adecuación y eficacia del Modelo.

- Mantener como se ha efectuado hasta el momento, la política interna de reporte y aprobación por parte del CIGD, de todos los artefactos de política, gestión, mantenimiento y monitoreo de avance del MSPI. A su vez, mantener las actas respectivas.

1.5. Fase 4: Mejoramiento continuo

1.5.1. Mejora continua

Lineamiento: ”Las entidades deben contar con un plan de mejoramiento continuo que integre oportunidades de mejora, no conformidades y desviaciones, con acciones correctivas claras, responsables, tiempos y recursos definidos para fortalecer el MSPI.”

Propósito: “Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.”

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Estado actual:

El Departamento cuenta con el mantenimiento y gestión del plan de mejoramiento institucional controlado a través del SGI, donde se registran y se tratan los hallazgos derivados de diferentes fuentes de control.

Actualmente se tienen algunos elementos que integran la gestión sobre la mejora continua, establecidos en el PESI V02 en el cual se incluye el eje 'Implementación de Controles' con proyectos de mejora (política de respaldos, gestión de cambios, desarrollo seguro, gestión de incidentes) y el eje de 'Gestión de Incidentes' con procedimientos formalizados. Así mismo El PAA 2026 registra el entregable E4-A3 'Realizar el reporte de las acciones de los planes de mejoramiento del área' , articulado al SGI institucional. No obstante, no se ha empezado a desarrollar aún un “Plan anual de mejora del MSPI”, como lo especifica una de las salidas del lineamiento, el cual incluya los controles de seguridad a implementar, oportunidades de mejora, no conformidades y demás desviaciones identificadas en la gestión de los diferentes procesos de seguridad y privacidad de la información que componen el SGSI, en la revisión por la alta dirección y en la auditoría.

Recomendación:

Como se expuso en el seguimiento efectuado por esta Oficina en la vigencia 2025. Una vez se implemente la fase de evaluación y desempeño, vista en el numeral 1.4. de este informe, se debe generar el plan de mejora del MSPI mencionado en el párrafo anterior, manteniendo los debidos niveles de gestión, monitoreo, reporte y retroalimentación.

Conclusiones

La Oficina de Control Interno, en cumplimiento al Plan anual de auditorías y seguimientos vigencia 2026, ejecutó este seguimiento al Modelo de Seguridad y Privacidad de la Información - MSPI, con el fin de apoyar al DAFP a través del proceso de evaluación independiente, en la identificación de factores de mejora críticos para la adopción e implementación del modelo mencionado, con el fin de dar cumplimiento a los lineamientos establecidos en la Resolución 0500 de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Propendiendo de esta manera con la generación de una base de información que permita determinar el grado de cumplimiento de todos los lineamientos que determinan al MSPI.

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Por otro lado, se resalta el trabajo gestionado por el Especialista de seguridad actual, que a pesar de estar ejecutando dos roles al interior del Departamento ha logrado gestionar la implementación y/o ajuste de la mayoría de los artefactos que componen el MSPI, de acuerdo con los lineamientos para la implementación de la estrategia de seguridad digital, tratando de formalizar con ello un Sistema de Gestión de Seguridad y privacidad de la Información – SGSPI y seguridad digital, como lo especifica el Modelo.

Recomendaciones Generales

A nivel general, la principal recomendación se orienta en primera instancia al establecimiento de una decisión formal por parte de la Dirección (CIGD) de promover los lineamientos respectivos para generar confianza en el uso de un entorno digital seguro al interior de la entidad, impulsando la adopción, implementación y mejora continua del MSPI, a través de la asignación de tiempo y el aseguramiento de los recursos humanos, financieros, técnicos y tecnológicos necesarios para su cumplimiento y evolución en el tiempo.

En segunda instancia, con el fin de mantener la consecución de la mejora continua de la implementación del MSPI, se recomienda con el apoyo de la OAP generar un plan de mejoramiento en el SIGP con los aspectos susceptibles de mejora inmersos en este informe. Lo anterior, por cuanto para la mayoría de escenarios, se había evidenciado en la vigencia pasada el mismo estado de gestión, se ha presentado recientemente rotación de personal responsable y se avecina el próximo cambio de administración.

Jorge Iván De Castro Barón

Firmado digitalmente por Jorge Iván De Castro Barón
Fecha: 2026.07.02 16:31:54 -05'00'

Jorge Iván De Castro Barón
Jefe Oficina de Control Interno

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Función Pública

INFORME DE SEGUIMIENTO A LA IMPLEMETACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - MSPI

Versión 01
Evaluación Independiente
Junio de 2026

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co