PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

2026

Supersolidaria

Contenido

1. INTRODUCCIÓN

La gestión de riesgos de seguridad de la información es un componente fundamental del Modelo de Seguridad y Privacidad de la Información (MSPI), en su versión 5.0 emitida por el MinTIC. Para la vigencia 2026, la Superintendencia de la Economía Solidaria orientará sus esfuerzos a fortalecer los mecanismos institucionales de identificación, análisis, valoración y seguimiento de riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

El presente Plan de Riesgos de Seguridad de la Información 2026 compila las actividades, metas y entregables orientados a mejorar la identificación de amenazas, el seguimiento a controles, la gestión de incidentes y la consolidación de capacidades técnicas que soporten la prevención y mitigación de riesgos digitales en la Entidad.

2. ANTECEDENTES

Durante 2025, la Entidad avanzó en procesos de estandarización de controles, fortalecimiento de políticas y actividades de monitoreo. Sin embargo, la actualización del MSPI v5.0 establece la necesidad de adoptar un enfoque más robusto de gestión de riesgos, en el cual se priorice la trazabilidad, el seguimiento continuo y la integración con las actividades misionales.

En este contexto, el PETI – Proyecto 02 Seguridad de la Información y los lineamientos institucionales definen la importancia de contar con un plan específico para el tratamiento y gestión de riesgos, que incluya acciones de identificación, seguimiento de controles, análisis técnico y articulación con los procesos de incidentes de seguridad.

Este plan constituye una hoja de ruta para fortalecer la madurez institucional en materia de riesgos de seguridad de la información y garantizar el cumplimiento de los lineamientos establecidos por el MinTIC en el MSPI v5.0.

3. OBJETIVO

Fortalecer la gestión institucional de riesgos de seguridad de la información mediante la identificación, análisis, seguimiento y reporte de riesgos, controles y amenazas, en coherencia con los lineamientos del MSPI v5.0 y con el fin de reducir la probabilidad e impacto de eventos de seguridad que puedan afectar la operación de la Entidad durante la vigencia 2026.

4. OBJETIVOS ESPECÍFICOS

- Identificar los riesgos de seguridad de la información presentes en los procesos misionales y de apoyo.
- Realizar seguimiento periódico a la aplicación de controles de seguridad registrados en la plataforma institucional.
- Evaluar riesgos e incidentes mediante indicadores institucionales y reportes periódicos.
- Fortalecer la capacidad de gestión de incidentes mediante reportes sistemáticos y trazables.
- Desarrollar análisis técnicos de vulnerabilidades, exposición de marca y monitoreo de seguridad para identificar amenazas emergentes.
- Ejecutar actividades de sensibilización orientadas a la reducción de riesgos asociados al factor humano.

5. ALCANCE

El Plan de Riesgos de Seguridad de la Información 2026 abarca las actividades relacionadas con la identificación, seguimiento, análisis y reporte de riesgos, así como la ejecución de controles técnicos, la gestión de incidentes y las acciones de sensibilización institucional.

Incluye la actualización de riesgos asociados a procesos misionales, el seguimiento a la aplicación de controles registrados en la plataforma institucional PABLO, la generación de indicadores asociados a riesgos e incidentes, la elaboración de análisis técnicos de vulnerabilidades y marca digital, y la ejecución de un ejercicio de ingeniería social como mecanismo de evaluación de la cultura de seguridad.

6. PLAN DE ACTIVIDADES 2026

No	ACTIVIDAD	ENTREGABLES / HITOS	INICIO	FIN
1. Riesgos.				
1.1	Seguimiento aplicación controles	Reporte en plataforma Pablo	15/01/26	31/12/26
1.2	Identificación Riesgos Procesos Misionales	Documento alcance Brechas a cerrar vigencia 2026	01/03/26	30/09/26
2. Indicadores.				
2.1	Riesgos	Indicador Reportado	15/01/26	31/12/26
2.2	Incidentes	Indicador Reportado	15/01/26	31/12/26
3. Incidentes Seguridad				
3.1	Gestión Incidentes	Reporte Incidentes de Seguridad	15/01/26	31/12/26
4. Controles Técnicos.				
4.1	Análisis de Vulnerabilidades	Documento con Resultados	01/03/26	30/11/26
4.2	Análisis de Marca	Documento con Resultados	01/03/26	30/11/26
4.3	Monitoreo Seguridad	Informes con resultados	01/03/26	30/11/26
5. Sensibilización Seguridad.				
5.1	Ejercicio Ingeniería Social	1 Ejercicio gestionado	01/10/26	30/11/26

7. SEGUIMIENTO AL PLAN

El avance del Plan de Riesgos de Seguridad 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.

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.

8. GESTIÓN DE CAMBIOS

Los cambios asociados al Plan de Riesgos de Seguridad de la Información se evaluarán y aprobarán conforme a las necesidades operativas, auditorías, actualizaciones normativas e incidentes que surjan durante la vigencia. Cualquier modificación al alcance, cronograma o actividades deberá ser revisada y aprobada por el Comité Institucional de Gestión y Desempeño (CIGD), y posteriormente registrada en el repositorio documental institucional.