

 FONDO DE PREVISIÓN SOCIAL DEL CONGRESO DE LA REPÚBLICA	FORMATO INFORME EJECUTIVO DE AUDITORÍA INTERNA	CODIGO: F11-PRO-CIG-001 VERSION: 1 Fecha de aprobación: 19/12/2025 Página 1 de 12
---	---	---

INFORME EJECUTIVO DE AUDITORÍA	
NOMBRE DEL PROCESO	Direccionamiento Estratégico institucional Gestión Tecnológica
LIDER DE PROCESO	GERMÁN CORREA AMADO Jefe Oficina Asesora de Planeación y Sistemas
EQUIPO AUDITOR	RAFAELA MONTOYA GONZÁLEZ Asesora de Control Interno WELFIN JHONATHAN CANRO R. Contratista

Reunión de Apertura	Ejecución de la Auditoría				Reunión de Cierre
01/07/2026	Desde	01/07/2026	Hasta	14/09/2026	24/09/2026

OBJETIVO DE LA AUDITORIA
Evaluar el grado de madurez, mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información (MSPI), verificando el cumplimiento de los lineamientos establecidos por MinTIC, la Política de Gobierno Digital y la normatividad interna aplicable.

ALCANCE DE LA AUDITORIA
Esta evaluación cubre las actividades ejecutadas por el proceso para el periodo comprendido entre el 1/01/2025 al 31/05/2026 para los siguientes aspectos:
1. Lineamientos del Documento Maestro del Modelo de Seguridad y Privacidad de la Información, versiones 2021 y 2025 expedidas por el MinTIC, asociados con las fases de diagnóstico, planificación y operación.
2. Indicadores asociados con el Modelo de Seguridad y Privacidad de la Información

DESCRIPCIÓN DE OBSERVACIONES			
# de Observación	Nombre	Condición	Responsable
1	Lineamientos Fase de Planificación	Del documento Comprensión de las Necesidades y Expectativas de las Partes Interesadas consultado en el Sistema de Gestión de la Calidad del proceso Direccionamiento estratégico Institucional, se observó que no se contempla dentro del título “las Entidades que controlan las actividades asociadas a la Entidad (Entorno)” al Ministerio de Tecnologías de la Información y Comunicaciones de Colombia	Oficina Asesora de Planeación y Sistemas

 FONDO DE PREVISIÓN SOCIAL DEL CONGRESO DE LA REPUBLICA	FORMATO INFORME EJECUTIVO DE AUDITORÍA INTERNA		CODIGO: F11-PRO-CIG-001 VERSION: 1 Fecha de aprobación: 19/12/2025 Página 2 de 12
		(MinTIC). Entidad que regula y norma aspectos relacionados con el Modelo de Seguridad y Privacidad de la información.	
2	Política de Gestión de Riesgos	Una vez consultada la Política de Gestión de Riesgos de la entidad que se documenta a través del Manual de Riesgos SIAR código MNL-SIAR 001 V.1, se observó que no cuenta con los lineamientos documentados para la gestión de riesgos de seguridad y privacidad de la información.	Oficina Asesora de Planeación y Sistemas UGIR
3	Declaración de aplicabilidad.	De la consulta realizada a la declaración de aplicabilidad vigente de la entidad, se observó desactualización frente a los controles establecidos en el anexo A del Documento Maestro del MSPI versión del 2025.	Oficina Asesora de Planeación y Sistemas

CONCLUSIONES DE LA AUDITORIA

- De la evaluación al cumplimiento de lineamientos del Documento Maestro del Modelo de Seguridad y Privacidad de la Información, versiones 2021 y 2025 expedidas por el MinTIC, se identificaron (2) conformidades y (3) observaciones, descritos en el informe definitivo y detallado de la auditoría.
- De la revisión a los Indicadores asociados con el Modelo de Seguridad y Privacidad de la Información documentados en la entidad, se identificó cumplimiento según la información aportada por el proceso auditado.

RECOMENDACIONES DE LA AUDITORIA

Fase planificación:

- Definir fechas precisas para las acciones establecidas en el plan de trabajo general y detallado del MSPI entregado con memorando 2026-220-001460-3 del 01 de septiembre de 2026. Lo anterior, dado que este plan define la hoja de ruta en la actualización de la documentación, lineamientos y acciones frente a la versión 2 de 2025 del Documento Maestro del modelo.
- Adicionalmente, la definición de estas fechas programa de manera integral a los responsables que deben surtir actividades en la entrega de los productos y con ello se fortalezca oportunamente la actualización del modelo en la entidad.
- Para la implementación efectiva y cumplimiento de acciones clave del MSPI, se



FORMATO INFORME EJECUTIVO DE AUDITORÍA INTERNA

recomienda programar en la agenda del Comité de Gestión y Desempeño la revisión periódica de la adopción del MSPI al menos dos veces por año, tal como lo indica el lineamiento del numeral 7.2.1 liderazgo y compromiso del Documento Maestro.

- Analizar la viabilidad en que el clausulado del contrato de prestación de servicios de la persona que actúa como responsable del MSPI en el Fondo, se registre explícitamente en sus obligaciones específicas los lineamientos establecidos en el artículo 6 de la Resolución 500 de 2021, expedida por MinTIC.
- Incluir en la agenda del Comité de Gestión y Desempeño los documentos del MSPI que serán actualizados conforme a la versión 2025 del Documento Maestro del modelo. Esto como estrategia de conocimiento, adopción y decisión por parte de sus miembros.
- Actualizar el inventario de activos de información de cada proceso del Fondo y presentar sus resultados ante el Comité de Gestión y Desempeño.
- Actualizar el Plan para el Tratamiento de Riesgos de Seguridad de la Información PLN-GTC-002, teniendo en cuenta los lineamientos definidos en el Documento Maestro del MSPI y la Guía para la Gestión Integral de Riesgos en Entidades Públicas. versión 7 de 2025 expedida por el DAFP. Lo anterior, dado que uno de los cambios registrados en dicha versión, comunica:

“6. Se actualizan contenidos relacionados con los riesgos de seguridad de la información, desplegando la totalidad de los pasos metodológicos y se incluye una matriz que desarrolla un ejemplo práctico como anexo”

- Analizar la viabilidad de solicitar al Comité de gestión y Desempeño la inclusión en el Plan Institucional de Capacitación – PIC vigencia 2027, la acreditación de personal de planta con la certificación en la norma técnica ISO/27001 para la implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información en la entidad.

Fase Operación:

- Incluir dentro del Plan para Sistema de Gestión de Seguridad de la Información – PLN-GTC-003, las actividades, acciones, fechas, recursos y responsables requeridos y programados en cada vigencia para el mantenimiento oportuno y efectivo del Modelo de Seguridad y Privacidad de la Información de la entidad, a fin de cumplir con los productos del numeral 8.1 de Control y Planeación Operacional del Documento Maestro del MSPI, versión 2025.
- Actualizar la matriz de riesgos de seguridad digital - MAP-SGSI-001, teniendo como



FONDO DE PREVISIÓN SOCIAL DEL
CONGRESO DE LA REPÚBLICA

FORMATO INFORME EJECUTIVO DE AUDITORÍA INTERNA

CODIGO: F11-PRO-CIG-001
VERSION: 1
Fecha de aprobación:
19/12/2025
Página 4 de 12

referente el Documento Maestro del MSPI y la Guía para la Gestión Integral de Riesgos en Entidades Públicas. versión 7 de 2025 expedida por el DAFP.

- Actualizar las evidencias documentadas de los siguientes controles, dado que surgieron alguna actualización, según se observó en la mesa de reunión del 08 de septiembre de 2026:
 - **8.9 Gestión de la configuración:** el control documentado es un libro Excel; sin embargo, esto migró a un desarrollo interno rotulado "Gestión Tecnológica".
 - **8.31. Separación de entornos de desarrollo, evidencia y producción:** el control no documenta la evidencia; no obstante, este se ejecuta en el desarrollo interno rotulado "Gestión Tecnológica".
 - **8.33. Información de las Pruebas:** actualizar el responsable de ejecutar el control, dado que no el jefe de la Oficina Asesora de Planeación no lo realiza.
- Documentar el manual de usuario del desarrollo interno rotulado como "Gestión Tecnológica". Adicionalmente, analizar si se debe y requiere tramitar su registro ante la Dirección Nacional de Derechos de Autor.
- Incorporar al MinTIC dentro del documento Comprensión de las Necesidades y Expectativas de las Partes Interesadas.
- Actualizar entre la UGIR y la Oficina Asesora de Planeación y Sistemas, la Política de Gestión de Riesgos de la entidad con los lineamientos para la gestión de seguridad y privacidad de la información, teniendo en cuenta la Guía para la Gestión Integral de Riesgos en Entidades Públicas. versión 7 de 2025 expedida por el DAFP. Lo anterior, dado que uno de los cambios registrados en dicha versión, comunica:

“6. Se actualizan contenidos relacionados con los riesgos de seguridad de la información, desplegando la totalidad de los pasos metodológicos y se incluye una matriz que desarrolla un ejemplo práctico como anexo”
- Actualizar la declaración de aplicabilidad y presentarla para su aprobación en el Comité de gestión y desempeño; y además, tener en cuenta los lineamientos del Documento Maestro que señala: *“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”*.

NOTA: El informe definitivo detallado y ejecutivo fue firmado y comunicado al proceso auditado y a la alta dirección de la entidad mediante memorando Radicado No.: 2026-200-001651-3 Fecha: 24 de septiembre del 2026.