PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2020

Superintendencia de Industria y Comercio

Enero, 2020

CONTENIDO

NOMBRE DEL DOCUMENTO	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
VIGENCIA	2020	
CREADO POR	Grupo de Trabajo de Informática Forense y Seguridad Digital.	Fecha: Enero, 2020
REVISADO POR	Eduar Enrique Navarro Morales Coordinador Grupo de Trabajo de Informática Forense y Seguridad Digital.	Fecha: Enero, 2020
APROBADO POR	Francisco Andrés Rodríguez Eraso Jefe Oficina de Tecnología e Informática.	Fecha: Enero, 2020

CONTROL DE CAMBIOS

Versión	**Fecha**	**Descripción del cambio**
1.0	Enero de 2020	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, 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 y de gestión de riesgos de seguridad de la información.
- Contar con políticas y procedimientos encaminados a mantener la integridad, confidencialidad y disponibilidad de la información.
- Gestionar los incidentes de seguridad presentados en la Entidad.
- Fortalecer la conciencia en cuanto a las amenazas y riesgos en el ciberespacio a los que se enfrentan los colaboradores en las labores diarias.
- Implementar 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.
- Contar con un repositorio de información actualizada del SGSI en la herramienta AGGIL.
- Identificar riesgos que pueden afectar la seguridad de la información en los procesos de la Entidad.

2 OBJETIVO

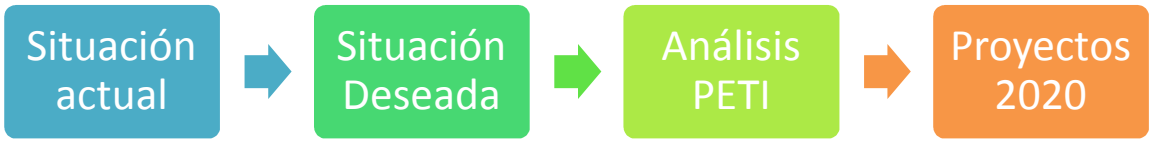
Establecer las acciones estratégicas, tendientes a fortalecer la seguridad y privacidad de la información en la Superintendencia de Industria y Comercio - SIC, mediante la planeación de actividades para la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI de la Entidad.

3 ALCANCE

El presente documento se encuentra articulado con el plan de acción institucional para el año 2020, Plan de Tratamiento de Riesgos de Seguridad de la Información, informe de revisión por la dirección del 2019 y Plan Estratégico de Tecnologías de Información (2019-2022).

4 METODOLOGÍA

La metodología utilizada para el desarrollo del Plan de Seguridad y Privacidad de la Información se muestra a continuación:



4.1 SITUACIÓN ACTUAL

Respecto a los resultados de FURAG del año 2018, se obtuvo un 76.9% para la Política de Gobierno Digital y un 79.8% para la Política de Seguridad Digital. Desde el punto de vista de Madurez de TI, el nivel encontrado fue contributivo. Lo cual fue corroborado por el Autodiagnóstico del MINTIC que indica un nivel medio alto quedando clasificado en la formula dos de la estrategia de Máxima Velocidad.

De otra parte, se identifican los niveles de madurez que posee la SIC con relación a la seguridad de la información por cada uno de los siguientes dominios:

- A.5 Política de seguridad.
- A.6 Organización de la seguridad de la información.
- A.7 Seguridad de los RRHH.
- A.8 Gestión de activos.
- A.9 Control de accesos.
- A.10 Criptografía.
- A.11Seguridad física y ambiental.
- A.12 Seguridad en las operaciones.
- A.13 Seguridad en las comunicaciones.
- A.14 Adquisición de sistemas, desarrollo y mantenimiento.
- A.15 Relación con proveedores.
- A.16 Gestión de los incidentes de seguridad.

- A.17 Continuidad del negocio.
- A.18 Cumplimiento con requerimientos legales y contractuales.

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

Controles administrativos:

ITEM	DESCRIPCIÓN	ISO
Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del	A.6.1.5

ITEM	DESCRIPCIÓN	ISO
	negocio principal, TI, gestión de instalaciones y otros procesos de soporte.	
Etiquetado de la información	Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	A.8.2.2
Manejo de activos	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	A.8.2.3
Planificación de la continuidad de la seguridad de la información	La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	A.17.1.1
Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa,	A.17.1.2
Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	A.17.1.3
Disponibilidad de instalaciones de procesamiento de información	Asegurar la disponibilidad de instalaciones de procesamiento de información.	A.17.2.1
Reglamentación de controles criptográficos.	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	A.18.1.5
Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	A.18.2.3

Controles técnicos:

ITEM	DESCRIPCIÓN	ISO
Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	A.9.4.5
Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	A.12.4.2
Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se debe registrar, y los registros se deben proteger y revisar con regularidad.	A.12.4.3
Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	A.13.2.1
Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	A.14.3.1

Adicionalmente y de acuerdo con el análisis de causas de los hallazgos evidenciados por la auditoría del SGSI del año 2019, se tienen los siguientes aspectos por mejorar:

- No se cuenta con un indicador del objetivo relacionado con la gestión de riesgos de seguridad de la información.
- No se cuenta con un procedimiento o instructivo que oriente adecuadamente la rotulación de la información, y que se responda a los requisitos de gestión documental y del MSPI.
- Existen falencias de presupuesto, método y personal suficiente para gestionar todas las actividades requeridas para planeación, diseño, ejecución y pruebas de las estrategias de continuidad tecnológica ante un desastre.
- Existen falencias en el seguimiento a los casos registrados en la herramienta de gestión de la mesa de servicios, asignados al Grupo de Trabajo de Sistemas de Información.
- Existen falencias en el seguimiento a los casos relacionados con la Infraestructura Tecnológica, registrados en la herramienta de gestión de la mesa de servicios.

- No se cuenta con un procedimiento establecido para la gestión y tratamiento de vulnerabilidades técnicas identificadas.
- Existen falencias en la gestión de usuarios privilegiados.
- No se tiene en cuenta a las partes interesadas en la definición de políticas de seguridad de la información.
- No se encuentra documentados riesgos de seguridad de la información ni planes de tratamiento en la gestión de los proyectos.
- Existen debilidades en la redundancia de canales de comunicación.

Finalmente, de acuerdo con las salidas del informe de Revisión por la Dirección del 2019, se deben realizar las siguientes acciones de mejora sobre el SGSI:

- Fortalecer el Plan de Recuperación de Desastres.
- Fortalecer la gestión de incidentes, incluyendo aspectos relacionados con información en formato físico, por ejemplo, expedientes y soportes magnéticos.
- Fortalecer la gestión de activos y etiquetado de información.
- Fortalecer los lineamientos relacionados con la privacidad de la información.
- Fomentar la participación de los funcionarios y contratistas en las actividades de sensibilización en seguridad de la información.
- Apoyar la implementación de políticas de seguridad de la información.
- Fomentar la cooperación entre entidades del Sector para temas de Ciberseguridad.

4.2 SITUACIÓN DESEADA

En primer lugar, el SGSI como proceso transversal pretende apoyar el logro de las metas institucionales, aportando desde la perspectiva de seguridad de la información en todos los proyectos en los que se encamine la Entidad. Como segundo aspecto, procura dar estricto cumplimento a las políticas y procedimientos de seguridad de la información, bajo un enfoque de sensibilización y concienciación de todas las partes interesadas, destacando el compromiso de la alta dirección con las estrategias de seguridad de la información. En tercer lugar, espera contar con un esquema robusto de monitoreo y respuesta a incidentes de seguridad de la información que permita responder adecuadamente y minimizar el impacto en la Entidad con el apoyo del CSIRT de Gobierno. En cuarto lugar, cerrar las brechas en la implementación de controles, encontradas en la auditoría Interna para superar una eventual auditoría de certificación en la Norma ISO 27001 vigente. En quinto lugar, contar con lineamientos claros y robustos para proteger la privacidad de la información, para la aplicación en todas las dependencias. Finalmente, contar con una Entidad preparada ante desastres que puedan afectar el normal funcionamiento, operación y prestación de los servicios al ciudadano.

4.3 ANÁLISIS PETI

4.3.1 En relación con los requerimientos de TI de las dependencias de la SIC

El SGSI apoyará el logro de los objetivos y necesidades del negocio en cuanto a Requerimientos de TI, fortaleciendo el cumplimiento del procedimiento de requisitos y pruebas de seguridad de la información, revisión y actualización del listado actual de 38 requisitos mínimos y fortalecimiento de las capacidades para efectuar pruebas de vulnerabilidad y hacking ético.

4.3.2 En relación con la seguridad y privacidad de la información Institucional

De acuerdo con lo estipulado en el Plan Estratégico de Tecnologías de Información de la SIC 2019-2022, se identifican mejoras en los controles de seguridad y privacidad de la información en lo concerniente con la ***comunicación, sensibilización y capacitación.***

Los controles asociados a la privacidad de la información en relación directa con los ***lineamientos de la protección de datos personales***, son un punto a mejorar pese a la existencia de un oficial del tema en la Entidad.

4.3.3 En relación con las situaciones objetivo del PETI

Para el logro de las situaciones objetivo del PETI producto del marco de referencia, presentadas a continuación, el SGSI participará en el diseño y documentación de los lineamientos de seguridad para la adopción, desarrollo, mantenimiento y actualización del marco de referencia de arquitectura empresarial de la Entidad, de tal forma que se mitiguen los riesgos de seguridad asociados a su implementación:

- Fortalecer gobernabilidad de la plataforma tecnológica de la SIC.
- Explotación de datos para apoyar la toma de decisiones.
- Sistematización y automatización de la cadena de valor.
- Interoperabilidad estándar.
- Implementación del esquema de documento electrónico.
- Seguridad y privacidad de la información.
- Normalización del modelo conceptual de la Entidad.
- Almacenamiento de backup histórico en la nube.
- Virtualización de escritorios remotos con terminales brutas.
- Consolidación de almacenamiento, backup y cómputo de la Entidad.

- Aumento de consumos de servicios de nube pública.
- Consolidación de mesa de servicios integrales.
- Mejoramiento del canal de conectividad de internet.
- Dimensionamiento de un plan de capacidad del componente tecnológico de acuerdo con las necesidades de la SIC.

5 PROYECTOS ESPECIFICOS 2020

Con base en la información presentada anteriormente, para la vigencia 2020 se ejecutarán los siguientes proyectos de seguridad de la información.

1. CSIRT Gobierno (fase 2).
2. Plan de tratamiento de riesgos de seguridad de la información.
3. Plan de recuperación ante Desastres -DRP.
4. Controles de seguridad de la información.
5. Sensibilización en seguridad de la información.
6. Fortalecer el componente de privacidad.
7. Lineamientos de seguridad para la Arquitectura Empresarial.

Adicionalmente, la Oficina de Tecnología e Informática implementará las mejoras en el Sistema de Gestión de Seguridad de la Información, con base en las recomendaciones de la Auditoría realizada en el cuarto trimestre del 2019.

Nombre	**CSIRT Gobierno (fase 2).**
Descripción	Implementar en el SIEM del CSIRT Gobierno los casos de uso aprobados para la SIC. Además de afinar las configuraciones de los dispositivos de seguridad monitoreados e implementar el instructivo de comunicaciones entre SIC Y CSIRT Gobierno.
Recursos	• Grupo de trabajo de Informática Forense y Seguridad Digital. • Grupo de Trabajo de Servicios Tecnológicos.
Áreas involucradas	OTI. MinTIC.
Fecha de inicio estimada	17 febrero de 2020
Fecha de fin estimada	30 noviembre 2020

Nombre	**Plan de tratamiento de riesgos de seguridad de la información.**
Descripción	Revisar, gestionar, realizar seguimiento y en los casos que aplique, implementar las actividades definidas en el plan de tratamiento de riesgos de seguridad de la información. Adicionalmente se pretende medir su efectividad.
Recursos	• Grupo de trabajo de Informática Forense y Seguridad Digital. • Oficina Asesora de Planeación.
Áreas involucradas	Toda la Entidad.
Fecha de inicio estimada	1 febrero de 2020
Fecha de fin estimada	15 diciembre 2020

Nombre	**Plan de recuperación ante Desastres -DRP.**
Descripción	Definir las actividades preventivas, detectivas y correctivas para reaccionar de manera eficiente ante un desastre que comprometa la prestación del servicio de la Superintendencia de Industria y Comercio, desde el punto de vista tecnológico.
Recursos	• Grupo de Trabajo de Informática Forense y Seguridad Digital. • Oficina Asesora de Planeación.
Áreas involucradas	Toda la Entidad.
Fecha de inicio estimada	15 febrero de 2020
Fecha de fin estimada	15 diciembre 2020

Nombre	**Controles de seguridad de la información.**
Descripción	Implementar actividades tendientes a fortalecer los siguientes controles de seguridad: • Etiquetado, clasificación y manejo de activos de información. • Identificación y gestión de eventos e incidentes. • Gestión de vulnerabilidades técnicas. • Protección de datos de prueba. • Gestión de usuarios privilegiados. • Análisis y especificación de requisitos de seguridad de la información.

	• Pruebas de seguridad de sistemas.
Recursos	Todos los Grupos de Trabajo de la Oficina de Tecnología e Informática
Áreas involucradas	Proceso de Gestión Documental
Fecha de inicio estimada	15 febrero de 2020
Fecha de fin estimada	15 diciembre 2020

Nombre	**Sensibilización en seguridad de la información.**
Descripción	Definir e implementar estrategias encaminadas a concienciar a los diferentes grupos focales de la Entidad, sobre políticas de seguridad de la información, buenas prácticas amenazas y controles en un entorno físico y digital.
Recursos	• Grupo de trabajo de Informática Forense y Seguridad Digital. • Equipo de Estrategia y Gobierno de TI.
Áreas involucradas	Oficina de Servicios al Consumidor y de Apoyo Empresarial
Fecha de inicio estimada	15 febrero de 2020
Fecha de fin estimada	15 diciembre 2020

Nombre	**Fortalecer el componente de privacidad.**
Descripción	Definir un programa integral de protección de datos personales en la SIC.
Recursos	• Grupo de trabajo de Informática Forense y Seguridad Digital. • Secretaria General. • Equipo de Estrategia y Gobierno de TI.
Áreas involucradas	Toda la Entidad
Fecha de inicio estimada	1 abril de 2020
Fecha de fin estimada	15 diciembre 2020

Nombre	**Lineamientos de seguridad para la Arquitectura Empresarial.**

Descripción	Apoyar el desarrollo e implementación del marco de referencia de arquitectura empresarial, aportando lineamientos y requisitos desde la óptica de seguridad digital.
Recursos	• Equipo de Estrategia y Gobierno de TI. • Grupo de trabajo de Informática Forense y Seguridad Digital.
Áreas involucradas	OTI
Fecha de inicio estimada	1 marzo de 2020
Fecha de fin estimada	15 diciembre 2020

_____

Fin documento