Superintendencia de Industria y Comercio

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

Superintendencia de Industria y Comercio

Enero 2025

CONTENIDO

NOMBRE DEL DOCUMENTO	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
VIGENCIA	2025	
CREADO POR	Grupo de Trabajo de Informática Forense y Seguridad Digital	Fecha: Enero, 2025
REVISADO POR	Oscar Fabian Ramírez Torres Oficial de Seguridad rol asumido por el Coordinador Grupo de Trabajo de Informática Forense y Seguridad Digital	Fecha: Enero, 2025
APROBADO POR	Oscar Fabian Ramírez Torres Oficial de Seguridad rol asumido por el Coordinador Grupo de Trabajo de Informática Forense y Seguridad Digital	Fecha: Enero, 2025

CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio

1.0	Enero de 2025	Creación del documento

1 INTRODUCCION

De acuerdo con lo estipulado en el numeral 2.1.3 del Manual de Gobierno Digital, el plan de seguridad y privacidad de la información establece los detalles de cómo se realizará la implementación y mejora de la seguridad de la información en la Entidad para cada vigencia, estipulando directrices, tiempos y responsables, de tal forma que se logren resultados anuales mejores que en la vigencia anterior.

Es de anotar que, en anteriores vigencias la SIC ha desarrollado proyectos que han permitido acceder, entre otros, a los siguientes beneficios:

- Contar con metodologías para la identificación y clasificación de activos, gestión de riesgos e incidentes de seguridad de la información.
- Contar con políticas de seguridad de la información.
- Fortalecer la conciencia en cuanto a las amenazas y riesgos en el ciberespacio a los que se enfrentan los colaboradores en sus labores diarias.
- Implementación de controles del Sistema de Gestión de Seguridad de la Información – SGSI.
- Establecer un proceso estratégico cuyo objetivo es proteger la información institucional.
- Contar con procedimientos, instructivos y formatos que orientan la gestión del SGSI.
- Identificar riesgos que pueden afectar la seguridad de la información en los procesos de la Entidad.
- Establecer controles para asegurar las aplicaciones cuya infraestructura se encuentra alojada en la nube.
- Implementación del BIA y DRP para las aplicaciones críticas de la Entidad.
- Gestión de Vulnerabilidades técnicas.

2 OBJETIVO

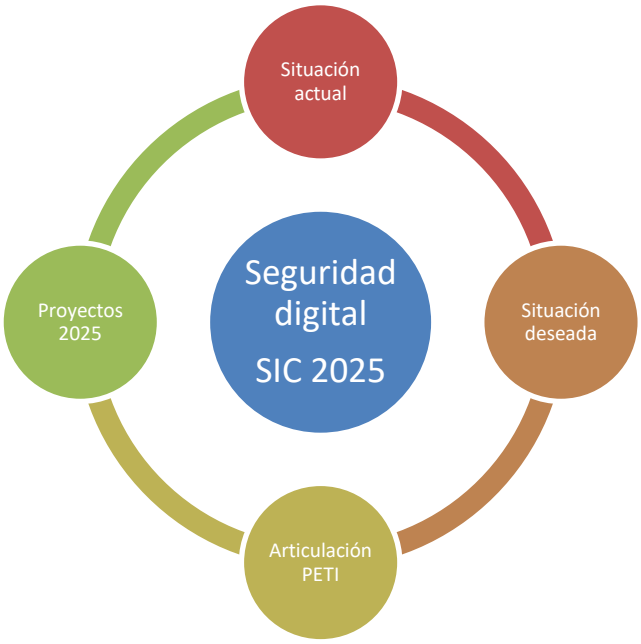
Establecer las acciones estratégicas tendientes a fortalecer la seguridad y privacidad de la información en la Superintendencia de Industria y Comercio - SIC, mediante la planeación de actividades para la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI de la Entidad para la vigencia 2025.

3 ALCANCE

El presente documento se encuentra articulado con el plan de acción institucional para el año 2025, Plan de Tratamiento de Riesgos de Seguridad de la Información y Plan Estratégico de Tecnologías de Información (PETI 2023-2026).

4 METODOLOGÍA

Para definir los proyectos del presente plan se analizó la situación actual vs la deseada, buscando en todo momento una alineación con el PETI. El resumen de la metodología se muestra a continuación:



4.1 SITUACIÓN ACTUAL

Respecto a los resultados del MIPG del año 2024, se encontró que para la vigencia 2025 es necesario atender las siguientes recomendaciones:

- Fortalecer las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de socialización y promoción del uso del modelo de gestión de riesgos de seguridad digital convocadas por el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como registrarse en el CSIRT Gobierno y/o ColCERT.
- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC.
- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la construcción de los planes sectoriales de protección de la infraestructura crítica cibernética.

Así mismo, en el análisis de brechas del Modelo de Seguridad y Privacidad de la Información – MSPI realizado en 2025, se obtuvo el siguiente resultado:

De la gráfica anterior, se identifican aspectos por mejorar en los siguientes controles de seguridad de la información:

ITEM	DESCRIPCIÓN	ISO
Revisión de las políticas para la seguridad de la información	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	A.5.1.2
Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de la información adoptado por la organización.	A.8.2.2
Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	A.10.1.2
Respaldo de la información	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	A.12.3.1
Registro de eventos	Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	A.12.4.1
Aprendizaje obtenido de los incidentes de seguridad de la información	Se debe entender cuál fue el impacto del incidente. Las lecciones aprendidas deben ser usadas para actualizar los planes de respuesta a los incidentes de SI.	A.16.1.6
Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	A.17.1.3
Protección y privacidad de la información de carácter personal	Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.	A.18.1.4

Reglamentación de controles criptográficos	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	A.18.1.5

4.2 SITUACIÓN DESEADA

La dirección de la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO (SIC), entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Para la SIC, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

El SGSI debe cumplir con las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la SIC.
- Garantizar la continuidad del negocio frente a incidentes.
- La SIC ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de la SIC:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- La SIC protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- La SIC protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La SIC protegerá su información de las amenazas originadas por parte del personal.
- La SIC protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La SIC controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La SIC implementará control de acceso a la información, sistemas y recursos de red.
- La SIC garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La SIC garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La SIC garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La SIC garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

4.3 ANÁLISIS PETI

El Sistema de Gestión de Seguridad de la Información (SGSI) es un componente fundamental para el éxito de cualquier iniciativa relacionada con Tecnologías de la Información (TI). Su apoyo es crucial en el logro de los objetivos y necesidades de TI, especialmente en proyectos como la implementación de la política digital. En este contexto, el SGSI debe asegurar la integridad, confidencialidad y disponibilidad de la información digitalizada, garantizando el cumplimiento de normativas y estándares de seguridad. Además, en la modernización del ecosistema de aplicaciones, el SGSI desempeña un papel esencial al evaluar y mitigar los riesgos asociados con la integración de nuevas tecnologías y la gestión de datos. Asimismo, en el mejoramiento y evolución de los servicios tecnológicos, el SGSI contribuye al diseño e implementación de controles de seguridad efectivos para proteger los activos de información y mantener la continuidad del negocio. Finalmente, en el fortalecimiento de capacidades de ciberseguridad, el SGSI lidera la identificación proactiva de amenazas, la respuesta a incidentes y la formación del personal en buenas prácticas de seguridad, fortaleciendo así la postura de seguridad de la Entidad en un entorno digital cada vez más complejo y dinámico.

5 PROYECTOS ESPECIFICOS 2025

Teniendo en cuenta el análisis previo, para la vigencia 2025 se ejecutarán los siguientes proyectos de seguridad de la información.

1. Implementar un Centro de Operaciones de Seguridad (SOC) propio de la SIC.
2. Diseñar de un equipo de respuesta ante emergencias informáticas CSIRT para protección de datos personales en la SIC
3. Fortalecer las debilidades en la gestión de incidentes de seguridad, según el análisis de brechas y la auditoría interna.
4. Formular el programa de capacitación y sensibilización en seguridad de la información
5. Fortalecer controles de seguridad de la información, según el análisis de brechas y la auditoría interna
6. Implementar las estrategias de recuperación ante Desastres.
7. Fortalecer debilidades en la identificación de riesgos de nube pública, según el resultado del FURAG.
8. Fortalecer estrategias en auditoría de proveedores
9. Fortalecer debilidades en la identificación de activos de información, según el análisis de brechas y la auditoría interna.

10. Apoyar la implementación del Programa Integral de Protección de Datos Personales.

A continuación, se detalla el alcance de cada proyecto:

Nombre	**Implementar un Centro de Operaciones de Seguridad (SOC) propio de la SIC.**
Descripción	El objetivo principal del proyecto es diseñar, implementar y operar un Centro de Operaciones de Seguridad (SOC) que permita fortalecer la capacidad de monitoreo, detección, análisis y respuesta ante incidentes de ciberseguridad en la Entidad.
Recursos OTI	● Grupo de Trabajo de Informática Forense y Seguridad Digital
Áreas involucradas	OTI
Fecha de inicio estimada	3 febrero de 2025
Fecha de fin estimada	12 diciembre 2025

Nombre	**Diseñar de un equipo de respuesta ante emergencias informáticas CSIRT para protección de datos personales en la SIC**
Descripción	El proyecto tiene como objetivo principal diseñar un Equipo de Respuesta ante emergencias informáticas CSIRT para protección de datos personales en la SIC.
Recursos OTI	● Grupo de Trabajo de Informática Forense y Seguridad Digital
Áreas involucradas	OTI Delegatura de Datos Personales

Fecha de inicio estimada	3 febrero de 2025
Fecha de fin estimada	12 diciembre 2025

Nombre	**Fortalecer las debilidades en la gestión de incidentes de seguridad, según el análisis de brechas y la auditoría interna.**
Descripción	Actualmente el Centro de Operaciones de Seguridad - SOC viene desempeñando un rol importante en la detección y respuesta a amenazas cibernéticas, no obstante, se ha evidenciado una falta de articulación con el Grupo de Trabajo de Informática Forense y Seguridad Digital para generar estrategias de prevención y aprendizaje de eventos de seguridad de información. Por lo cual este proyecto busca generar protocolos de manejo de eventos de seguridad, comunicación continua y la implementación de una estrategia preventiva frente a ciberamenazas.
Recursos OTI	Grupo de Trabajo de Informática Forense y Seguridad Digital Grupo de Trabajo de Servicios Tecnológicos Mesa de Servicios
Áreas involucradas	OTI
Fecha de inicio estimada	3 febrero de 2025

Fecha de fin estimada	12 diciembre 2025

Nombre	**Implementar el programa de capacitación y sensibilización en seguridad de la información.**
Descripción	De acuerdo con el Modelo de Seguridad y Privacidad de la Información la capacitación de las personas es un aspecto fundamental para la gestión eficiente de la seguridad de la información. En este sentido, este proyecto busca desarrollar actividades articuladas con el plan institucional de capacitación para fortalecer el conocimiento de colaboradores de la SIC sobre las políticas de seguridad de la información, buenas prácticas, amenazas y controles en un entorno físico y digital.
Recursos OTI	● Grupo de Trabajo de Informática Forense y Seguridad Digital
Áreas involucradas	• OTI • Oficina de Servicios al Consumidor y de Apoyo Empresarial • Grupo de Desarrollo de Talento Humano
Fecha de inicio estimada	3 febrero de 2025
Fecha de fin estimada	12 diciembre 2025

Nombre	**Fortalecer controles de seguridad de la información, según el análisis de brechas y la auditoría interna.**
Descripción	Implementar actividades tendientes a fortalecer los controles de seguridad conforme al instrumento MSPI del Mintic.

Recursos OTI	Grupo de Trabajo de Informática Forense y Seguridad Digital Grupo de Trabajo de Servicios Tecnológicos
Áreas involucradas	OTI
Fecha de inicio estimada	3 febrero de 2025
Fecha de fin estimada	12 diciembre 2025

Nombre	**Implementar las estrategias de recuperación ante Desastres.**
Descripción	Se identificaron procesos y sistemas de información críticos, tiempos de recuperación, escenarios de riesgo y se definieron estrategias de recuperación. Este proyecto busca darle continuidad a lo trabajado previamente, buscando implementar estrategias de recuperación según la hoja de ruta definida.
Recursos	Grupo de Trabajo de Informática Forense y Seguridad Digital Grupo de Trabajo de Servicios Tecnológicos
Áreas involucradas	OTI
Fecha de inicio estimada	3 febrero 2025
Fecha de fin estimada	12 diciembre 2025

Nombre	**Fortalecer debilidades en la identificación de riesgos de nube pública, según el resultado del FURAG.**
Descripción	Este proyecto tiene como objetivo realizar una revisión continua de los riesgos de nube pública, una vez identificados socializar con las partes interesadas.

Recursos	Grupo de Trabajo de Informática Forense y Seguridad Digital Servicios Tecnológicos
Áreas involucradas	OTI
Fecha de inicio estimada	3 febrero de 2025
Fecha de fin estimada	12 diciembre 2025

Nombre	**Fortalecer estrategias en auditoría de proveedores**
Descripción	Es fundamental establecer un marco basado en estándares reconocidos como ISO 27001 y NIST, que permita evaluar riesgos, cumplimiento normativo y desempeño contractual. Esto incluye clasificar a los proveedores según su criticidad, definir criterios claros de evaluación, implementar herramientas para gestionar auditorías y automatizar revisiones, así como asegurar que los proveedores gestionen adecuadamente los riesgos de su propia cadena de suministro.
Recursos	Grupo de Trabajo de Informática Forense y Seguridad Digital
Áreas involucradas	Supervisores de los contratos Proveedores con los que se transfiere información
Fecha de inicio estimada	3 febrero de 2025
Fecha de fin estimada	12 diciembre 2025

Nombre	**Fortalecer debilidades en la identificación de activos de información, según el análisis de brechas y la auditoría interna.**

Descripción	Establecer las directrices y actividades generales para identificar, clasificar y valorar los activos de información de la Superintendencia de Industria y Comercio - SIC, a través de los lineamientos establecidos en este documento. Esta metodología orienta a los líderes de procesos en identificar los activos de información con el diligenciamiento del documento SC05-F03 Registro de Activos de Información, que ha sido establecido por la Entidad.
Recursos	Grupo de Trabajo de Informática Forense y Seguridad Digital Grupo de Gestión Documental y Archivo
Áreas involucradas	Lideres de los procesos de la entidad
Fecha de inicio estimada	3 febrero de 2025
Fecha de fin estimada	12 diciembre 2025

Nombre	**Apoyar la implementación del Programa Integral de Protección de Datos Personales**
Descripción	Se definió e implementó un programa integral de protección de datos personales en la SIC, el cual requiere la mejora continua. Este proyecto tiene el objetivo apoyar al oficial de datos personales de la SIC con los temas relacionados con seguridad de la información, así como mantener alineadas las políticas de PDP y el MSPI.
Recursos OTI	Grupo de trabajo de Informática Forense y Seguridad Digital.
Áreas involucradas	Oficina Asesora de Planeación
Fecha de inicio estimada	3 febrero de 2025
Fecha de fin estimada	12 diciembre 2025

Fin documento