CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Oscar Fabián Ramírez Torres. Cargo: Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital.	Nombre: Jaroslav Marlen López Chávez (E). Cargo: Jefe Oficina de Tecnología e Informática.	Nombre: Amanda Estella Pedraza Rodríguez Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad. Fecha: 2023-04-10

1 OBJETIVO

Definir las actividades para revisar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) de la Superintendencia de Industria y Comercio, a través de la revisión y seguimiento de los resultados de las actividades realizadas para la implementación del SGSI, las cuales serán realizadas por los servidores públicos o contratistas asignados de la Oficina de Tecnología e Informática - OTI.

2 DESTINATARIOS

Servidores públicos y contratistas del Grupo de Trabajo de Informática Forense y Seguridad Digital.

3 GLOSARIO

EVALUACIÓN DE DESEMPEÑO: Fase donde se evalúa y mide el desempeño del SGSI contra la política, los objetivos y la experiencia práctica de la gestión de la seguridad de la información, a la vez que se reportan los resultados a la dirección para su revisión y toma de decisiones.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Presencia identificada de un estado del sistema, servicio o de red de datos, que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INSTRUMENTO DE EVALUACIÓN DEL MSPI: Herramienta creada por el Ministerio de Tecnologías de la Información y las Comunicaciones con el fin de identificar el nivel de madurez en la implementación del Modelo de Seguridad y Privacidad de la Información, - MSPI, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas.

MSPI: Modelo de Seguridad y Privacidad de la Información.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

SGSI (Sistema de Gestión de la Seguridad de la Información): Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

SOC: Centro de operaciones de seguridad.

4 GENERALIDADES

De acuerdo con el Modelo de Seguridad y Privacidad de la Información - MSPI, la Superintendencia de Industria y Comercio - SIC, debe evaluar y medir el desempeño del Sistema de Gestión de la Seguridad de la Información - SGSI y reportar los resultados a la alta dirección para su revisión y toma de decisiones.

Para lo anterior, la SIC debe desarrollar un conjunto de actividades de seguimiento donde se mida y verifique el cumplimiento de los aspectos planteados en la fase de planificación del SGSI. Los resultados obtenidos deben ser utilizados para ajustar los aspectos de la seguridad y privacidad de la información, de tal forma que sea eficiente y eficaz en el cumplimiento de los objetivos trazados en la fase de planificación.

De acuerdo con el MSPI, se debe realizar seguimiento a lo siguiente:

- Ejecución de auditorías al SGSI.
- Programación y ejecución de las revisiones por parte del encargado de seguridad y privacidad de la información.
- Alcance e implementación del SGSI.
- Plan de seguridad y privacidad de la información.
- Eventos e incidentes de seguridad y privacidad de la información.

De igual forma, se debe realizar evaluación de los siguientes aspectos:

- Efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo residual después de la aplicación de controles y medidas administrativas.
- Medición de los indicadores de gestión del SGSI.
- Revisión de la ejecución de las actividades definidas en los planes de mejoramiento.

5 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO

A continuación, se muestra la representación esquemática del procedimiento:

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
1	REALIZAR EL SEGUIMIENTO DEL SGSI.	Programa de auditorías del SGSI. Instrumento de evaluación del MSPI. Plan de seguridad y privacidad de la información. Políticas y Objetivos del SGSI. Informes de incidentes de seguridad y medidas implementadas.	Esta etapa consiste en verificar la ejecución de las actividades planeadas para el SGSI, mediante la ejecución de las siguientes actividades: - Verificar el alcance e implementación del SGSI. - Revisar el cumplimiento de las actividades del Plan de Seguridad y Privacidad de la Información. - Verificar los eventos / incidentes de seguridad y privacidad de la información. - Verificar las auditorías al SGSI.	Profesionales de apoyo a la gestión operativa del SGSI. Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital.	Informes con los resultados del seguimiento al SGSI.

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
2	EVALUAR EL SGSI.	Plan de tratamiento revisado y actualizado en el SIGI. Riesgos de seguridad de la información. Indicadores del SGSI en el SIGI. Informes de auditorías anteriores. Planes de mejoramiento.	Esta etapa consiste en evaluar el SGSI mediante la ejecución de las siguientes actividades: - Evaluar la efectividad de los controles de seguridad de la información. - Revisar la evaluación de los niveles de riesgo residual. - Medir los indicadores de gestión del SGSI. - Apoyar en la revisión de las actividades definidas en los planes de mejoramiento.	Profesionales de apoyo a la gestión operativa del SGSI. Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital.	Informes con los resultados del seguimiento al SGSI.
3	ANALIZAR LOS RESULTADOS DEL SGSI.	Informes con los resultados del seguimiento al SGSI. Informes con los resultados de la evaluación del SGSI.	Esta etapa consiste en analizar los resultados del SGSI y preparar la revisión por la dirección, mediante la siguiente actividad: - Consolidar el informe de revisión por la alta dirección	Profesionales de apoyo a la gestión operativa del SGSI. Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital. Jefe Oficina de Tecnología e Informática.	Informe de revisión del SGSI para la Alta Dirección.

6 DESCRIPCION DE ETAPAS Y ACTIVIDADES

A continuación, se describen las etapas y actividades para el seguimiento, evaluación y análisis de resultados del SGSI.

6.1 ETAPA 1. REALIZAR EL SEGUIMIENTO DEL SGSI

En esta etapa se realizan las siguientes actividades:

6.1.1 Verificar el alcance e implementación del SGSI

Los profesionales de apoyo a la gestión operativa del SGSI, mensualmente presentan al Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, o quien él delegue, el estado de la implementación del MSPI en la entidad, mediante la evaluación de la efectividad de los controles de seguridad de la información y el avance en el ciclo PHVA, proporcionados por el Instrumento de Evaluación MSPI.

6.1.2 Revisar el cumplimiento de las actividades del plan de seguridad y privacidad de la información

Los profesionales de apoyo a la gestión operativa del SGSI, trimestralmente presentan al Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, o quien él delegue, el estado de la implementación del plan de seguridad y privacidad de la información, el cual debe contemplar el estado de las actividades, problemas presentados durante el periodo, próximas actividades con sus respectivos requisitos y propuestas para la implementación.

Nota No. 1: El plan de seguridad y privacidad de la información es un documento el cual es aprobado por el Oficial de Seguridad de la Información, rol asumido por el Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital.

6.1.3 Verificar los eventos e incidentes de seguridad y privacidad de la información

Semanalmente la mesa de servicios y el SOC generan un reporte del estado de los eventos e incidentes de seguridad y privacidad de la información recibidos y atendidos si se llegaron a presentar, conforme al documento SC05-P01 Procedimiento de gestión de incidentes.

En este sentido, el equipo gestor de Incidentes conformado por el SOC y los responsables de las herramientas tecnológicas, mantienen actualizada la información sobre los eventos e incidentes de seguridad en la herramienta de gestión y en los registros de casos y lecciones aprendidas.

6.1.4 Verificar las auditorías al SGSI

El Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, o quien él delegue, en conjunto con los profesionales de apoyo a la gestión operativa del SGSI, atienden la ejecución de las auditorías al SGSI coordinadas

por la Oficina de Control Interno conforme a lo establecido en el procedimiento CI02-P02 Procedimiento Auditorías Sistema Integral de Gestión Institucional.

6.2 ETAPA 2. EVALUAR EL SGSI

6.2.1 Evaluar la efectividad de los controles de seguridad de la información

Los profesionales de apoyo a la gestión operativa del SGSI, trimestralmente reportan al Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, o a quien él delegue, el avance en la implementación del plan de tratamiento de riesgos, efectividad de los controles, los problemas presentados en su implementación y cambios o mejoras propuestas para el plan de tratamiento de riesgos.

Para lo anterior, los profesionales de apoyo a la gestión operativa del SGSI, deben consultar la información sobre el plan de tratamiento de riesgos en el módulo de riesgos de la herramienta del Sistema Integral de Gestión Institucional SIGI y realizan seguimiento mensual a las actividades propuestas por los líderes de los procesos para mitigar el riesgo.

6.2.2 Revisar la evaluación de los niveles de riesgo residual

Anualmente los profesionales de apoyo a la gestión operativa del SGSI, revisan que los controles implementados para mitigar el riesgo inherente estén siendo efectivos. De lo contrario, se debe revisar con los dueños del riesgo la implementación de nuevos controles.
Lo anterior se reporta al Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital por medio del correo electrónico institucional.

6.2.3 Medir los indicadores de gestión del SGSI

Trimestralmente los profesionales de apoyo a la gestión operativa del SGSI deben reportar al Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, o a quien él delegue, el resultado de la medición de los indicadores del SGSI y deben mantener actualizado el módulo de indicadores de la herramienta del Sistema Integral de Gestión Institucional SIGI.

6.2.4 Apoyar en la revisión de la ejecución de las actividades definidas en los planes de mejoramiento

Los líderes de los procesos de la SIC, objeto de auditorías del SGSI, implementan las acciones definidas en los planes de mejoramiento, conforme a lo establecido en el formato CI01-F09 Plan de mejoramiento.

En este sentido, los profesionales de apoyo a la gestión operativa del SGSI en caso de ser requerido, realizaran actividades tendientes a la orientación requerida por las áreas en temas relacionados con la seguridad de la información.

El Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, o quien él delegue, en conjunto con los profesionales de apoyo a la gestión operativa del SGSI, atienden la ejecución de las actividades definidas en el plan de mejoramiento del proceso.

6.3 ETAPA 3. ANALIZAR LOS RESULTADOS DEL SGSI

6.3.1 Consolidar el informe de revisión por la alta dirección

Los profesionales de apoyo a la gestión operativa del SGSI deben presentar al Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, el proyecto de informe de revisión para la Alta Dirección, el cual contiene el análisis de los resultados de la implementación del SGSI, teniendo en cuenta los informes de seguimiento y evaluación del SGSI almacenados en la carpeta compartida del servicio de alojamiento en la nube.

Una vez aprobado dicho informe, la Oficina Asesora de Planeación - OAP lo presenta a la alta dirección, de acuerdo con los lineamientos del procedimiento CI02-P01 Revisión de la alta dirección al Sistema Integral de Gestión Institucional.

7 DOCUMENTOS RELACIONADOS

SC05-P01 Procedimiento de gestión de incidentes.
CI02-P01 Revisión de la alta dirección al Sistema Integral de Gestión Institucional.
CI02-P02 Procedimiento auditorías Sistema Integral de Gestión Institucional.
SC05-POL01 Políticas del Sistema de Gestión de Seguridad de la Información SGSI.

7.1 DOCUMENTOS EXTERNOS

NTC-ISO-IEC 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones.

8 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Se realizan ajustes en actividades de las Etapas 1, 2 y 3. Se adiciona el numeral 7.1 Documentos externos.

_____

Fin documento