CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Eduar Enrique Navarro Morales. Cargo: Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital.	Nombre: Oscar Javier Asprilla Cruz. Cargo: Jefe Oficina de Tecnología e Informática.	Nombre: Giselle Johanna Castelblanco Muñoz. Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad. Fecha: 2018-11-27

1 OBJETIVO

Establecer la estrategia para revisar la eficacia del 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 de la OTI.

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.

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.

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

4 REFERENCIAS

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
Norma Técnica Colombiana NTC-ISO-IEC	27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.	Todo el documento.	Todo el documento.
Guía	Modelo de Seguridad y Privacidad de la Información	Modelo de Seguridad y Privacidad de la Información.	Todo el documento.	Todo el documento.

5 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 MPSI, se debe realizar seguimiento a lo siguiente:

- Programación y 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 inherente y 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.

6 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 la herramienta de apoyo al SGSI. Riesgos de seguridad de la información. Ficha de indicadores del SGSI. 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 inherente y riesgo residual. - Medir los indicadores de gestión del SGSI. - Revisar la ejecución 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, de conformidad con el procedimiento CI02-P01 Revisión por la 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.

7 DESCRIPCION DE ETAPAS Y ACTIVIDADES

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

7.1 ETAPA 1. REALIZAR EL SEGUIMIENTO DEL SGSI

En esta etapa se realizan las siguientes actividades:

7.1.1 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 MPSI 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".

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

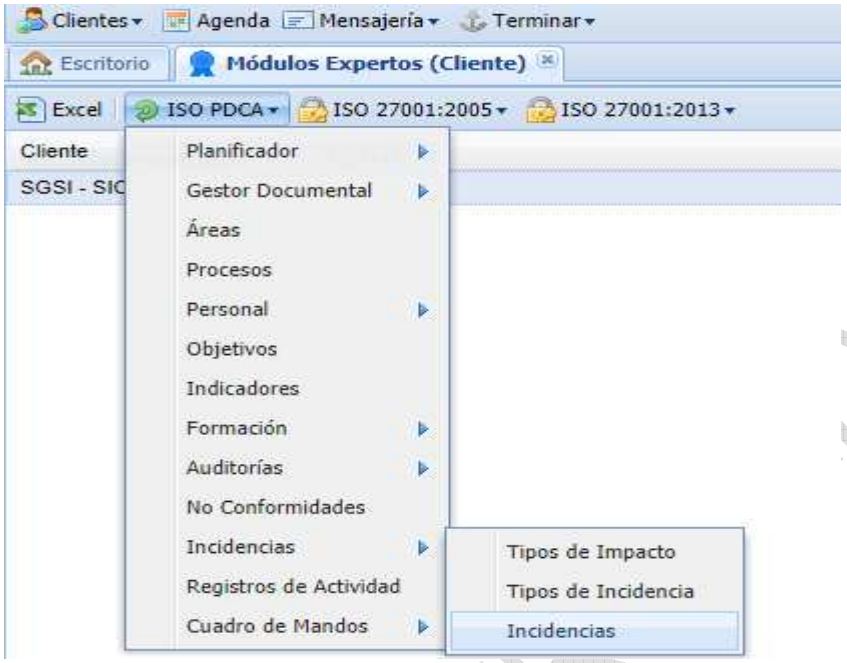
Los profesionales de apoyo a la gestión operativa del SGSI, mensualmente presentan al Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, o quien él delegue, el estado de la implementación del plan de seguridad y privacidad de la información, el cual debe contemplar el estado 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 que se encuentra ubicado en la herramienta de apoyo al SGSI y es aprobado por el Responsable de la seguridad digital y de la información de la Entidad.

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

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 los eventos e incidentes de seguridad y privacidad de la información tratados conforme al documento SC05-P01 Procedimiento de gestión de incidentes.

En este sentido, los profesionales de apoyo a la gestión operativa del SGSI, deben consultar y mantener actualizada la información sobre los eventos e incidentes de seguridad en la herramienta de apoyo al SGSI, para ello se debe remitir al módulo "ISO PDCA", menú "Incidencias" y seleccionar la opción "Incidencias". Tal como se muestra en la siguiente imagen:

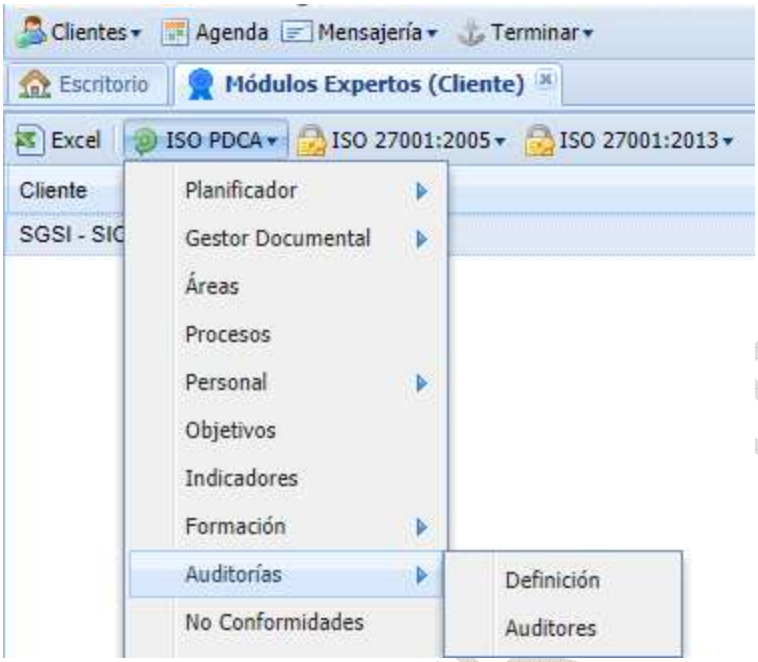


La base de conocimiento de incidentes puede ser consultada para apoyar la resolución de situaciones similares que se presenten con posterioridad.

7.1.4 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, coordinan la ejecución de las auditorías al SGSI conforme a lo establecido en el procedimiento CI02-P02 Procedimiento auditorías sistema integral de gestión institucional.

Para lo anterior, los profesionales de apoyo a la gestión operativa del SGSI deben consultar y mantener actualizada la información sobre la programación y detalle de las auditorías de seguridad de la información en la herramienta de apoyo al SGSI, para ello se deben remitir al módulo ISO PDCA, menú Auditorías y seleccionar la opción Definición. Tal como se muestra en la siguiente imagen.

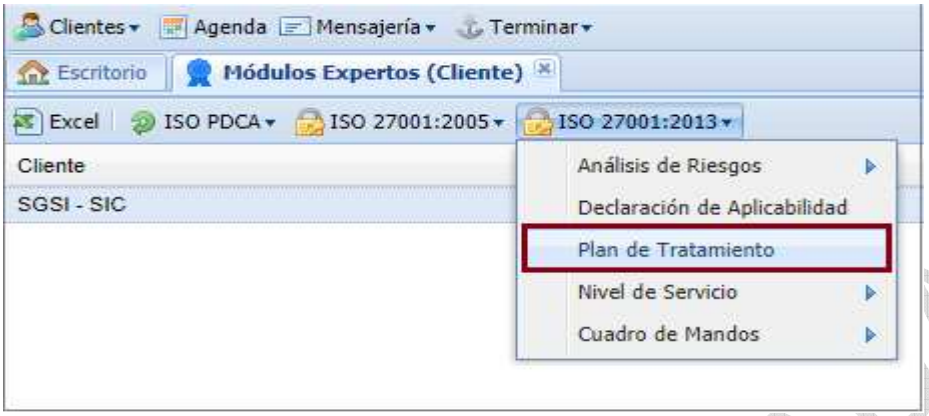


7.2 ETAPA 2. EVALUAR EL SGSI

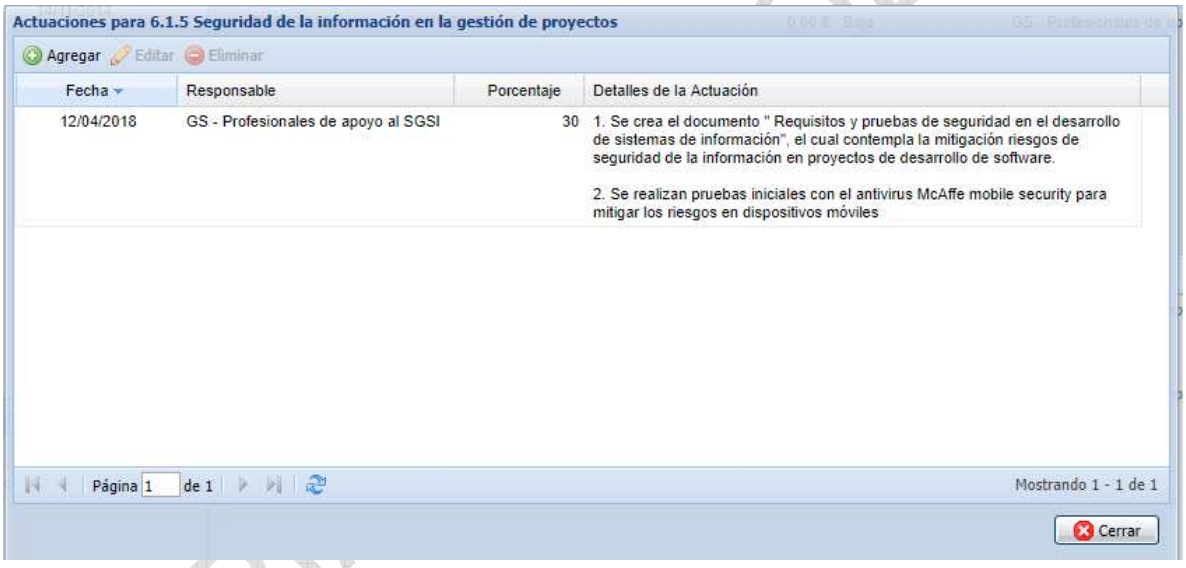
7.2.1 Evaluar la efectividad de los controles de seguridad de la información

Los profesionales de apoyo a la gestión operativa del SGSI, mensualmente 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 y mantener actualizada la información sobre el plan de tratamiento de riesgos en la herramienta de apoyo al SGSI, para lo cual se deben remitir al módulo ISO 27001:2013, menú Plan de tratamiento. Tal como se muestra a continuación:



En este menú, se diligencian las actuaciones realizadas durante mes inmediatamente anterior.



7.2.2 Revisar la evaluación de los niveles de riesgo inherente y riesgo residual

Los profesionales de apoyo a la gestión operativa del SGSI, anualmente presentan al Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, o quien él delegue, la evaluación de los niveles de riesgo inherente y riesgo residual luego de aplicar el plan de tratamiento de riesgos.

Para lo anterior, los profesionales de apoyo a la gestión operativa del SGSI, deben remitirse al módulo ISO 27001:2013, menú Análisis de riesgos de la herramienta de apoyo al SGSI y seleccionar la opción Análisis. Tal como se muestra a continuación:

7.2.3 Medir los indicadores de gestión del SGSI

Mensualmente, 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 reportarlos a la Oficina Asesora de Planeación.

Para lo anterior, los profesionales de apoyo a la gestión operativa del SGSI, deben consultar y mantener actualizada la información del SIGI y del módulo ISO PDCA, menú Indicadores de la herramienta de apoyo al SGSI, mostrado en la siguiente imagen:

7.2.4 Revisar 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 documento CI02-P05 Procedimiento acciones correctivas y preventivas y el formato CI02-F07 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 y mensualmente reportar al Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, o a quien él delegue, el resultado de las actividades.

7.3 ETAPA 3. ANALIZAR LOS RESULTADOS DEL SGSI

7.3.1 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.

Una vez aprobado dicho informe, la OAP presenta a la alta dirección, de acuerdo con los lineamientos del procedimiento CI02-P01 Revisión por la dirección.

8 DOCUMENTOS RELACIONADOS

SC05-P01 Procedimiento de gestión de incidentes.
CI02-P02 Procedimiento auditorías sistema integral de gestión institucional.
CI02-P05 Procedimiento acciones correctivas y preventivas.
CI02-P01 Revisión por la dirección.
SC05-I01 Políticas del Sistema de Gestión de Seguridad de la Información SGSI.

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

1. Creación del documento.

_____
Fin documento