INFORME ACTIVIDAD DE REQUERIMIENTO LEGAL SEGUIMIENTO A LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI EN EL MHCP

Objetivo

Verificar el cumplimiento, por parte del MHCP, de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), mediante el seguimiento a la implementación de los lineamientos establecidos por MinTIC en la Resolución 2277 de 2025, su articulación con los requisitos de la norma ISO/IEC 27001:2022 y la existencia de evidencias de soporte.

Alcance

La evaluación comprendió el cumplimiento de la normatividad aplicable en materia de Seguridad y Privacidad de la Información (SPI) en el MHCP, mediante la verificación de la implementación de los lineamientos establecidos en la Resolución 2277 de 2025 del MinTIC (que actualiza el Anexo 1 de la Resolución 500 de 2021) y su articulación con la norma ISO/IEC 27001:2022, con fecha de corte al 30 de junio de 2026.

Principales Criterios

- Resolución 2277 de 2025 (MinTIC).
- Norma Internacional ISO/IEC 27001:2022.
- Decreto 1078 de 2015 sobre la Política de Gobierno Digital y el habilitador de Seguridad y Privacidad de la Información en el sector público.
- Documentación de Procesos Internos: Est.3.1 Gobierno y Gestión TIC junto con sus manuales y guías del SMGI.

Desarrollo y resultado de la ARL

Cumplimiento General de la implementación MSPI

Calificación promedio MSPI

94/100

Nivel: OPTIMIZADO

Basado en Autodiagnóstico MinTIC y 93 Controles del Anexo A ISO 27001:2022

✓	La Entidad cuenta con un análisis del contexto organizacional documentado.
✓	La Entidad cuenta con elementos documentados para establecer, implementar, mantener y mejorar la Seguridad de la Información.
✓	El MHCP promueve la apropiación de las responsabilidades en los diferentes niveles organizacionales.
✓	La Entidad cuenta con controles organizacionales consolidados que fortalecen la gobernanza, la gestión de riesgos y la seguridad de la información, alcanzando un nivel de madurez sobresaliente.
✓	El MHCP dispone de controles asociados al ciclo de vida del personal que promueven la apropiación de la seguridad de la información y el cumplimiento de responsabilidades.
✓	El MHCP cuenta con controles físicos para la protección de instalaciones, equipos y activos de información.
✓	La Entidad dispone de controles tecnológicos para proteger los activos de información institucionales.

Cumplimiento parcial de los criterios evaluados

Cumple parcialmente

13 Aspectos

15 % Cumplimiento parcial

85% | 15%

13 de 93 criterios y 10 cláusulas evaluados

Identificación y gestión de los requisitos de las partes interesadas del Sistema de Gestión de Seguridad de la Información (SGSI).
Incorporación de compromisos de cumplimiento y mejora continua del SGSI.
Definición y seguimiento de los objetivos de seguridad de la información.
Actualización de la información documentada del SGSI.
Documentación de las entradas de la revisión por la dirección del SGSI.
Gestión y análisis de inteligencia de amenazas para la seguridad de la información.
Controles de acceso a recursos externos de internet.
Gestión del licenciamiento de software y los derechos de propiedad intelectual
Protección de equipos portátiles fuera de las instalaciones de la Entidad.
Validación de la remediación de vulnerabilidades técnicas.
Implementación de controles de enmascaramiento de datos.
Validación periódica de las copias de respaldo de la información.
Filtrado de servicios web externos de correo y almacenamiento en la nube.

Análisis de la Gestión de Riesgos

Revisado el Mapa de Riesgos del Proceso Est.3.1 Gobierno y Gestión TIC, se identificaron los siguientes cuatro (4) riesgos asociados al alcance definido para el seguimiento:

- *Posible afectación económica y/o reputacional por la falla o no disponibilidad de sistemas misionales críticos, causada por problemas técnicos, falta de mantenimiento o actualizaciones, debido a deficiencias en la gestión y planificación de la infraestructura tecnológica, que puede generar interrupciones en los servicios digitales.*
- *Posible afectación económica y reputacional de la entidad por la interrupción o disminución (degradación) de servicios tecnológicos críticos, causada por fallas o incumplimientos de proveedores, debido a debilidades en la gestión y supervisión de proveedores.*
- *Posible afectación económica y reputacional de la entidad por la interrupción o compromiso de servicios e información, causada por la ejecución de código malicioso, debido a d*ebilidades en la gestión de vulnerabilidades, controles de seguridad insuficientes y uso inadecuado de los recursos tecnológicos.
- *Posible afectación económica y reputacional de la entidad por la divulgación o pérdida no autorizada de información sensible, causada por accesos indebidos o ciberataques, debido a deficiencias en la gestión y control de la seguridad de la información.*

Los cuales cuentan con dos (2) controles asociados cada uno, sobre los cuales se validó:

Diseño del riesgo	Diseño del Control	Efectividad
Adecuadamente estructurado conforme con los criterios metodológicos definidos en la Guía para la Gestión Integral del Riesgo – DAFP.	Adecuado diseño, alineado con el componente del SCI y con los criterios definidos por el DAFP, en cuanto a: i) **Estructura del control**: responsable de ejecutar el control, acción y complemento, ii) **Tipología**: controles preventivos y iii) **Forma de ejecución: manual**.	De acuerdo con lo reportado en el SMGI a la fecha de la evaluación no se evidencia la materialización del riesgo.
Oportunidad	**Evidencia de Ejecución**	**Formalización**
El primer monitoreo está programado para el 31 de agosto de 2026.	Información disponible en el SMGI.	Se verificó la existencia de la documentación Caracterización Proceso Est.3.1 versión 1 del 01/Dic/2025 13:38:00 y en sus procedimientos asociados. Sin embargo, se identificó una oportunidad de mejora orientada a fortalecer la incorporación y socialización de dicho proceso en el Mapa de Procesos Institucional.

Fortalezas

- ***Gestión de políticas de seguridad de la información:*** *La Entidad dispone de controles de seguridad de la información que fortalecen el SGSI y favorecen la gestión de los riesgos asociados a los activos de información institucionales.*
- ***Procesos de verificación de antecedentes:*** *La Entidad cuenta con controles para la gestión de personas que fortalecen la protección de la información y promueven la cultura de seguridad de la información.*
- ***Perímetros de seguridad:*** *La Entidad dispone de controles de seguridad física y ambiental que fortalecen la protección de los activos de información y la gestión de riesgos asociados a la infraestructura institucional.*
- ***Desarrollo seguro:*** *La Entidad dispone de mecanismos que fortalecen el desarrollo seguro de software y contribuyen a la protección de los sistemas de información institucionales.*

Hacienda

Observaciones y Acciones SMGI

Observación	Criticidad
OCI-2026-ARL-52-01: Gestión de requisitos de las partes interesadas del SGSI. Se evidenció que la Entidad no había definido ni documentado los requisitos y expectativas de las partes interesadas que deben gestionarse a través del SGSI, ni las actividades para su implementación, lo que puede afectar el cumplimiento de obligaciones aplicables y la gestión de riesgos de seguridad de la información. Esta situación incumple lo establecido en la Resolución 500 de 2021 y la cláusula 4.2 de la ISO/IEC 27001:2022. Se recomienda actualizar la matriz de partes interesadas incorporando los requisitos aplicables, responsables, controles, evidencias y mecanismos de seguimiento.	Baja
OCI-2026-ARL-52-02: Fortalecimiento del cumplimiento y mejora continua del SGSI. Se evidenció que la Política de Seguridad de la Información no incluía de forma expresa los compromisos de cumplimiento de requisitos aplicables ni de mejora continua del SGSI, en contravia de lo establecido en la Resolución 500 de 2021 y la cláusula 5.2 de la ISO/IEC 27001:2022. Se recomienda fortalecer y actualizar la política, incorporando dichos compromisos y estableciendo mecanismos de revisión, aprobación, divulgación y mantenimiento alineados con los lineamientos del MSPI.	Baja
OCI-2026-ARL-52-03: Fortalecimiento de los objetivos de seguridad de la información. Se evidenció que los objetivos de seguridad de la información definidos por la Entidad no presentan trazabilidad con la Política de Seguridad de la Información y carecen de planes documentados, indicadores y mecanismos de seguimiento que permitan evaluar su cumplimiento y efectividad. Esta situación incumple la cláusula 6.2 de la ISO/IEC 27001:2022 y los lineamientos del MSPI. Se recomienda ajustar los objetivos de seguridad de la información, asegurando su alineación con la Política de Seguridad.	Extrema
OCI-2026-ARL-52-04: Fortalecimiento de la actualización de la información documentada del SGSI. Se evidenció que el SGSI no disponía de controles formalizados para la actualización, control de cambios, retención y disposición de la información documentada, identificándose documentos relevantes sin evidencias de revisión o actualización. Esta situación incumple la cláusula 7.5.3 de la ISO/IEC 27001:2022. Se recomienda fortalecer el control de la información documentada del SGSI mediante la actualización de una matriz.	Baja
OCI-2026-ARL-52-05: Debilidades en la documentación de las entradas para la revisión por la dirección del SGSI. Se evidenció que la revisión por la dirección del SGSI no contó con la totalidad de la información requerida para evaluar su desempeño y mejora continua, lo que puede limitar la toma de decisiones y el fortalecimiento del sistema. Esta situación incumple la cláusula 9.3 de la ISO/IEC 27001:2022. Se recomienda fortalecer y estandarizar la revisión por la dirección del SGSI, mediante herramientas que incluya todas las entradas requeridas por ISO/IEC 27001:2022.	Baja
OCI-2026-ARL-52-06: Gestión y análisis de amenazas de seguridad de la información. Se evidenciaron aspector por fortalecer en la gestión de la información documentada del SGSI, relacionadas con su actualización, control de cambios, conservación y disposición, lo que puede afectar la trazabilidad y el cumplimiento de los requisitos del sistema. Esta situación incumple el control organizacional A.5.7 de la ISO/IEC 27001:2022. Se recomienda formalizar e implementar una metodología de inteligencia de amenazas que contemple la identificación de fuentes de información, criterios de análisis, clasificación y priorización de amenazas.	Baja
OCI-2026-ARL-52-07: Gestión de accesos a recursos externos de Internet. Se evidenció que los controles de acceso a recursos externos de Internet requieren fortalecimiento para asegurar una gestión adecuada de las excepciones y reducir la exposición a riesgos de seguridad de la información. Esta situación incumple el control organizacional A.5.15 de la ISO/IEC 27001:2022. Se recomienda revisar y fortalecer la política de navegación y los controles de acceso a recursos externos de internet, definiendo criterios de autorización basados en perfiles de usuario.	Baja
OCI-2026-ARL-52-08: Gestión del licenciamiento de software y derechos de propiedad intelectual. Se evidenció que la Entidad no disponía de la totalidad de los soportes requeridos para acreditar el cumplimiento de los procedimientos relacionados con la protección de los derechos de propiedad intelectual del software utilizado. Esta situación incumple el control organizacional A.5.32 de la ISO/IEC 27001:2022. Se recomienda fortalecer la gestión de activos de software mediante la identificación, verificación, documentación y conservación de las evidencias de licenciamiento de las aplicaciones instaladas.	Baja
OCI-2026-ARL-52-09: Protección de equipos portátiles fuera de las instalaciones. Se evidenció que algunos equipos portátiles asignados para actividades fuera de las instalaciones institucionales no contaban con medidas de protección acordes con los riesgos asociados a su uso en entornos externos. Esta situación incumple el control físicos A.7.9 de la ISO/IEC 27001:2022. Se recomienda definir, documentar, implementar y verificar controles de seguridad para los equipos portátiles utilizados fuera de las instalaciones de la Entidad, de acuerdo con los riesgos identificados y la criticidad de la información procesada.	Baja
OCI-2026-ARL-52-10: Validación de la remediación de vulnerabilidades técnicas. Se evidenciaron debilidades en la validación y tratamiento de las vulnerabilidades técnicas, debido a la ausencia de evidencias que permitan confirmar el cierre efectivo de las vulnerabilidades críticas y la efectividad de las acciones implementadas. Esta situación incumple el control tecnológicos A.8.8 de la ISO/IEC 27001:2022. Se recomienda fortalecer el ciclo de gestión de vulnerabilidades técnicas mediante la incorporación en la documentación de las pruebas de validación (retest),	Baja
OCI-2026-ARL-52-11: Protección de datos mediante enmascaramiento. Se evidenció que las bases de datos en ambiente productivo de los sistemas de información SARA, SOFIA (Contabilidad), administradas sobre motor de base de datos Oracle, no contaban con mecanismos de enmascaramiento de datos. Esta situación incumple el control tecnológicos A.8.11 de la ISO/IEC 27001:2022. Se recomienda fortalecer la documentación incorporando los lineamientos y criterios para el enmascaramiento.	Baja
OCI-2026-ARL-52-12: Validación de copias de respaldo de la información. Se evidenciaron debilidades en la validación periódica de las copias de respaldo, debido a la falta de pruebas de restauración que permitan verificar su efectividad y capacidad de recuperación. Esta situación incumple el control tecnológicos A.8.13 de la ISO/IEC 27001:2022. Se recomienda fortalecer un cronograma formal de pruebas de restauración, con periodicidad definida, responsables, sistemas incluidos, resultados, tiempos de recuperación, entre otras.	Baja
OCI-2026-ARL-52-13: Deficiencia en el filtrado de servicios web externos de correo y almacenamiento en la nube. Se evidenciaron debilidades en los controles de filtrado y acceso a servicios externos de correo electrónico y almacenamiento en la nube, lo que puede aumentar la exposición a riesgos asociados a la protección de la información institucional. Esta situación incumple el control tecnológicos A.8.23 de la ISO/IEC 27001:2022. Se recomienda fortalecer los controles de filtrado web mediante la definición de criterios de acceso basados en necesidades operativas y análisis de riesgos, así como implementar mecanismos de monitoreo.	Baja

Oportunidades de Mejora y Recomendaciones

OM-2026-ARL-52-01: Formalización de la arquitectura de procesos institucional, relacionada con la incorporación del proceso "Est.3.1 Gobierno y Gestión TIC" dentro del Mapa de Procesos Institucional. De acuerdo con el Modelo Integrado de Planeación y Gestión (MIPG) y los lineamientos de gobernanza digital, resulta pertinente fortalecer la articulación estratégica de la gestión de las TIC dentro del modelo de operación institucional. ***Se recomienda*** *evaluar su clasificación como proceso estratégico y actualizar los instrumentos de gestión aplicables para fortalecer la gobernanza digital y la alineación estratégica de las capacidades tecnológicas institucionales.*

OM-2026-ARL-52-02: Formalización y actualización del acto administrativo de adopción de la Política de Seguridad de la Información, de conformidad con la cláusula 5.1 Liderazgo y compromiso y el control 5.1 Política de seguridad de la información de la ISO/IEC 27001:2022, cuya situación podría afectar la alineación con los requisitos vigentes del SGSI y la evidencia del compromiso de la Alta Dirección. ***Se recomienda*** *actualizar, publicar y comunicar el acto administrativo para fortalecer la gobernanza del SGSI, su apropiación institucional y la coherencia con los lineamientos vigentes de seguridad de la información.*

OM-2026-ARL-52-03: En la medición y seguimiento de las actividades de concientización en seguridad de la información, relacionada con la ausencia de indicadores y mecanismos para evaluar su efectividad, de acuerdo con lo establecido en la cláusula 7.3 Concientización y el control de Personas 6.3 Concientización, educación y capacitación en seguridad de la información de la ISO/IEC 27001:2022. ***Se recomienda*** *establecer un esquema de medición que permita evaluar la participación, cobertura, comprensión y apropiación de las buenas prácticas de seguridad de la información.*

OM-2026-ARL-52-04: Gestión de riesgos asociados a la implementación y sostenibilidad del MSPI, de conformidad con lo establecido en las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política de Gobierno Digital. ***Se recomienda*** *documentar e incorporar estos riesgos en el mapa institucional, definiendo mecanismos de seguimiento que permitan fortalecer la gobernanza de la seguridad y privacidad de la información.*

Conclusiones

De manera general, se evidenció que el MHCP ha adelantado acciones orientadas al cumplimiento de los requisitos establecidos en la Resolución 500 de 2021 del MinTIC, relacionados con la implementación de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).

*Como resultado de la evaluación realizada, se estableció que la Entidad alcanzó un nivel de madurez "**Optimizado**" en la implementación del MSPI, con una calificación promedio de **94** sobre 100, de acuerdo con la metodología establecida por MinTIC. Si bien la evaluación evidencia un nivel general de madurez optimizado en la implementación del MSPI y una adecuada alineación con la ISO/IEC 27001:2022, se identificaron aspectos específicos susceptibles de fortalecimiento. Estos no desconocen los avances del SGSI, sino que buscan consolidar su sostenibilidad, mejorar la evidencia de aplicación de controles y cerrar brechas puntuales frente a requisitos normativos, técnicos y documentales.*

En relación con la gestión de los riesgos asociados al proceso Est.3.1 Gobierno y Gestión TIC, durante el periodo evaluado, no se identificó materialización de los riesgos. No obstante, se identificó la oportunidad de fortalecer la gestión integral del riesgo mediante la incorporación de riesgos específicos relacionados con el cumplimiento de los lineamientos definidos para la implementación y sostenibilidad del MSPI, con el fin de robustecer los mecanismos de seguimiento y control sobre dichos requisitos.

Finalmente, como resultado de la presente actividad, se emitieron trece (13) observaciones relacionadas con: i) identificación y gestión de los requisitos de las partes interesadas del Sistema de Gestión de Seguridad de la Información (SGSI), ii) formalización de la Política de Seguridad de la Información del SGSI, iii) definición y seguimiento de los objetivos de seguridad de la información, iv) control de la información documentada del SGSI, v) documentación de las entradas de la revisión por la dirección del SGSI, vi) gestión y análisis de inteligencia de amenazas para la seguridad de la información, vii) controles de acceso a recursos externos de internet, viii) gestión del licenciamiento de software y los derechos de propiedad intelectual, ix) protección de equipos portátiles fuera de las instalaciones de la Entidad, x) validación de la remediación de vulnerabilidades técnicas, xi) implementación de controles de enmascaramiento de datos, xii) validación periódica de las copias de respaldo de la información y xiii) implementación de controles de filtrado y acceso a sitios web externos, las cuales requieren la suscripción de un plan de mejoramiento interno que se incluirá en el Sistema para el Monitoreo de la Gestión Integral – SMGI, con el fin de asegurar la implementación de las acciones correctivas y el seguimiento a su eficacia.

De igual manera, se identificaron cuatro (4) oportunidades de mejora relacionadas con: i) formalizar el proceso "Est.3.1 Gobierno y Gestión TIC" dentro de la arquitectura de procesos institucional, ii) actualizar, publicar y comunicar el acto administrativo de adopción de la Política de Seguridad de la Información, iii) fortalecer la documentación incorporando el esquema de medición y seguimiento para las actividades de concientización en seguridad de la información y iv)documentar e incorporar y formalizar en el mapa de riesgos del MHCP los factores de riesgos asociados a la implementación y sostenibilidad del MSPI. En tal sentido, se recomienda que los responsables analicen la pertinencia y viabilidad de estas.

Listado de siglas

MHCP: Ministerio de Hacienda y Crédito Público
MSPI: Modelo de Seguridad y Privacidad de la INformación.
OCI: Oficina de Control Interno
SCI: Sistema de Control Interno
SMGI: Sistema de Monitoreo de la Gestión Integral.
SGPI: Sistema de Gestión de Seguridad y Privacidad de la Información.

Sin observaciones: Se cumplieron los criterios evaluados.

Oportunidades de mejora: Debilidad identificada respecto a la optimización de la gestión.

Observaciones: Incumplimiento que requiere un plan de mejoramiento interno.