CONTENIDO

1 OBJETIVO

Establecer las acciones estratégicas, tendientes a fortalecer la seguridad y privacidad de la información de 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, las cuáles serán gestionadas por los servidores públicos o contratistas asignados de la Oficina de Tecnología e Informática - OTI.

2 DESTINATARIOS

Todos los colaboradores de la SIC.

3 GLOSARIO

CSIRT: Equipo de Respuesta a Incidentes de Seguridad Informática.

MIPG: Modelo Integrado de Planeación y Gestión.

MSPI: Modelo de Seguridad y Privacidad de la Información.

OTI: Oficina de Tecnología e Informática.

PHVA: Ciclo de mejora continua, Planear, Hacer, Verificar y Actuar.

PRIVACIDAD DE LA INFORMACIÓN: Derecho que tienen todos los titulares de la información, en relación con la información que involucre datos personales y la información clasificada que éstos hayan entregado o esté en poder de la entidad, en el marco de las funciones que a ella le compete realizar y que generan en las entidades la correlativa obligación de proteger dicha información en observancia del marco legal vigente[1].

SEGURIDAD DE LA INFORMACIÓN: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano[2].

[1] Modelo de Seguridad y Privacidad de la Información.
[2] Decreto 1008 de 14 de junio de 2018, por el cual se establecen los lineamientos generales de la Política de Gobierno Digital.

4 GENERALIDADES

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 debe establecer los detalles de cómo se realizará la implementación de la seguridad de la información en cada uno de los procesos de la entidad, estipulando directrices, tiempo y responsables para lograr un adecuado proceso de gestión, administración y evaluación.

5 DIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN

5.1. Modelo de seguridad y privacidad de la Información

A corte diciembre de 2018, el avance general en el ciclo PHVA del Sistema de Gestión de Seguridad de la Información de la SIC es del 99%, de acuerdo con la medición del instrumento de identificación de la línea base de seguridad, proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones, tal como se presenta a continuación:

AVANCE PHVA		
COMPONENTE	**AVANCE ACTUAL**	**AVANCE ESPERADO**
Planificación	40%	40%
Implementación	19%	20%
Evaluación de desempeño	20%	20%
Mejora continua	20%	20%
TOTAL	**99%**	**100%**

El 100% en el ciclo PHVA se alcanzará cuando se logre un nivel optimizado en el componente de implementación, el cual está relacionado directamente con el nivel de efectividad de controles actual:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES				
No	**Dominio**	**Calificación actual**	**Calificación objetivo**	**Evaluación de efectividad**
A.5	Políticas de seguridad de la información.	100	100	Optimizado
A.6	Organización de la seguridad de la información.	96	100	Optimizado
A.7	Seguridad de los recursos humanos.	100	100	Optimizado
A.8	Gestión de activos.	78	100	Gestionado
A.9	Control de acceso.	97	100	Optimizado
A.10	Criptografía.	60	100	Efectivo

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES				
No	**Dominio**	**Calificación actual**	**Calificación objetivo**	**Evaluación de efectividad**
A.11	Seguridad física y del entorno.	99	100	Optimizado
A.12	Seguridad de las operaciones.	80	100	Gestionado
A.13	Seguridad de las comunicaciones.	95	100	Optimizado
A.14	Adquisición, desarrollo y mantenimiento de sistemas.	80	100	Gestionado
A.15	Relaciones con los proveedores.	100	100	Optimizado
A.16	Gestión de incidentes de seguridad de la información.	100	100	Optimizado
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio.	80	100	Gestionado
A.18	Cumplimiento.	93,5	100	Optimizado
PROMEDIO EVALUACIÓN DE CONTROLES		**90**	**100**	**Optimizado**

A continuación, se presentan los controles que requieren alcanzar un nivel optimizado en su implementación:

ITEM	ISO
Seguridad de la información en la gestión de proyectos	A.6.1.5
Clasificación de la información	A.8.2.1
Etiquetado de la información.	A.8.2.2
Manejo de activos.	A.8.2.3
Transferencia de medios físicos.	A.8.3.3
Planificación de la continuidad de la seguridad de la información.	A.17.1.1
Implementación de la continuidad de la seguridad de la información.	A.17.1.2
Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	A.17.1.3
Disponibilidad de instalaciones de procesamiento de información.	A.17.2.1
Reglamentación de controles criptográficos.	A.18.1.5
Cumplimiento con las políticas y normas de seguridad.	A.18.2.2
Suministro de acceso de usuarios.	A.9.2.2
Control de acceso a códigos fuente de programas.	A.9.4.5
Política sobre el uso de controles criptográficos.	A.10.1.1
Gestión de llaves.	A.10.1.2
Seguridad de equipos y activos fuera de las instalaciones.	A.11.2.6

ITEM	ISO
Gestión de capacidad.	A.12.1.3
Registro de eventos.	A.12.4.1
Protección de la información de registro.	A.12.4.2
Registros del administrador y del operador.	A.12.4.3
Controles sobre auditorías de sistemas de información.	A.12.7.1
Políticas y procedimientos de transferencia de información.	A.13.2.1
Mensajería electrónica.	A.13.2.3
Protección de datos de prueba.	A.14.3.1

5.2. Modelo Integrado de Planeación y Gestión

Mediante el análisis de resultados del autodiagnóstico de la Política de Gobierno Digital, realizado con la herramienta proporcionada por MIPG, se evidenció que, de las 19 actividades de gestión formuladas para el componente de seguridad y privacidad de la información, 4 se encuentran con un porcentaje menor al 100%. Dichas actividades son presentadas a continuación:

ACTIVIDADES DE GESTIÓN	PUNTAJE (0 - 100)
La entidad ha construido, implementado y aprobado por medio de acto administrativo el Registro de Activos de Información de la entidad	**1**
En el periodo evaluado, la entidad cuenta con una metodología de gestión de activos de información donde se tienen en cuenta aspectos como: Cumplimiento legal, fechas de actualización, propietarios y criticidad de los activos. a La metodología de gestión de activos de información está en construcción. b La metodología de gestión de activos de información está en revisión. c La metodología de gestión de activos de información está en aprobación. d La metodología de gestión de activos de información está revisada, aprobada y divulgado por comité institucional de desarrollo administrativo o el que haga sus veces. e No la tiene.	**75**
Respecto al plan de tratamiento de riesgos de seguridad y privacidad de la información, indique las acciones realizadas por la entidad: a. Está construyendo el plan control operacional, en el cual se indica la metodología para implementar las medidas de seguridad definidas en	**50**

ACTIVIDADES DE GESTIÓN	PUNTAJE (0 - 100)
el plan de tratamiento de riesgos. b. Generó y aprobó el plan control operacional, en el cual se indica la metodología para implementar las medidas de seguridad definidas en el plan de tratamiento de riesgos c. Está construyendo los informes relacionados con la implementación de los controles de seguridad y privacidad de la información d. Generó y aprobó los informes relacionados con la implementación de los controles de seguridad y privacidad de la información e. Está definiendo los indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPI es eficiente, eficaz y efectiva f. Definió y aprobó los indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPI es eficiente, eficaz y efectiva	
Seleccione las actividades realizadas por la entidad en materia de apropiación de la Estrategia de Gobierno en línea: a. Formulación del plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información b. Ejecución del plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información, sin tener en cuenta la caracterización de grupos focales (Usuarios, Directivos, Técnicos y Terceros). c. Ejecución del plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información, con base en la caracterización de grupos focales (Usuarios, Directivos, Técnicos y Terceros).	**50**

Para cada actividad, se definió para la vigencia 2019, un plan de mejoramiento a fin de alcanzar un puntaje del 100%.

6 ESTRATEGIAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Teniendo en cuenta los anteriores autodiagnósticos, en la vigencia 2019 se planea llevar a cabo las siguientes estrategias, las cuales serán lideradas por la OTI:

ESTRATEGIAS	META	UNIDAD DE MEDIDA	AREAS INVOLUCRADAS	FECHA DE INICIO	FECHA FIN
Fortalecer a un nivel optimizado, controles del Sistema de	23	Controles	Todos los procesos	4 de febrero 2019	16 diciembre de 2019

ESTRATEGIAS	META	UNIDAD DE MEDIDA	AREAS INVOLUCRADAS	FECHA DE INICIO	FECHA FIN
Gestión de Seguridad de la información.					
Implementar estrategias de sensibilización en seguridad de la información.	3	Estrategias	Oficina de Tecnología e Informática	4 de febrero 2019	16 de diciembre de 2019
Desarrollar el plan de trabajo para la cooperación con el CSIRT Gobierno	1	Plan	Oficina de Tecnología e Informática	4 de febrero 2019	16 diciembre de 2019

7 DIRECTRICES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Los 23 controles de seguridad de la información a fortalecer son aquellos que tienen un nivel menor al 100% de implementación, según lo expuesto en el numeral 5.1 del presente documento.

- Las estrategias de sensibilización, con base en la caracterización de grupos focales (Usuarios, Directivos, Técnicos y Terceros), se definirán en el Plan de sensibilización, concienciación y culturización organizacional – SGSI.

- Se deberán cumplir las actividades definidas para cada línea estratégica del Plan de Protección para la Infraestructura Crítica Cibernética del Sector Comercio, Industria y Turismo (SCIT) que sean de competencia de la Entidad.

LÍNEA ESTRATÉGICA	DESCRIPCIÓN	ACTIVIDAD
Formación y Sensibilización	Desarrollar procesos de formación y sensibilización de la gestión de riesgos de seguridad digital y ciberseguridad en las entidades del sector.	Coordinar la sensibilización a Nivel Gerencial.
		Campaña Sectorial de sensibilización.
Mecanismos de Cooperación	Establecer alianzas de cooperación con CSIRT Gobierno para la prevención y mitigación de incidentes	Tramitar la inclusión de las Entidades del Sector a los servicios aplicables prestados por CSIRT de

LÍNEA ESTRATÉGICA	DESCRIPCIÓN	ACTIVIDAD
	cibernéticos.	Gobierno
		Gestionar a nivel de cada entidad la puesta en marcha de los servicios acordados con CSIRT de Gobierno.
Red de Apoyo Sectorial en temas de ciberseguridad	Fortalecer de forma colaborativa a nivel sectorial el conocimiento en temas de ciberseguridad.	Transferencia de conocimiento e información entre responsables de la Seguridad Digital.
Alinear los Planes de Gestión de Riesgos	Propender por la oportuna actualización de la gestión de riegos de ciberseguridad en cada entidad.	Validación conjunta de amenazas y vulnerabilidades que puedan afectar la infraestructura crítica del sector.

- El ciclo PHVA llevado a cabo en el periodo anterior debe continuar en el 2019, es decir, se debe verificar y actualizar, si se requiere, los siguientes aspectos del SGSI:

FASE	ACTIVIDADES
Planeación.	Revisar y actualizar el alcance.
	Revisar y actualizar las políticas de seguridad y privacidad de la información.
	Crear, actualizar y operar los procedimientos de seguridad y privacidad de la información.
	Revisar y actualizar los roles y responsabilidades para la seguridad de la información.
	Actualizar el inventario de activo de información.
	Realizar una nueva identificación y valoración de riesgos de seguridad de la información.
	Realizar el tratamiento de riesgos de seguridad de la información.
	Definir e implementar las estrategias para la toma de conciencia, educación y formación en la seguridad de la información.
Implementación.	Revisar y actualizar el procedimiento para la planificación y control operacional.
	Implementar o fortalecer los controles de seguridad.
	Realizar la Implementación del plan de tratamiento de riesgos.
	Medir los indicadores de gestión del SGSI.
Evaluación del	Revisar y actualizar el plan de seguimiento, evaluación y

FASE	ACTIVIDADES
desempeño.	análisis del SGSI.
	Definir un plan de auditoría interna.
	Realizar la evaluación del plan de tratamiento de riesgos.
Mejora continua.	Verificar los resultados del plan de seguimiento, evaluación y análisis del SGSI.
	Definir y ejecutar el plan de mejoramiento para los hallazgos de la auditoría interna.

- El ciclo del SGSI, en lo que respecta a la actualización del inventario de activos de información, identificación de riesgos, definición del plan de tratamiento e implementación del mismo, tendrá un ciclo de 18 meses contados a partir de enero de 2019. Este periodo se define en respuesta al proceso en curso para la integración del SGSI con el Sistema Integral de Gestión Institucional – SIGI, no obstante, para los siguientes ciclos el periodo será de 12 meses.

_____

Fin documento