PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2025

Superintendencia de la Economía Solidaria
Avenida Calle 24 (Esperanza) N° 60-50 Piso 8 Centro Empresarial Gran Estación
PBX: (+57)(601)7 560 557
Línea Gratis: 018000-180-430

Contenido

Superintendencia de la Economía Solidaria
Avenida Calle 24 (Esperanza) N° 60-50 Piso 8 Centro Empresarial Gran Estación
PBX: (+57)(601)7 560 557
Línea Gratis: 018000-180-430

1. INTRODUCCIÓN

La Superintendencia de la Economía Solidaria mediante la Resolución 2024120007655 de 2024 adopta el Modelo Integrado de Planeación y Gestión indicando que es “el marco de referencia que permite dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de la entidad” (art. 1)

Así mismo, ratifica que la implementación del Modelo Integrado de Planeación y Gestión tiene el fin de “generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad del servicio” (art. 2); por lo que para esto, el cumplimiento de la política de gobierno digital en la dimensión de gestión con valores para el resultado es fundamental.

En este sentido, y en cumplimiento de los lineamientos establecidos en la resolución 500 de 2021 del Ministerio de Tecnologías de la Información (MINTIC), “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”, el presente Plan de Seguridad y Privacidad de la Información tiene como propósito fortalecer las capacidades organizacionales en gestión de riesgos y protección de la información, así como plantear las actividades que permitan el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), en el marco de la normatividad vigente.

El enfoque estratégico incluye la homologación de controles hacia la versión 2022 de la norma ISO/IEC 27001, la mejora continua en gestión de riesgos y seguridad de la información, y la promoción de una cultura organizacional de seguridad. Lo anterior, con el objetivo de alcanzar un 70% de cumplimiento del MSPI y garantizar la integración con los objetivos estratégicos gubernamentales.

Superintendencia de la Economía Solidaria
Avenida Calle 24 (Esperanza) N° 60-50 Piso 8 Centro Empresarial Gran Estación
PBX: (+57)(601)7 560 557
Línea Gratis: 018000-180-430

2. ANTECEDENTES

El análisis de brechas realizado para la vigencia 2024, a partir del autodiagnóstico de la implementación del MSPI, se revela un promedio general de efectividad de controles del 60%, destacando importantes avances y áreas por fortalecer. Entre los logros más significativos, el cumplimiento total en **Políticas de seguridad de la información** (100%) refleja un sólido compromiso en este ámbito. Sin embargo, otros dominios, como la **Organización de la seguridad de la información** (32%) y los **Aspectos de la continuidad del negocio** (30%), requieren un enfoque estratégico más profundo.

En este contexto, la Superintendencia de la Economía Solidaria ha reconocido la importancia de la información y los datos como activos estratégicos y en respuesta a ello, se han implementado diversas iniciativas en materia de seguridad de la información, entre las cuales se destacan:

1. **Adopción del Modelo de Seguridad y Privacidad de la Información (MSPI):** Este modelo pertenece al habilitador transversal de Seguridad y Privacidad de la Política de la Política de Gobierno Digital. Este modelo ha orientado las acciones organizacionales en materia de seguridad y privacidad de la información de la entidad.
2. **Cumplimiento de normativas gubernamentales:** La entidad ahondó sus esfuerzos para la articulación del MSPI con la Política de Gobierno Digital y las directrices del Decreto 612 de 2018, es así que el Modelo de Seguridad y Privacidad de la Información hace parte del portafolio de proyectos del Plan Estratégico de Tecnologías de la Información - PETI.
3. **Actualización hacia ISO/IEC 27001:** Se han realizado esfuerzos para homologar los controles de la norma ISO/IEC 27001:2013 y avanzar hacia su versión 2022, donde se realizó un diagnóstico inicial de brechas, entre lo implementado vs los cambios de la norma, lo cual permitió establecer el plan de trabajo para la vigencia 2025, donde se estructurará el Modelo de Seguridad de la Información (MSPI).
4. **Fomento de una cultura de seguridad:** Se conformó el comité de Seguridad y Privacidad de la información, actualización de la documentación del modelo, así como campañas de concienciación y capacitación, donde se buscó fortalecer las competencias del personal frente a los riesgos y amenazas cibernéticas.

Superintendencia de la Economía Solidaria
Avenida Calle 24 (Esperanza) N° 60-50 Piso 8 Centro Empresarial Gran Estación
PBX: (+57)(601)7 560 557
Línea Gratis: 018000-180-430

5. **Fortalecimiento del Plan de Continuidad del Negocio (PCN)**

   Se debe Implementar y mantener el Plan de Continuidad del Negocio (PCN) que permita garantizar la operación continua de los procesos críticos de la Superintendencia de la Economía Solidaria ante eventos disruptivos, alineado con los estándares de la ISO 22301 y en sinergia con los objetivos del MSPI 2025.

Así mismo y aunque se han registrado ligeros avances en áreas como la **Seguridad de los recursos humanos** (+2%) es necesario establecer esfuerzos para el fortalecimiento de este campo, también se evidencian retrocesos significativos, especialmente en "Relaciones con los proveedores" (-20%) y **Aspectos de la continuidad del negocio** (-16.5%). Estos resultados resaltan la necesidad de priorizar esfuerzos para alinear el modelo con los objetivos establecidos en el plan de seguridad y privacidad de la información 2025.

Estas acciones han sentado las bases para la elaboración del presente plan, que busca consolidar y mejorar las capacidades existentes.

Superintendencia de la Economía Solidaria
Avenida Calle 24 (Esperanza) N° 60-50 Piso 8 Centro Empresarial Gran Estación
PBX: (+57)(601)7 560 557
Línea Gratis: 018000-180-430

3. OBJETIVO

Fortalecer el Modelo de Seguridad y Privacidad de la Información con un cumplimiento del 70% al 2025.

4. OBJETIVOS ESPECÍFICOS

1. **Actualizar el MSPI conforme a estándares internacionales:** garantizando la homologación de los controles de la norma ISO/IEC 27001:2013 a la versión ISO/IEC 27001:2022, y fortaleciendo la estructura del sistema de gestión de la seguridad de la información.
2. **Asegurar el cumplimiento de la normativa nacional,** mediante la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en concordancia con leyes como la Ley 1581 de 2012, el Decreto 1078 de 2015 y la Circular 003 de 2017, promoviendo un marco de gestión de seguridad alineado a los requisitos legales.
3. **Fortalecer la seguridad organizacional**, mediante la aplicación de controles críticos y prioritarios que mitiguen los riesgos asociados a los activos de información, garantizando su confidencialidad, integridad y disponibilidad.
4. **Optimizar la gestión de riesgos**, a través de la identificación y tratamiento de vulnerabilidades con herramientas y ejercicios especializados como ethical hacking, auditorías internas y la gestión continua de activos de información.
5. **Incrementar la concienciación y capacitación de los colaboradores**, mediante la implementación de una estrategia de divulgación, apropiación y transferencias de conocimiento en seguridad de la información que fomenten la participación y preparen al equipo para enfrentar posibles amenazas.
6. **Monitorear y auditar el desempeño del MSPI**, a través de mecanismos efectivos para el seguimiento continuo, la evaluación de resultados y la implementación de ajustes mediante auditorías internas y análisis periódicos.

Superintendencia de la Economía Solidaria
Avenida Calle 24 (Esperanza) N° 60-50 Piso 8 Centro Empresarial Gran Estación
PBX: (+57)(601)7 560 557
Línea Gratis: 018000-180-430

5. ALCANCE

El alcance del presente plan está centrado en el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), abarcando las siguientes dimensiones:

1. **Homologación de Controles:** Adaptar los controles actuales de la ISO/IEC 27001:2013 a la versión ISO/IEC 27001:2022, asegurando la actualización y alineación con estándares internacionales vigentes.
2. **Declaración de Aplicabilidad:** Implementar y priorizar los controles establecidos en la Declaración de Aplicabilidad, garantizando que los recursos se concentren en los puntos más críticos de seguridad.
3. **Capacitación del Personal:** Sensibilizar a los colaboradores sobre las políticas y procedimientos del SGSI, fomentando una cultura de seguridad alineada con el MSPI.
4. **Gestión de Riesgos:** Identificar, analizar y tratar los riesgos asociados a los activos de información mediante el seguimiento continuo a través del Mapa de Riesgos de Seguridad Digital, el cual permite priorizar las vulnerabilidades y definir estrategias de mitigación. Este proceso se complementa con la realización de inventarios periódicos, auditorías internas y ejercicios de ethical hacking, asegurando una gestión proactiva y efectiva de los riesgos.
5. **Respuesta a Incidentes:** Establecer procedimientos efectivos de gestión de incidentes que incluyan simulacros y validaciones regulares de los planes establecidos.

Superintendencia de la Economía Solidaria
Avenida Calle 24 (Esperanza) N° 60-50 Piso 8 Centro Empresarial Gran Estación
PBX: (+57)(601)7 560 557
Línea Gratis: 018000-180-430

6. PLAN DE ACTIVIDADES

Este Plan de Actividades está diseñado con tareas clave y entregables específicos para reforzar el MSPI. Comprende acciones como la actualización de estándares, la gestión de riesgos, la capacitación y el fortalecimiento de la continuidad del negocio, asegurando la protección de los activos de información y el logro de los objetivos estratégicos de 2025.

NÚMERO EDT	TÍTULO DE LA TAREA	ENTREGABLES / HITOS	FECHA DE INICIO	FECHA DE ENTREGA
1	**Actualizar el MSPI conforme a estándares internacionales**			
1.1	Homologar controles de la norma ISO/IEC 27001:2013 a la versión ISO/IEC 27001:2022	Controles actualizados y alineados con la versión 2022 de la norma.	15/01/25	31/03/25
1.2	Revisar y actualizar la Declaración de Aplicabilidad (SoA)	Documento actualizado con controles implementados.	01/03/25	30/04/25
2	**Asegurar el cumplimiento de la normativa nacional**			
2.1	Revisar la normativa nacional aplicable (Ley 1581, Decreto 1078, Circular 003)	Informe de brechas y plan de acción para cumplimiento normativo.	01/02/25	31/03/25
2.2	Actualizar políticas de seguridad alineadas al MSPI	Políticas revisadas y aprobadas por el Comité de Seguridad.	01/04/25	30/06/25
3	**Fortalecer la seguridad organizacional**			
3.1	Implementar controles prioritarios según análisis de riesgos	Evidencias de controles aplicados.	01/03/25	31/10/25
3.2	Realizar pruebas de vulnerabilidad y penetración (ethical hacking)	Informes con hallazgos y recomendaciones.	01/06/25	31/07/25
4	**Optimizar la gestión de riesgos**			
4.1	Identificar activos de información y actualizar su inventario	Inventarios actualizados y aprobados.	01/04/25	30/06/25
4.2	Evaluar y aprobar los riesgos asociados a los activos	Mapa de riesgos actualizado con planes de mitigación.	01/04/25	30/05/25
5	**Incrementar la concienciación y capacitación de los colaboradores**			
5.1	Definir temáticas de capacitación	Lista de temáticas prioritarias en seguridad de la información.	15/01/25	28/02/25
5.2	Preparar materiales de formación	Materiales listos para impartir.	01/02/25	31/03/25
5.3	Realizar sesiones de capacitación	Registro de capacitaciones, asistencia y participación activa.	01/03/25	28/11/25
5.4	Evaluar el impacto de la capacitación	Informe de resultados de encuestas y pruebas.	01/03/25	28/11/25
6	**Monitorear y auditar el desempeño del MSPI**			
6.1	Establecer métricas y tableros de control	Tableros de control implementados para seguimiento continuo.	01/04/25	30/06/25
6.2	Realizar simulacros del plan de respuesta a incidentes	Informe de simulacros realizados y ajustes al plan.	01/10/25	28/11/25
7	**Fortalecimiento del Plan de Continuidad del Negocio (PCN)**			
7.1	Análisis de Impacto al Negocio (BIA)	Informe de Análisis de Impacto al Negocio (BIA)	01/04/25	30/06/25
7.2	Gestión de Riesgos de Continuidad	Matriz de Riesgos Operativos y Plan de Mitigación	01/04/25	30/06/25
7.3	Diseño del Plan de Continuidad del Negocio	Manual de Procedimientos de Respuesta y Restauración Operativa	01/04/25	30/06/25

7. MEDICIÓN Y SEGUIMIENTO

El Avance implementación del Plan de Seguridad y Privacidad de la Información (%) es un indicador clave para medir el progreso en la implementación de las actividades establecidas en el Plan de Trabajo. Este indicador se calcula utilizando la siguiente fórmula:

$$\text{Avance del Cronograma (\%)} = \left(\frac{\text{Número de actividades completadas}}{\text{Número total de actividades planificadas}} \right) \times 100$$

- Número de actividades completadas: Cantidad de actividades del cronograma que han sido finalizadas satisfactoriamente en el periodo.
- Número total de actividades planificadas: Total de actividades programadas para el mismo periodo.

Por otra parte, se realizarán diferentes actividades para medir la percepción y cultura en la entidad, actividades entre las cuales se destacan:

Superintendencia de la Economía Solidaria
Avenida Calle 24 (Esperanza) N° 60-50 Piso 8 Centro Empresarial Gran Estación
PBX: (+57)(601)7 560 557
Línea Gratis: 018000-180-430

- Realizar encuestas regulares a los colaboradores para evaluar su nivel de conocimiento y percepción sobre las políticas de seguridad.
- Realizar seguimiento al Mapa de Riesgos de Seguridad Digital semestralmente.
- Fortalecer en función de los resultados obtenidos en la medición del impacto del modelo de seguridad y privacidad.

8. GESTIÓN DE CAMBIOS

La gestión de cambios es esencial para mantener la relevancia y efectividad del Plan de Seguridad de la Información y Privacidad de la Información ante un entorno dinámico. Esta sección detalla los procedimientos para evaluar, aprobar e implementar modificaciones al plan de seguridad y privacidad de la información.

1. **Evaluación de cambios:**
   - Identificar la necesidad de cambios debido a nuevas normativas, amenazas emergentes o resultados de auditorías.
   - Analizar el impacto potencial de los cambios en los objetivos y recursos disponibles.
2. **Aprobación de cambios:**
   - Someter las propuestas al Comité de Seguridad y Privacidad de la Información para su validación.
   - Documentar las decisiones tomadas, incluyendo justificaciones y responsables.
3. **Implementación de cambios:**
   - Asignar responsables para ejecutar las modificaciones aprobadas.
   - Actualizar documentos relacionados, como políticas, procedimientos y cronogramas.
4. **Seguimiento y documentación:**
   - Realizar un seguimiento periódico de los cambios implementados para asegurar su efectividad.
   - Mantener un registro actualizado de todos los cambios realizados al plan.

Superintendencia de la Economía Solidaria
Avenida Calle 24 (Esperanza) N° 60-50 Piso 8 Centro Empresarial Gran Estación
PBX: (+57)(601)7 560 557
Línea Gratis: 018000-180-430