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

Septiembre de 2025

Objetivo

Verificar y evaluar por parte de la Oficina de Control Interno el estado actual de implementación del 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:

- ✓ 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 ha venido aplicando la herramienta, la cual se encuentra en desarrollo. Actualmente se está levantando la información con el Grupo de Gestión Contractual. Se tiene planeado entregar el diagnostico completo a diciembre de la presente vigencia, según se pudo evidenciar en el plan de acción.

En la ruta \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS APOYO \SEGURIDAD \PLANES POLITICAS, se evidencia el documento de autodiagnóstico diligenciado hasta la fecha (“2025-07-15_Autodiagnostico_mspi_2025.xls”), en esta herramienta se puede detallar entre otros la evaluación de la efectividad de los controles para los 4 dominios

(Organizacional, Persona, físico y tecnológico), el avance cláusulas del modelo de operación (PHVA), la calificación frente a las mejores prácticas en ciberseguridad (NIST) y un detalle de los 93 controles diversificados en cada dominio (Id.Item, Control, Rol, Descripción, Prueba, Evidencia, Brecha, Nivel de Cumplimiento Anexo A ISO 27001, Recomendación, Tipo de Control, Propiedades de S.I., Conceptos de ciberseguridad, capacidades operativas y Dominio de Seguridad).

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: No se ha definido aún el alcance.

Recomendación:

Para el desarrollo de esta fase, se debe tener como insumo los resultados del diagnóstico inicial a raíz de la aplicación de la "herramienta de autodiagnóstico", determinando previamente:

- ✓ El contexto de la entidad (elementos externos e internos que son relevantes con las actividades que realiza la entidad en el desarrollo de su misión y que pueden influir en el logro de sus objetivos estratégicos), con el fin de conocer en detalle las características de la entidad y su entorno para implementar el MSPI.
- ✓ La necesidades y expectativas de los interesados: se deben identificar las partes interesadas internas y externas que puedan influir o verse afectadas por la seguridad y privacidad de la información, así como sus necesidades y expectativas. Esta

identificación debe incluir los requisitos legales, reglamentarios y contractuales, e integrarse adecuadamente al SGSI.

Con el insumo de los elementos antes mencionados se debe proceder a generar el alcance del MSPI, tal y como lo especifica el lineamiento, el cual debe quedar registrado en el Sistema Integrado de Planeación y Gestión (Contar con el apoyo de la OAP).

Según el manual del MSPI, se puede tener como base entre otros los siguientes ítems:

- Manual Operativo MIPG.
- Marco de Referencia de Arquitectura Empresarial definido por MinTIC
- Plan estratégico de la entidad
- informes de auditoria al MSPI
- Plan Nacional de Desarrollo.
- Política de Gobierno Digital.
- Política de seguridad digital
- Entrevistas con los líderes de procesos de la entidad.
- Listado de proveedores de la entidad.
- Normatividad que le aplique a la entidad de acuerdo con funcionalidad respectivamente.
- Presupuesto disponible para implementar el MSPI.

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 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.

✓ 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”.

Recomendación:

Se debe actualizar el acto administrativo de creación del CIGD, incluyendo en el artículo 2 como miembro al responsable de seguridad de la información, 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:

Actualmente, se encuentra publicada en el SIPG, en el proceso de "Gestión de las Tecnologías de la información" la "Política General de Seguridad de la Información", versión 01/octubre 2024 (Ruta: https://www1.funcionpublica.gov.co/documents/34645357/34703081/politica-general-seguridad-informacion-v1.pdf/415dc2a2-cc14-475c-b109-91aa5400c94b?t=1728482670613) . Esta política ya había sido verificada por la OCI durante el seguimiento a la Implementación de Gobierno Digital en esta vigencia, encontrándose el siguiente estado:

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."***

Acorde a lo anterior, en esta vigencia el responsable de seguridad y privacidad de la información, ha venido adelanto la actualización de la Política acorde con la plantilla de producto tipo establecida por MinTIC (https://gobiernodigital.MinTIC.gov.co/seguridadyprivacidad /portal/Estrategias/MSPI/) como se había recomendado, evidenciándose el borrador del nuevo documento de política versión 02 de junio 2025. Revisando dicho documento, se encuentran los siguientes elementos pendientes de implementar o ajustar de acuerdo a nuestras recomendaciones previas:

- ✓ 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***.

- ✓ 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."***

De otro lado, en el mismo micrositio del SIGP, estan publicadas las Políticas Específicas de Seguridad de la Información , donde se consolidan "las políticas internas de seguridad de la información para garantizar la confidencialidad, integridad, disponibilidad, no repudio y cumplimiento de las obligaciones en materia de tratamiento de datos personales, el buen uso, aseguramiento y cuidado de la información y el funcionamiento adecuado de los recursos tecnológicos puestos a disposición de los usuarios".

Recomendaciones:

1. En lo posible para esta versión de la Política general de seguridad de la información o para una próxima actualización implementar en el documento de la política los elementos mencionados que ya había recomendado esta Oficina en el seguimiento a la implementación de Gobierno Digital (Ver párrafo anterior).
   .
2. Una vez se tenga la versión actualizada, es importante presentar la política en el CIGD, para que sea debidamente aprobada y posteriormente proceder a su publicación oficial en el proceso respectivo del SIPG y en la página web de la entidad (Transparencia/ Planeación y seguimiento sectorial e institucional/Políticas y lineamientos sectoriales e institucionales)

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 expuso en el informe de seguimiento a la Implementación de Gobierno Digital de esta vigencia, donde actualmente por temas coyunturales la Entidad unificó los roles del Oficial de Seguridad de la Información (CISO) con el Especialista de Seguridad de la Información.

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.
- ✓ 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:

De acuerdo con la plantilla sugerida por MinTIC para el MSPI, el profesional de seguridad de la OTIC con el apoyo de la OAP y el Grupo de Gestión Administrativa actualizó el archivo de inventario de activos de información, el cual reposa en la Ruta: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS APOYO\ SEGURIDAD\PLANES POLITICAS\PLAN ESTRATEGICO SEGURIDAD. En este documento se puede evidenciar la siguiente información:

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)

Registros	**ID**
	Serie/Subserie documental
Identificación y categorización del activo	**Proceso**
	Dependencia
	Nombre o titulo del activo
	Descripción del contenido del activo de información
Clasificación del activo	**Software**
	Hardware
	Información
Características del activo	**Medio de conservación y/o soporte**
	Formato de almacenamiento
	Idioma
	Disponibilidad de la información del activo
Ubicación del activo o lugar de consulta	**Tipo de ubicación**
	El activo está a cargo de un tercero o proveedor
	Electrónica /Digital
Ciclo de vida del activo	**Fecha de generación o adquisición**
	Estado
Responsabilidades de acceso, custodia y soporte al activo de información	**Usuarios**
	Custodio
	Responsable técnico
Calificación del activo	**El activo es crítico para las operaciones Internas del negocio**
	El activo es crítico para el servicio externo (grupos de valor) o del negocio
	Clasificación de la información Ley 1712 de 2014
	Clasificación de la información Ley 1581 de 2012 y Ley 1266 de 2008 (Habeas Data) sólo aplica para datos personales
Valoración del activo	**Confidencialidad**
	Integridad o Completitud
	Disponibilidad
	Valoración del activo
	Valoración acumulativa

Fuente: Archivo de inventario “2025-07-31_Formato_inventario_activos_mostrar.xls”

Al respecto, no se evidencia la estructuración de un procedimiento metodológico de inventario y clasificación de activos de información.

Recomendación:

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.

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.

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)

- ✓ 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.
- ✓ 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:

La especialista de seguridad de la información, actualizó la matriz de riesgos de seguridad de la información, acorde con la herramienta sugerida por MinTIC en el MSPI, la cual esta evidenciada en la ruta: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\PLAN_TRATAMIENTO_RIESGOS_SEGURIDAD. En esta matriz se puede observar la siguiente información:

Proceso	
Referencia	
Activo de Información	
Tipo de activo	
Amenazas (Causa Inmediata)	
Vulnerabilidades (Causa raiz)	
Tipo de riesgo	
Descripción del Riesgo	
Clasificación riesgo	
Frecuencia	
Probabilidad inherente	
Impacto inherente	
Zona de Riesgo inherente	
No Control	
Control Anexo A	
Descripción del control	
Afectación	Probabilidad
	Impacto
Atributos	Tipo
	Implementación
	Calificación del Control
	Documentación
	Frecuencia
	Evidencia
Probabilidad residual	
Impacto residual	
Probabilidad residual final	
%	
Impacto residual final	
%	
Zona de riesgo final	
Tratamiento	
Plan de Acción	
Responsable	
Fecha de Implementación	
Seguimiento	
Estado	

Fuente: Matriz de riesgos de SI, julio 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)

Verificando la información registrada en la matriz mencionada, no se pudo evidenciar la inclusión de los siguientes riesgos de seguridad digital y controles asociados de los demás procesos de la entidad que se encuentran en la matriz de riesgos institucional en el SGI:

PROCESO	DEPENDENCIA	ESTADO	RIESGO	TIPO	CLASIFICACIÓ
Gestión del Talento Humano	Grupo de Gestión Humana	APROBADO	Posibilidad de afectación reputacional por acceso no autorizado a la información confidencial de la Historia Laboral - HL o datos personales reservados del trabajador, debido a la inadecuada gestión de permisos de acceso a los sistemas de información del proceso de Talento Humano.	Operativos	Seguridad Digital
Relacionamiento Estado Ciudadanías	Oficina de Relación Estado Ciudadanías	APROBADO	Posibilidad de afectación reputacional por queja o denuncia del grupo de valor al ente de control (superintendencia de industria y comercio) debido a la pérdida de confidencialidad en los activos de la información personal	Operativos	Seguridad Digital
Gestión Documental	Grupo de Gestión Documental	APROBADO	Posibilidad de afectación reputacional Por perdida de confidencialidad Debido a inadecuada configuración de roles y permisos en el sistema de gestion documental	Operativos	Seguridad Digital
Gestión Contractual	Grupo de Gestión Contractual	INACTIVO	Posibilidad de afectación reputacional por insatisfacción de los grupos de valor debido a la pérdida de confidencialidad del token de firma digital de ORFEO del grupo de gestión contractual	Operativos	Seguridad Digital
Gestión Financiera	Grupo de Gestión Financiera	INACTIVO	Posibilidad de afectación económica por realización de operaciones financieras no autorizadas en el sistema SIIF Nación debido a pérdida de confidencialidad de los tokens asociado a operaciones de carácter financiero (bancario)	Operativos	Seguridad Digital
Gestión Administrativa	Grupo de Gestión Administrativa, Grupo de Gestión Documental	INACTIVO	Posibilidad de afectación reputacional por insatisfacción de los grupos de valor debido a la pérdida de confidencialidad del token de firma digital del grupo de gestión administrativa	Operativos	Seguridad Digital
Gestión Financiera	Grupo de Gestión Financiera	INACTIVO	Posibilidad de afectación reputacional por insatisfacción del grupo de valor debido a la pérdida de confidencialidad del token asociado con las actividades administrativas de firma digital de documentos de ORFEO	Operativos	Seguridad Digital
Gestión Financiera	Grupo de Gestión Financiera	APROBADO	Posibilidad de afectación reputacional por insatisfacción del grupo de valor debido a pérdida de confidencialidad de los datos personales semiprivados asociados a números de cuenta de proveedores y contratistas.	Operativos	Seguridad Digital
Evaluación Independiente	Oficina de Control Interno	APROBADO	Posibilidad de afectación reputacional por pérdida de confidencialidad de la información clasificada, reservada o en construcción que está bajo responsabilidad de la dependencia debido al incumplimiento de las políticas de seguridad de la información institucionales	Operativos	Seguridad Digital
Comunicación	Oficina Asesora de Comunicaciones	APROBADO	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	Operativos	Seguridad Digital
Gestión Administrativa	Grupo de Gestión Administrativa	APROBADO	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	Operativos	Seguridad Digital
Seguimiento y Evaluación a la Gestión	Dirección General, Oficina Asesora de Planeación	INACTIVO	Posibilidad de afectación reputacional por sanciones de entes de control, debido a errores en la información divulgada y suministrada.	Operativos	Seguridad Digital
Acción Integral en la Administración Pública Nacional y Territorial	Dirección de Participación Transparencia y Servicio al Ciudadano	APROBADO	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. - DPTSC	Operativos	Seguridad Digital
Acción Integral en la Administración Pública Nacional y Territorial	Dirección de Empleo Público	APROBADO	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	Operativos	Seguridad Digital
Gestión del conocimiento y Grupos de Valor	Dirección Gestión del Conocimiento	APROBADO	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	Operativos	Seguridad Digital
Acción Integral en la Administración Pública Nacional y Territorial	Grupo de Apoyo a la Gestión Meritocrática	APROBADO	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	Operativos	Seguridad Digital
Acción Integral en la Administración Pública Nacional y Territorial	Grupo de Apoyo a la Gestión Meritocrática	APROBADO	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.	Operativos	Seguridad Digital
Gestión Financiera	Grupo de Gestión Financiera	APROBADO	Posibilidad de afectación económica y reputacional por insatisfacción de los grupos de valor debido a la pérdida de confidencialidad por la realización de operaciones financieras no autorizadas o a la pérdida de los tokens asociado a operaciones de carácter financiero (bancario) o actividades administrativas de firma digital de documentos de ORFEO.	Operativos	Seguridad Digital
Generación de Productos y Servicios para la Gestión Pública	Dirección de Empleo Público, Oficina de Tecnologías de la Información y las Comunicaciones	APROBADO	Posibilidad de afectación reputacional por divulgación no autorizada debido a pérdida de confidencialidad de la información reservada o clasificada almacenada en las bases de datos del aplicativo por la integridad pública.	Operativos	Seguridad Digital
Control Disciplinario Interno	Oficina de Control Disciplinario Interno	APROBADO	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.	Operativos	Seguridad Digital

Fuente: Informe gestión riesgos SGI 29-sept-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)

A su vez, en la matriz de riesgos de seguridad, no se evidencia el registro del siguiente riesgo y sus controles, establecidos en la matriz de riesgo institucional:

DEPENDENCIA	ESTADO	RIESGO	TIPO	CLASIFICACIÓN
Oficina de Tecnologías de la Información y las Comunicaciones	APROBADO	Posibilidad de afectación reputacional por quejas de grupos de valor y/o sanciones de entes de control debido a pérdida de Integridad (modificación no autorizada) de la información o configuración de los servicios gestionados por la OTIC causados por posible ataque informático, falla eléctrica, errores de configuración, error humano en la aplicación de procedimientos, falla tecnológica, vulnerabilidades conocidos o desconocidos en el software y hardware	Operativos	Seguridad Digital

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.

Recomendación:

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 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:

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)

- ✓ 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 2025 Versión 1 - enero 2025", el cual esta publicado en la Página web del DAPF y tiene por objetivo: "identificar, evaluar y mitigar los riesgos relacionados con la seguridad de la información y los activos de la entidad. abordando diversos aspectos para garantizar la integridad, confidencialidad y disponibilidad de la información, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016). Garantizando que los riesgos asociados con la seguridad de la información y los activos de la organización estén adecuadamente gestionados, para minimizar el impacto de eventos negativos"; en dicho plan se tienen especificadas las siguientes actividades:

Actividades	Meta	indicador	Fecha Inicio	Fecha Fin
Identificar y analizar las amenazas actuales y potenciales que podrían afectar la seguridad de los activos identificados	Realizar un Análisis de Amenazas y sus posibles soluciones	número de amenazas atendidas VS número de amenazas reportadas	1/02/2025	20/06/2025
Monitorear los mantenimientos programados de la infraestructura de la entidad	realizar los mantenimientos preventivos de los servicios de infraestructura identificados	números de mantenimientos realizados VS números de mantenimientos planeados	1/04/2025	20/10/2025
Revisión sobre usuarios, roles y privilegios en los sistemas de información	Depuración de los usuarios, roles y privilegios en los sistemas de información	dos (2) revisiones de los planes al año	1/02/2025	30/10/2025
Revisar los planes de recuperación de servicios de T.I	Actualización de los planes de recuperación	dos (2) revisiones de los planes al año	3/02/2025	30/11/2025
Implementar programas de concientización y formación en seguridad para el personal, con el objetivo de crear una cultura de seguridad.	Realizar dos campañas de concientización y Capacitación a todos los empleados de la entidad sobre formación de seguridad	número de campañas realizadas VS número de campañas planificadas	1/02/2025	30/11/2025

Fuente: Plan de Tratamiento de Riesgos de Seguridad 2025 Versión 1 - enero 2025

Actualmente la especialista de SI, maneja un control interno de gestión en Excel de cada actividad del plan (Ruta: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS_APOYO\

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\REPORTE_SGI), el cual contiene la siguiente información: Entregable/nombre/riesgo, Control, Mes de reporte, Reporte, Ruta de evidencia, Nombre de archivo, indicadores.

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
- ✓ 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.

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, en esta vigencia en el CIGD se efectuó la aprobación del plan de tratamiento de riesgos de seguridad y privacidad de la información, evidenciándose en el acta 001 del Comité del 29 de enero de 2025, su presentación y aprobación.

Recomendación:

El (Los) responsable(s) asignado (s) para la gestión de implementación del MSPI, deben como segunda línea de defensa, efectuar el monitoreo periódico a la gestión en el tratamiento de riesgos de Seguridad Digital en la entidad y mantener al proceso respectivo informado sobre su evolución.

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 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:

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)

DNP / PIIP	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

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 2025 (Versión 1 – enero 20215) 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 2025 que apalancan cada uno de los productos a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones para el producto “Servicio de actualización del Sistema de Gestión - Dar continuidad a la implementación de la política de Gobierno Digital”, se registra la meta, costo asociado y la justificación representada en:

- ✓ Mejorar la implementación de la estrategia de seguridad y privacidad de la información acorde a la normatividad vigente
- ✓ Fortalecer la estrategia de gobierno digital cumpliendo la normatividad existente.

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)

Además, se resalta la actividad asociada al producto mencionado relacionada con el mejoramiento de la implementación de la estrategia de seguridad y privacidad de la información acorde a la normatividad vigente, donde se ponderan los costes requeridos para:

- ✓ "…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"

- ✓ "…disponer para la vigencia 2024- 2027 de un oficial de la seguridad de la información para garantizar que los activos de información de Función Pública estén y se conserven adecuadamente protegidos, continuar con la realización de Ethical Hacking, la actualización de políticas, normas y procedimientos relacionados con la seguridad digital, 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."

Recomendación:

Como se expone en la proyección de necesidades de TI, relacionadas en el PETI 2025, la entidad debe disponer para el siguiente año 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.

- ✓ Un oficial de la seguridad de la información (CISO) para garantizar que los activos de información de Función Pública estén y se conserven adecuadamente protegidos,

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)

mantener la actualización de políticas, normas y procedimientos relacionados con la seguridad digital, 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 y por ende del MSPI.

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.
- ✓ 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:

Al respecto, se han efectuado campañas de concientización a servidores y contratistas interesadas en la importancia de la protección de la información, además 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 "1. Realizar jornadas de sensibilización en seguridad de la información para Función Pública". En esta actividad, se evidencia la debida gestión y registro en la planeación institucional de la gestión trimestral efectuada por la especialista

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)

en SI de la OTIC; dicha capacitación se orientó para el primer trimestre de 2025 a Ciberseguridad Temporada Fishing y para el segundo trimestre Confidencialidad en los servicios de información personal al grupo de la OREC (Soportes en las rutas: \\Yaksa\10030otic\2025\DOCUMENTOS_APOYO\SEGURIDAD\REPORTE_SG y \\Yaksa\10030otic\2025\DOCUMENTOS_APOYO\SEGURIDAD\COMPROMISOS\CAPACITACIONES). Están aún pendientes las capacitaciones para tercer y cuarto trimestre.

Con relación a lo anterior, 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.

De otra parte, la identificación de las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información la efectúa el responsable actual de la implementación del MSPI.

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 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.

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”

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:

“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:

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).

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 estan generando a raíz de este seguimiento como el alcance del MSPI y los Actos administrativos derivados del

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)

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 lideres 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. “

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 y el Plan de Tratamiento de Riesgos de Seguridad 2025 Versión 1 - enero 2025, 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\2025\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\PLAN_ESTRATEGICO_SEGURIDAD, bajo el nombre “2025-06-10_Plan_estrategico_seguridad_Informacion_pesi_dafp.doc”. En este borrador se

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)

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 ha definido 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.

Recomendación:

- ✓ 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.

- ✓ Una vez se defina y apruebe la adopción del MSPI al interior del DAFP y por ende el recurso humano requerido para la gestión del MSPI, para la próxima vigencia se debe actualizar y aprobar la siguiente versión del PESI con la inclusión 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. Al respecto, tener en cuenta el universo de los controles definidos por cada riesgo determinado en el Plan de tratamiento de los riesgos de seguridad de la información.

  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."

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:

“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:

La OTIC con el apoyo de la OAP, a partir de junio de la presente vigencia inició la tarea de ajustar e implementar algunos los indicadores de seguridad de la información, actividad que fue culminada y que se encuentra en etapa de aprobación y publicación por parte de la OAP para esta vigencia. Para ello, se especificaron dos nuevos indicadores, a los que se les genero la respectiva ficha técnica como se muestra a continuación:

Marco de referencia: evaluación del cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) ,cumplimiento de los controles del Anexo A de la ISO/IEC 27001:2022 del dominio A.8 (Controles tecnológicos).

- Indicador 1: “CONTROL A.8.11 – Seguridad del software en desarrollo”:

  - ✓ Objetivo: Garantizar que los procesos de desarrollo de software (interno o externo) sigan buenas prácticas de seguridad para evitar vulnerabilidades desde la etapa de diseño. Avalando que los datos sensibles sean enmascarados o anonimizados cuando se utilizan en entornos de desarrollo, pruebas o capacitación.
  - ✓ Descripción: Este indicador permite medir la capacidad de respuesta técnica y de mejora continua ante incidentes de seguridad relacionados con vulnerabilidades por inyección de código (como SQL Injection, Cross-site Scripting, Command Injection, etc.). Evalúa la cantidad de requerimientos correctivos, preventivos o de mejora que han sido documentados y reportados formalmente a raíz de estos incidentes.

- Indicador 2: “Protección contra denegación de servicio Sistema de Información y Gestión del Empleo Público SIGEPII. Control A.8.32”:

  - ✓ Objetivo: Capacidad de detectar y mitigar eficazmente los intentos de denegación de servicio (DoS/DDoS), ayudando a preservar la disponibilidad de los servicios críticos.

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)

- ✓ Descripción: Este indicador permite medir el porcentaje de ataques de denegación del servicio atendidos y resueltos en el Sistema de Información y Gestión del Empleo Público SIGEPII.

No obstante, los indicadores mencionados no permiten medir el estado actual de la gestión general y madurez evolutiva de la implementación del MSPI al interior de la entidad. Estos coadyuvan a medir algunos controles tecnológicos, pero no todo el universo del plan.

Recomendación:

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)n incluirse en el tablero de control del plan de acción, tal como lo ordena el Decreto 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 modelo de tratamiento de riesgos y de planeación institucional implementado en el Departamento a través del SGI, se puede monitorear el avance en la implementación de los artefactos y controles que se han evidenciado en este informe y que conforman parte de la adopción general del 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 el momento, 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.

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:

Hasta la fecha la OCI, ha venido adelantando seguimientos tangenciales al MSPI derivados de la implementación de los habilitadores de Gobierno Digital. Teniendo en cuenta lo establecido en la Resolución 00500 de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y en su acápite 9.2 de auditoría interna, se planeó para esta vigencia el presente seguimiento, con el fin de brindar el insumo inicial de mejora continua sobre la adopción, implementación y mantenimiento del MSPI.

Recomendación:

En el Plan anual de auditorías y seguimientos generado por la OCI, programar para cada vigencia la ejecución anual del seguimiento o auditoría al cumplimiento del MSPI, dependiendo del estado de adopción e implementación del modelo en la entidad. El cual debe tener la aprobación del Comité de Coordinación de Control Interno.

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

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)

1.4.3. 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.”

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.

Por otro lado, no se evidencia 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

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.”

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

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, 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.

Recomendación:

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.

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)

Conclusiones

La Oficina de Control Interno, en cumplimiento al Plan anual de auditorías y seguimientos vigencia 2025, 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 inicial que permita determinar el grado de cumplimiento de todos los lineamientos que determinan al MSPI.

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 algunos 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, se recomienda previo análisis tener en cuenta la implementación en el corto o mediano plazo de las recomendaciones detalladas en cada una de las etapas del MSPI, registradas a lo largo del presente informe.

Jorge Iván De Castro Barón
Firmado digitalmente por Jorge Iván De Castro Barón
Fecha: 2025.09.30 16:39:27 -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
Septiembre de 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