PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

Supersolidaria

Contenido

1. INTRODUCCIÓN

La Superintendencia de la Economía Solidaria, en cumplimiento de la Política de Gobierno Digital y los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), continúa fortaleciendo la gestión de la seguridad digital como un habilitador esencial para la operación institucional, la protección de los activos de información y la prestación de servicios públicos confiables y eficientes.

Durante la vigencia 2025 se avanzó significativamente en la actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) y en la alineación con la norma ISO/IEC 27001:2022, alcanzando los hitos previstos en el plan de seguridad de dicho periodo. Para 2026, y conforme a las directrices establecidas en la versión 5.0 del MSPI emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, la Entidad orientará sus esfuerzos a consolidar la madurez del modelo mediante la implementación progresiva de controles, la actualización documental y el fortalecimiento de la cultura institucional de seguridad.

El presente Plan de Seguridad y Privacidad de la Información 2026 define las actividades, metas y mecanismos de seguimiento necesarios para avanzar hacia el cumplimiento del 60% de implementación del MSPI, garantizando el cumplimiento normativo, la mitigación de riesgos digitales, la protección de la información y la mejora continua de las prácticas institucionales en materia de seguridad y privacidad de la información.

2. ANTECEDENTES

El diagnóstico realizado en 2025 evidenció avances importantes en materia de gobierno, políticas, capacitación y estandarización de controles. No obstante, la actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) a su versión 5.0 introduce nuevas exigencias para la Entidad, especialmente en aspectos como el reforzamiento de la gestión de riesgos digitales, la consolidación del inventario y clasificación de los activos de información, la actualización del ciclo documental en materia de seguridad, la incorporación de lineamientos de desarrollo seguro en los sistemas institucionales y el fortalecimiento de las capacidades de sensibilización y cultura organizacional. Así mismo, se requiere avanzar en mecanismos de monitoreo continuo de amenazas, reputación digital e incidentes que puedan afectar la operación.

De acuerdo con el documento oficial del MSPI v5.0 del MinTIC, la implementación del modelo se desarrolla bajo un ciclo PHVA (Planear–Hacer–Verificar–Actuar), soportado en evidencia documental, controles aplicados, seguimiento a actividades y apropiación institucional por parte de los responsables y propietarios de procesos. Esto implica que la Entidad debe continuar estructurando y priorizando acciones que respondan a su contexto, riesgos y nivel de madurez.

En este escenario, la matriz de actividades definida para la vigencia 2026 se configura como una hoja de ruta estratégica orientada a cerrar brechas identificadas, fortalecer la gobernanza y gestión institucional en materia de seguridad digital y avanzar hacia el cumplimiento de la meta del 60% de implementación del MSPI, en coherencia con los lineamientos del PETI – Proyecto 02 - Seguridad de la Información.

3. OBJETIVO

Fortalecer el Modelo de Seguridad y Privacidad de la Información (MSPI v5.0) mediante la implementación progresiva de controles, actualización documental, desarrollo de capacidades y gestión integral de riesgos, con el propósito de alcanzar una meta institucional del 60% de implementación del modelo en la vigencia 2026.

4. OBJETIVOS ESPECÍFICOS

1. Actualizar y aplicar el instrumento de autodiagnóstico MSPI conforme a los lineamientos del MinTIC y a los requisitos de la ISO/IEC 27001:2022.
2. Elaborar, actualizar y formalizar el Manual de Seguridad de la Información, integrando los capítulos de liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora continua.
3. Mantener vigente el marco normativo interno mediante la actualización, aprobación y divulgación de las políticas de seguridad de la información.
4. Fortalecer la gestión de activos de información, garantizando inventarios actualizados, uso aceptable y trazabilidad con el mapa de riesgos.
5. Consolidar la cultura organizacional de seguridad mediante campañas, charlas y ejercicios de ingeniería social.
6. Formalizar y aplicar lineamientos de desarrollo seguro en los sistemas de información institucionales.
7. Ejecutar actividades de monitoreo permanente de amenazas, vulnerabilidades e identidad digital.
8. Medir el desempeño del MSPI mediante indicadores institucionales de madurez, activos y sensibilización.

5. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información 2026 comprende las acciones necesarias para avanzar en la implementación del MSPI v5.0 y fortalecer la gestión institucional de seguridad digital, orientadas al cumplimiento de la meta del 60% de implementación establecida para la vigencia.

En este marco, el plan incluye la actualización del instrumento de autodiagnóstico y la identificación de brechas, permitiendo definir prioridades y orientar las acciones de mejora. Así mismo, contempla la elaboración y formalización del Manual de Seguridad de la Información, consolidando los lineamientos institucionales en materia de liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora.

El alcance incorpora la actualización, aprobación y divulgación de las políticas de seguridad, garantizando directrices vigentes y aplicables a todos los procesos de la Entidad. También se desarrollarán actividades para mantener actualizado el inventario de activos de información y formalizar su uso aceptable, reforzando la adecuada gestión y protección de estos recursos críticos.

De igual manera, se ejecutará un programa de sensibilización que comprende campañas, charlas y ejercicios prácticos orientados a fortalecer la cultura de seguridad digital. En cuanto al componente técnico, el plan incluye la formalización y aplicación de lineamientos de desarrollo seguro en los sistemas institucionales.

El plan considera además acciones de monitoreo permanente de vulnerabilidades, riesgos reputacionales y eventos de seguridad, con el fin de fortalecer la capacidad de detección, prevención y respuesta de la Entidad. Finalmente, se realizará el seguimiento a los indicadores de madurez, activos y sensibilización, permitiendo evaluar el avance del MSPI y orientar la mejora continua del modelo.

6. PLAN DE ACTIVIDADES 2026

No	ACTIVIDAD	ENTREGABLES / HITOS	INICIO	FIN
1. Autodiagnóstico Seguridad.				
1.1	Actualizar instrumento MSPI versión 27001:2022	Instrumento Actualizado	15/01/26	28/02/26
1.2	Identificación Brechas	Documento alcance Brechas a cerrar vigencia 2026	15/01/26	28/02/26
1.3	Aprobación Instrumento	Aprobación Comités CIGD	01/02/26	30/04/26
2. Manual de Seguridad.				
2.1	Elaboración capítulos 5 liderazgo y 6 Planificación	Documento con capítulos 5 y 6	01/03/26	30/03/26
2.2	Elaboración capítulos 7 Soporte y 8 Operación	Documento con capítulos 7 y 8	01/04/26	30/04/26
2.3	Elaboración capítulos 9 evaluación del Desempeño y 10 Mejora	Documento con capítulos 9 y 10	01/05/26	30/05/26
2.4	Formalización Manual de Seguridad	Manual de Seguridad	01/06/26	30/06/26
3. Políticas de Seguridad.				
3.1	Actualización Políticas de Seguridad	Políticas Actualizadas	15/02/26	15/03/26
3.2	Divulgación Políticas con responsables	Políticas Aprobadas por responsables	01/04/26	30/05/26
3.3	Aprobación Políticas	Políticas aprobadas por el Comité CIGD	01/06/26	30/07/26
4. Activos de Información.				
4.1	Actualización Activos de Información	Matriz Actualizada	01/02/26	30/09/26
4.2	Uso Aceptable Activos de Información	Documento formalizado	01/08/26	30/09/26
5. Sensibilización Seguridad.				
5.1	30 campañas jueves Seguro	30 campañas	15/01/26	15/12/26
5.2	Charlas de Seguridad	3 charlas gestionadas	15/01/26	15/12/26
5.3	Ejercicio Ingeniería Social	1 ejercicio gestionado	01/10/26	30/11/26
6. Desarrollo Seguro.				
6.1	Documento Desarrollo Seguro	Formalización Documento	01/03/26	30/05/26
6.2	Aplicación Lineamientos Desarrollo Seguro	Documento con verificación aplicada lineamientos	01/06/26	30/11/26
7. Monitoreo Seguridad.				
7.1	Análisis de Vulnerabilidades (ethical hacking)	Documento con Resultados	01/03/26	30/11/26
7.2	Monitoreo Seguridad	Informes con resultados	01/03/26	30/11/26
8. Indicadores Seguridad.				
8.1	Madurez MSPI	Indicador Reportado	15/01/26	31/12/26
8.2	Activos de Información	Indicador Reportado	15/01/26	31/12/26
8.3	Sensibilización Seguridad	Indicador Reportado	15/01/26	31/12/26

7. SEGUIMIENTO AL PLAN

El avance del Plan de Seguridad y Privacidad de la Información se medirá a través del Plan de Acción Institucional para la vigencia 2026, en donde se presentará el cumplimiento de las actividades programadas para la vigencia, así como el grado de implementación del MSPI v5.0.

El seguimiento se realizará de manera trimestral y permitirá establecer el progreso real del plan, así como tomar decisiones informadas frente a ajustes o acciones complementarias que se requieran durante la vigencia.

Complementos de seguimiento:

- Revisión bimestral del avance en el Comité Institucional de Gestión y Desempeño (CIGD).
- Reporte trimestral al CIGD sobre avances, riesgos y actividades críticas.
- Evaluación semestral del Mapa de Riesgos de Seguridad Digital.
- Seguimiento anual al indicador de madurez del MSPI para determinar el nivel de implementación alcanzado frente a la meta del 60%.

8. GESTIÓN DE CAMBIOS

La gestión de cambios del Plan de Seguridad y Privacidad de la Información 2026 garantiza que cualquier ajuste requerido se evalúe y aplique de manera controlada, oportuna y en coherencia con los lineamientos del MSPI v5.0. Este proceso inicia con la identificación de nuevas necesidades derivadas de auditorías internas o externas, actualizaciones normativas, incidentes de seguridad o cambios en el contexto institucional, determinando su impacto en las actividades y compromisos establecidos en el plan.

Una vez identificada la necesidad de cambio, ésta será sometida a revisión y aprobación por el Comité Institucional de Gestión y Desempeño (CIGD), instancia responsable de validar su pertinencia, definir las acciones correspondientes y dejar constancia formal mediante acta. Con la aprobación del comité, se procederá a implementar el cambio, lo que incluye la actualización de los documentos que sean necesarios —como políticas, lineamientos, manuales, procedimientos o matrices— y la socialización de los ajustes con los responsables involucrados.

Finalmente, se llevará a cabo la verificación del cambio implementado, con el fin de confirmar su correcta aplicación y registrar las modificaciones en el repositorio documental institucional. Este proceso contribuye a mantener la coherencia, trazabilidad y mejora continua del Plan de Seguridad y Privacidad de la Información durante la vigencia 2026.