CONTENIDO

1 OBJETIVO 2
2 DESTINATARIOS 2
3 GLOSARIO 2
4 GENERALIDADES 3
5 DESCRIPCION DE ACTIVIDADES 3
5.1 REVISAR POLÍTICAS DEL SGSI 3
5.2 EVALUAR LA DOCUMENTACIÓN ASOCIADA 3
5.3 REALIZAR CONTACTO CON LAS PARTES INTERESADAS 4
5.4 AJUSTAR LA DOCUMENTACIÓN 4
5.5 APROBAR LA DOCUMENTACIÓN 5
5.6 DIVULGAR ACTUALIZACIÓN 5
6 DOCUMENTOS RELACIONADOS 5
6.1 DOCUMENTOS EXTERNOS 6
7 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN 6

COPIA NO CONTROLADA

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Oscar Fabián Ramírez Torres Cargo: Coordinador Grupo de Trabajo de Informática Forense y Seguridad Digital.	Nombre: Francisco Andrés Rodríguez Eraso 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: 2022-09-07

Cualquier copia impresa, electrónica o de reproducción de este documento sin la marca de agua o el sello de control de documentos, se constituye en copia no controlada.

1 OBJETIVO

Ejecutar una revisión periódica de las políticas de seguridad de la información de la Superintendencia de Industria y Comercio – SIC con el fin de proteger la confidencialidad, integridad, disponibilidad y privacidad de la información de la Entidad. A través del desarrollo de las actividades descritas en este documento, las cuales son realizadas por los servidores públicos o contratistas designados y autorizados por el Oficial de Seguridad de la Información.

2 DESTINATARIOS

Las políticas de seguridad de la información de la Superintendencia de Industria y Comercio - SIC, deben ser revisadas y actualizadas en caso de ser necesario, por el Oficial de Seguridad de la Información o quien designe para tal fin.

3 GLOSARIO

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada.

INFORMACIÓN: Hace referencia a los datos en formato digital o físico, tratados, creados, procesados, almacenados, archivados o borrados durante la ejecución de procesos misionales de la Superintendencia de Industria y Comercio.

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

ISO 27001: Estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según la metodología del Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar).

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

SGSI: Sistema de Gestión de la Seguridad de la Información.

SIC: Superintendencia de Industria y Comercio.

COPIA NO CONTROLADA

SISTEMA DE GESTIÓN DE 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.

4 GENERALIDADES

Las políticas que integran el Sistema de Gestión de Seguridad de la Información – SGSI de la SIC, se encuentran enfocadas a las buenas prácticas de seguridad de la información basadas en la norma ISO 27001:2013, al Modelo de Seguridad y Privacidad de la Información de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones y a al cumplimiento de la normatividad legal colombiana vigente.

La Superintendencia de Industria y Comercio realizará periódicamente la difusión, actualización y consolidación tanto de las presentes políticas como de los demás componentes del Sistema de Gestión de la Seguridad de la Información, integrando el SGSI los demás sistemas de gestión, de tal forma que apoye a la Entidad en la protección de los derechos de los consumidores, la libre y sana competencia, y el actuar de la Entidad como autoridad nacional en la propiedad industrial y protección de datos personales.

5 DESCRIPCION DE ACTIVIDADES

5.1 REVISAR POLÍTICAS DEL SGSI

El oficial de seguridad de la información o quien designe para tal fin, realizará una revisión anual de la documentación existente relacionada con las políticas del SGSI en la entidad, a fin de determinar si debido a un evento crítico, un cambio en la normatividad vigente, un hallazgo de auditoría, entre otros eventos, se requiere realizar una actualización, creación, modificación y/o eliminación de las políticas de seguridad de la información o por el contrario se mantienen igual. En caso de requerirse, se debe realizar también la actualización de los procedimientos e instructivos asociados que se vean impactados por la creación, actualización, modificación y/o eliminación de dichas políticas.

La creación, actualización, modificación y/o eliminación de las políticas, en adelante se conocerá como el tipo de cambio o el cambio.

5.2 EVALUAR LA DOCUMENTACIÓN ASOCIADA

En caso de tratarse de una política existente, el servidor público o contratista del SGSI, debe revisar la documentación asociada teniendo en cuenta los cambios

COPIA NO CONTROLADA

normativos, hallazgos de auditoría o los eventos identificados en el numeral anterior, para determinar si es necesario realizar una modificación, actualización o eliminación de esta. También es necesario corroborar si, después de realizar el cambio, las partes interesadas seguirán siendo las mismas y definir el impacto que este les causará.

En caso de tratarse de la creación de una política nueva o inexistente en la SIC, es necesario definir si se requiere generar nuevos procedimientos y/o instructivos, o si se realizará una actualización en la documentación existente. Así mismo, es necesario definir cuáles son las áreas de la entidad que se verán afectadas y de esta manera, determinar cuáles serán las partes interesadas que se deben involucrar en el proceso.

5.3 REALIZAR CONTACTO CON LAS PARTES INTERESADAS

Dependiendo del tipo de cambio que se haya definido en la actividad anterior, el servidor público o contratista del SGSI, hará contacto con las partes interesadas, a fin de socializar las novedades que se presentarán, así como el impacto que tendrán para cada una de ellas. El objetivo de este contacto será la recepción de observaciones y/o comentarios y la identificación de los requerimientos y/o necesidades por parte de las áreas; y su resultado será un correo electrónico que contenga la información suministrada en la sesión y las actividades y responsables definidos para iniciar la ejecución del cambio.

De acuerdo con el objetivo de la sesión definida, el contacto con las partes interesadas podrá ser de manera virtual mediante correo electrónico, herramientas digitales para efectuar reuniones, encuestas, entre otros, o podrá ser de forma presencial en caso de requerirse.

5.4 AJUSTAR LA DOCUMENTACIÓN

En caso de tratarse de una política existente, el servidor público o contratista del SGSI elabora la propuesta de modificación, actualización o eliminación de esta y/o de la documentación asociada, de acuerdo con el alcance del cambio y teniendo en cuenta las observaciones, comentarios e insumos, resultado del contacto con las partes interesadas.

En caso de tratarse de la creación de una política nueva o inexistente, se elaborará tanto la política, como la documentación creada y/o modificada (según sea el caso), de acuerdo con el alcance definido y teniendo en cuenta las observaciones, comentarios e insumos, resultado del contacto con las partes interesadas.

COPIA NO CONTROLADA

Una vez se cuente con la versión final de la propuesta, la persona designada, debe socializar en una reunión virtual o presencial, la documentación tanto con las partes interesadas, como con los miembros del Grupo de Informática Forense y Seguridad Digital, a fin de recibir observaciones y/o solicitudes adicionales y generar así la versión final de la propuesta. El servidor público o contratista del SGSI, envía esta versión final vía correo electrónico al Oficial de Seguridad de la Información, para su revisión y visto bueno.

5.5 APROBAR LA DOCUMENTACIÓN

El Oficial de Seguridad de la Información, remitirá la propuesta revisada a la persona designada, a fin de realizar los ajustes pertinentes, y en caso de ser necesario, se deberán socializar los cambios con las partes interesadas.

Una vez se cuente con la versión final del documento de Políticas del SGSI ajustado y la documentación asociada, se remitirá la propuesta a la Oficina Asesora de Planeación para iniciar la revisión metodológica, de acuerdo con lo indicado en el procedimiento SC01-P01 Documentación y Actualización del Sistema Integral de Gestión Institucional – SIGI.

De acuerdo a la complejidad del cambio, así como al impacto que se pueda generar el mismo, la documentación será aprobada por el Jefe de la Oficina de Tecnología e informática o por el Oficial de Seguridad de la Información, para posteriormente ser presentada al Comité Institucional de Gestión y Desempeño.

Finalmente, el documento Políticas del Sistema de Gestión de Seguridad de la Información – SGSI, será aprobado y firmado por el Superintendente de Industria y Comercio.

5.6 DIVULGAR ACTUALIZACIÓN

Una vez se encuentre publicada la documentación en el SIGI, el servidor público o contratista del SGSI solicita a OSCAE la publicación de un banner en la IntraSIC y se enviará también un correo electrónico con el banner a cada uno de los servidores públicos y contratistas de la entidad, precisando los ajustes y cambios de las o la política.

6 DOCUMENTOS RELACIONADOS

SC05-POL01 Políticas del Sistema de Gestión de Seguridad de la Información – SGSI.

COPIA NO CONTROLADA

6.1 DOCUMENTOS EXTERNOS

Modelo de Seguridad y Privacidad de la Información – MSPI de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.

7 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Las políticas del Sistema de Gestión de Seguridad de la Información – SGSI se registran en la política SC05-POL01. En este documento se describen las actividades para revisión de las políticas SGSI.

Fin documento

COPIA NO CONTROLADA