CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: John Edward Molano Hernández Cargo: Grupo de Trabajo de Infraestructura Tecnológica Y Seguridad Informática. Firma: (Original firmado)	Nombre: Oscar Javier Asprilla Cruz Cargo: Jefe Oficina de Tecnología e Informática Firma: (Original firmado)	Nombre: Juan Pablo Herrera Saavedra Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2017-12-14 Firma: (Original firmado)

1. OBJETIVO

El presente documento establece la directriz general para la protección de la confidencialidad, integridad y disponibilidad de la información a través del establecimiento del contexto, la definición de la política general, objetivos, alcance y roles del Sistema de Gestión de Seguridad de la Información de la Superintendencia de Industria y Comercio, acorde con la norma NTC-ISO-IEC 27001:2013 y el Modelo de Seguridad y Privacidad de Gobierno el Línea – GEL.

2. DESTINATARIOS

Aplica para la Superintendencia de Industria y Comercio, sus servidores públicos y contratistas, terceros, proveedores y practicantes.

3. GLOSARIO

ACTIVO DE INFORMACIÓN: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la entidad, por ejemplo: archivos, bases de datos, documentación del sistema, manuales de usuarios, material de formación, procedimientos, planes de continuidad, configuración de soporte, etc.

ADMINISTRADOR DE LOS SISTEMAS DE SEGURIDAD: profesional encargado de la administración de los dispositivos de seguridad perimetral.

AGENTE DEL PRIMER PUNTO DE CONTACTO: profesional de la Mesa de Servicios, encargado de recibir, registrar escalar los posibles incidentes de seguridad de la información reportados por los usuarios.

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

CIO (Chief Information Officer): es el líder de la gestión estratégica de tecnologías de información, encargado de planificar, organizar, coordinar, gestionar y controlar la estrategia de uso y apropiación de TI y el Modelo de Seguridad y Privacidad de la Información, y todo lo que conlleva esta tarea.

DISPONIBILIDAD: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

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

INFORMACIÓN: se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: es el profesional responsable de alinear las iniciativas de seguridad con los objetivos misionales, garantizando que los bienes y las tecnologías de la información están adecuadamente protegidos.

SGSI: Sistema de Gestión de seguridad de la Información.

SIC: Superintendencia de Industria y Comercio.

SIGI: Sistema Integral de Gestión Institucional.

4. DESCRIPCIÓN DE ACTIVIDADES

4.1 Información de contexto del SGSI

A continuación, se presenta la información pertinente sobre el contexto de la SIC, entorno al SGSI.

Contexto	Descripción
Entidad.	Entidad pública adscrita al Ministerio de Comercio, Industria y Turismo del estado colombiano. La estructura actual y funciones actuales se encuentran establecidas en el Decreto 4886 de 2011.
Misión.	*"La SIC salvaguarda los derechos de los consumidores, protege la libre y sana competencia, actúa como autoridad nacional de la propiedad industrial y defiende los derechos fundamentales relacionados con la correcta administración de datos personales.* *De esta manera, la SIC es parte fundamental en la estrategia estatal en favor de la competitividad y la formalización de la economía, lo cual incluye la vigilancia a las cámaras de comercio y la metrología legal en Colombia ".* Disponible en: http://www.sic.gov.co / Nuestra Entidad / Información Institucional / Misión y Visión.

Contexto	Descripción
Visión.	*"Seremos reconocidos como una Entidad líder en el control y apoyo a la actividad empresarial y en la defensa de los derechos del consumidor colombiano y de la protección de datos personales.* *Para el efecto, se consolidará una estructura administrativa soportada en un talento humano que se distinguirá por su profesionalismo y compromiso y con una clara orientación de servicio al país y en un sistema integrado de gestión, apoyado en procesos automatizados que atenderán los requerimientos de los usuarios institucionales".* Disponible en: http://www.sic.gov.co / Nuestra Entidad / Información Institucional / Misión y Visión.
Estructura organizacional y responsabilidades.	La estructura y funciones actuales de la SIC se encuentran establecidos en el Decreto 4886 de 2011. La información detallada sobre la estructura organizacional y funciones se encuentra en http://www.sic.gov.co / Nuestra Entidad / Información Institucional /Perfiles Directivos y Organigrama.
Funciones.	Los temas relacionados con las funciones de la SIC son los siguientes: - Propiedad industrial. - Protección al consumidor. - Control y verificación de reglamentos técnicos y metrología legal. - Protección de la competencia. - Vigilancia de las Cámaras de Comercio. - Protección de datos personales. - Asuntos jurisdiccionales. La información detallada sobre las funciones y objetivos se encuentra en: http://www.sic.gov.co / Nuestra Entidad / Información Institucional / Objetivos y funciones.
Trámites y servicios.	La SIC ofrece trámites y servicios en relaciona con sus objetivos y funciones institucionales.

Contexto	Descripción
	La información detallada sobre los trámites y servicios de la SIC se encuentra disponible en el documento SC01-M01 Manual Integral de Gestión Institucional – SIGI, numeral 7.5 Producción y prestación del servicio, anexo E – Listado de trámites y servicios prestados por la SIC.
Procesos.	Los siguientes son los tipos de procesos que operan en la SIC: - Procesos estratégicos. - Procesos misionales. - Procesos de apoyo. - Procesos de seguimiento, evaluación y control. La descripción detallada de los diferentes procesos y procedimientos se encuentra disponible en: SC01-M01 Manual Integral de Gestión Institucional – SIGI, numeral 4.1 Requisitos Generales y en la Página web: http://www.sic.gov.co / Nuestra Entidad / Información Institucional / Sistema Integral de Gestión Institucional.
Sedes.	Sede principal: Bogotá D.C, Carrera 13 No. 27 – 00, Pisos: 1,3,4,5,6,7,10 y Mezanine. Horario de atención: lunes a viernes de 8:00 a.m. a 4:30 p.m. Teléfono: 5920400. La SIC cuenta con Puntos de Atención al Ciudadano (PAC) en diferentes ciudades del país. Información detallada en: http://www.sic.gov.co / Nuestra Entidad / Información Institucional / Ubicación Geográfica.
Otros sistemas de gestión.	Sistemas de Gestión de Calidad, Sistemas de Gestión Ambiental y Sistemas de Gestión de Salud y Seguridad en el Trabajo.

4.2 Requisitos y partes interesadas del SGSI

Los requisitos pertinentes para el Sistema de Gestión de Seguridad de la Información de la SIC se encuentran identificados en el normograma del proceso Gestión de la Seguridad de la Información ubicado en el SIGI. Así mismo, las partes

interesadas, los proveedores, clientes internos y externos del SGSI se identifican en la caracterización del proceso mencionado.

4.3 Política general del sistema de gestión de seguridad de la información

La Superintendencia de Industria y Comercio, entendiendo la importancia de una adecuada gestión de la información para el logro de su misión y objetivos institucionales, se compromete a:

Preservar la confidencialidad, integridad y disponibilidad de los activos de información de los diferentes procesos de la entidad, por medio de la gestión de los riesgos, implementación de programas, controles y políticas de seguridad de la información.

Lo anterior dentro de un marco del trabajo en equipo, aseguramiento de las competencias, suministro de los recursos necesarios, cumplimiento de los requisitos legales aplicables en relación con el manejo de la información y otras disposiciones que apliquen para la mejora continua del Sistema de Gestión de Seguridad de la Información.

4.4 Alcance del sistema de gestión de seguridad de la información

El Sistema de Gestión de Seguridad de la Información, aplica para todos los procesos de la entidad, sus servidores públicos, contratistas, terceros y la ciudadanía en general.

4.5 Objetivos de la seguridad de la información

Los objetivos de la seguridad de la información son los siguientes:

a) Proteger los activos de información mediante la implementación de políticas, procedimientos y controles de seguridad necesarios y suficientes de acuerdo con el análisis de riesgo.

b) Gestionar los riesgos de seguridad de la información de manera que estén dentro de los niveles de aceptación definidos por la SIC.

c) Conseguir y mantener una cultura de seguridad la información, reflejada en la aceptación y aplicación de las políticas y controles de seguridad por parte de los servidores públicos y contratista de la SIC.

d) Prevenir, identificar y gestionar los incidentes que atenten contra la disponibilidad, confidencialidad e integridad de la información, con la

cooperación y asistencia activa de las autoridades en materia de seguridad de la información.

4.6 Roles involucrados en la gestión de la seguridad de la información

A continuación, se realiza la descripción de roles involucrados en la gestión de la seguridad de la información de la Superintendencia de Industria y Comercio, conforme la norma NTC-ISO-IEC 27001:2013, el Modelo de Seguridad y Privacidad de la Información de MinTIC y el Marco de Referencia de Arquitectura Empresarial de MinTIC. Los roles del SGSI se muestran en la figura 1.

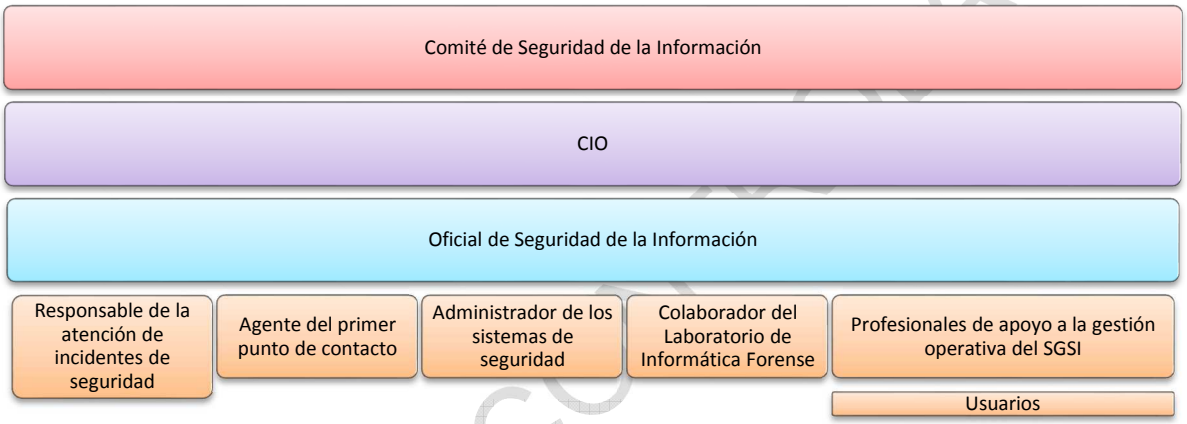

Figura 1 Distribución de roles relacionados a la gestión de la seguridad de la información.

4.6.1 Usuarios

Los usuarios del SGSI son todos los servidores públicos, contratistas y terceros de la SIC y tienen las siguientes responsabilidades:

- Cumplir con las políticas de seguridad de la información.
- Reportar incidentes de seguridad que atenten contra la confidencialidad, integridad o disponibilidad de la información o evidencien un incumplimiento de las políticas de seguridad de la SIC.
- Participar activamente de las campañas de sensibilización en SGSI.
- Participar de las actividades para la identificación de activos y riesgos de seguridad de la información.
- Apoyar el desarrollo de las auditorías internas y externas al SGSI

4.6.2 Responsable de la atención de incidentes de seguridad

Las funciones de este rol son las siguientes:

- Responder a las consultas sobre incidentes de seguridad.

- Revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a la alta dirección.

- Convocar la participación de otros servidores públicos de la entidad cuando el incidente lo amerite (Comunicaciones, Gestión de Talento Humano, Gestión Jurídica, Tecnología, Representante de las Directivas para el SGSI, etc.).

- Revisar el cumplimiento de los procedimientos y mejores prácticas en gestión de incidentes y recomendar, si lo amerita, la aplicación de planes de contingencia y/o continuidad.

- Revisar todos los incidentes de seguridad y los aspectos contractuales que aplican para el outsourcing de la Mesa de Servicios.

Se recomienda que el responsable de la atención de incidentes cuente con formación en la recepción, análisis, tratamiento y resolución de incidentes de seguridad de la información. Adicionalmente se recomienda que conozca y maneje los fundamentos jurídicos que exigen la intervención de un perito en informática forense y que tenga conocimientos sobre la ejecución de procedimientos de gestión de vulnerabilidades y test de penetración sobre la plataforma tecnológica.

Nota: Las actividades descritas en el presente rol serán realizadas por un servidor público y/o contratista de la Oficina de Tecnología e Informática.

4.6.3 Agente del primer punto de contacto

Es el encargado de recibir las solicitudes por parte de los usuarios sobre posibles incidentes y registrarlos en la base de conocimiento del software de Mesa de Servicios. Debe contar con capacitación en Seguridad de la Información que le permita diferenciar los incidentes de soporte de los incidentes de seguridad de la información y debe conocer a quien escalar los incidentes de seguridad (Administrador de los sistemas de seguridad, Oficial de seguridad de la información, etc.).

Los eventos y/o debilidades que se pueden ser reportados hacia los agentes del primer punto de contacto para su respectiva investigación, análisis y gestión deben

ser aquellos que atenten contra la confidencialidad, disponibilidad e integridad de la información, entre los cuales se pueden mencionar:

- Accesos no autorizados a los sistemas de información.
- Uso indebido de los recursos informáticos de la Entidad.
- Divulgación de información a quien no tiene derecho a conocerla.
- Uso de la información con el fin de obtener beneficio propio o de terceros.
- Hacer pública la información sin la debida autorización.
- Realización de copias no autorizadas de software.
- Descargar software a través de Internet sin la debida autorización.
- Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.
- Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.
- Enviar cualquier comunicación electrónica fraudulenta.
- Violación de cualquier ley o regulación nacional respecto al uso de sistemas de información.
- Robo de información sensible.
- Robo y pérdida de equipos de cómputo con información sensible.
- Denegación de servicio sobre equipos de la red, afectando la operación diaria de la Entidad.
- Denegación de servicio por el ingreso y propagación de virus que explotan vulnerabilidades.
- Amenazas a través de diferentes medios de comunicación (por ejemplo, correo electrónico) que generen un impacto directo sobre la seguridad de la información.

- Cambios o modificaciones en registros de bases de datos sin previa autorización.

- Generación o distribución de código malicioso.

- Fallas en los sistemas de información y pérdidas de servicio.

- Otros eventos y/o vulnerabilidades relacionadas con la seguridad de la información.

Nota: Las actividades descritas en el presente rol serán realizadas por los agentes de la Mesa de Servicios.

4.6.4 Administrador de los sistemas de seguridad

Las funciones de este rol son las siguientes:

- Configurar y mantener los activos informáticos relacionados con la gestión de la seguridad de la información, por ejemplo, equipo de firewall, sistemas de prevención de intrusos (IPS), enrutadores de frontera, sistemas de gestión y monitoreo, consola de despliegue de políticas de seguridad, etc.

- Debe ser notificado por el Agente del primer punto de contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar el incidente de seguridad.

- Debe documentar y notificar al Agente del primer punto de contacto y al Oficial de Seguridad de la Información sobre el incidente y la solución del mismo.

- Generar los reportes de eventos de seguridad que sean solicitados por parte del Oficial de Seguridad de la Información, por ejemplo, aquellos relacionados al uso de un canal de comunicaciones, registro de accesos a recursos, entre otros.

- Realizar los ajustes necesarios sobre los sistemas de seguridad que gestione y que sean indicados por el Oficial de Seguridad de la Información a manera de control detectivo o correctivo.

- Dar cumplimiento a las disposiciones definidas para el uso de dispositivos móviles. Esto aplica particularmente para el administrador de la solución de gestión de la movilidad de la SIC.

Se recomienda que el administrador de los sistemas de seguridad de la información tenga conocimiento en tecnologías de seguridad perimetral (con un componente

tecnológico en redes y erradicación de vulnerabilidades, Ethical Hacking y técnicas forenses) y debe tener claridad sobre el procedimiento de gestión de incidentes de la entidad.

Nota: Las actividades descritas en el presente rol serán realizadas por un servidor público o contratista del Grupo de Trabajo de Infraestructura Tecnológica y Seguridad Informática.

4.6.5 Servidor público y/o contratista del laboratorio de informática forense

Las funciones de este rol son las siguientes:

- Debe estar disponible en caso de que ocurra un incidente de impacto alto (o uno que amerite acciones disciplinarias o legales o investigación profunda) que requieran la recopilación de evidencia digital.

- Debe ser un apoyo para los demás roles en caso de dudas sobre los procedimientos o acciones a seguir con respecto a la gestión de incidentes y debe ejercer un liderazgo técnico en el proceso de atención de incidentes de seguridad de la información.

Se recomienda que el primer respondiente cuente con habilidades y experiencia en recolección de evidencia digital de diferente tipo y sobre diferentes tipos de activos. Adicionalmente se recomienda que conozca y maneje los fundamentos jurídicos que exigen la intervención de un perito en informática forense y que tenga conocimientos sobre la ejecución de procedimientos de gestión de vulnerabilidades y test de penetración sobre plataforma tecnológica.

Nota: Las actividades descritas en el presente rol serán realizadas por el Laboratorio de Informática Forense de la SIC o por un servidor público y/o contratista de la Oficina de Tecnología e Informática de la SIC, que preferiblemente tenga formación como *Access Data Certified Examiner*.

4.6.6 Profesionales de apoyo a la gestión de operativa del SGSI

Las funciones de este rol son las siguientes:

- Apoyar al oficial de seguridad y a los líderes del proceso en la identificación de activos de información.

- Apoyar al oficial de seguridad a los líderes de proceso en la aplicación de la metodología de valoración de riesgos.

- Apoyar la medición de indicadores del SGSI.

- Alimentar la herramienta dispuesta para la documentación del SGSI.

- Proponer al Oficial de seguridad de la información actualización a la documentación del SGSI existente.

- Gestionar las campañas de sensibilización o divulgación del SGSI.

- Apoyar la mejora continua del SGSI.

Nota: Las actividades descritas en el presente rol, serán realizadas por los servidores públicos y/o contratistas del Grupo de Trabajo de Infraestructura Tecnológica y Seguridad Informática, responsables de apoyar la gestión operativa del SGSI.

4.6.7 Oficial de seguridad de la información

Las funciones de este rol son las siguientes:

- Responsable de planear, coordinar y administrar los procesos de seguridad de la información en la entidad.

- Tiene la función de brindar los servicios de seguridad en la SIC a través de la planeación, coordinación y administración de los procesos de seguridad de la información.

- Difundir la cultura de seguridad de la información entre todos los miembros de la SIC.

- Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de la información de la SIC.

- Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e Información.

- Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de la implantación de las medidas de seguridad.

- Supervisar la respuesta a incidentes, así como la investigación de las violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.

- Promover y supervisar la firma del documento “Acuerdo de Seguridad de la Información” que hace las veces de un control disuasivo por cuanto contiene las condiciones aceptables de uso de los activos de información por parte de los colaboradores de la SIC. Esto para apoyar el cumplimiento de la Política de Uso Aceptable de Activos.
- Revisar el cumplimiento de la ejecución del plan de mantenimiento de los equipos que se ha definido.

- Incentivar y validar la extensión en el uso del gestor de contraseñas, como control preventivo, con el fin de evitar la revelación de contraseñas y el uso de contraseñas débiles.

- Incentivar y validar la extensión en el uso de la solución DLP (Data Loss Prevention) de la SIC con el propósito de evitar la fuga de información hacia medios removibles o hacia sistemas externos a la SIC.

- Solicitar los reportes que considere pertinentes a los demás roles con el propósito de tomar las medidas preventivas, correctivas, defectivas o disuasorias necesarias para la gestión de la seguridad de la información.

Se recomienda que el Oficial de seguridad de la información cuente con formación en auditoria de sistemas de información o seguridad de la información con base a la norma NTC-ISO-IEC 27001:2013. Debe tener experiencia en temas de seguridad de la información en los ámbitos de auditorías informáticas, informática forense, seguridad informática, auditoria de sistemas de información y comunicación, plataforma tecnológica (base de datos, sistemas operativos, redes, desarrollo, soporte técnico, aplicaciones), riesgos y controles de seguridad de la información.

Nota: Las actividades descritas en el presente rol serán realizadas por el Coordinador del Grupo de Trabajo de Infraestructura Tecnológica y Seguridad Informática.

4.6.8 CIO

La función principal de este rol es apoyar al Superintendente de Industria y Comercio y al Comité de seguridad de la información en la planeación estratégica de la seguridad de la información, es el responsable de planificar, organizar, coordinar, gestionar y controlar la estrategia de uso y apropiación de TI y la implementación del Modelo de Seguridad y Privacidad de la Información- MSPI.

Nota: Las actividades descritas en el presente rol serán realizadas por el Jefe de la Oficina de Tecnología e Informática de la SIC.

4.6.9 Comité de seguridad de la información

La función principal del comité, es asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

Las actividades específicas del comité son las siguientes:

- Coordinar la implementación del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.

- Revisar los diagnósticos del estado de la seguridad de la información en la Entidad.

- Acompañar e impulsar el desarrollo de proyectos de seguridad.

- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Superintendencia de Industria y Comercio.

- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.

- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.

- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.

- Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.

- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.

- Poner en conocimiento de la entidad, los documentos de seguridad que impacten de manera transversal a la misma.

- Promover el compromiso en el desarrollo y mejoramiento del SGSI.

- Discutir y aprobar las propuestas de implementación de medidas de seguridad de la información, cuya aplicación sea de carácter transversal a la operación de la Entidad.

- Procurar la consecución de los recursos humanos y físicos, necesarios para el desarrollo y mantenimiento del SGSI.

- Incorporar dentro de los ejercicios de planeación, los temas asociados al componente de Gestión de Tecnologías de la Información que hacen parte de la Política de Eficiencia Administrativa a ser implementada a través de la planeación sectorial e institucional de la Entidad.

- Realizar el seguimiento a los indicadores de gestión del Sistema de Gestión de Seguridad de la Información, y emitir un reporte al Superintendente de Industria y Comercio, indicando el desempeño obtenido, las acciones correctivas y de mejora continua.

Nota: Las actividades descritas en el presente rol, serán realizadas por el Comité Institucional de Gestión y Desempeño de la SIC.

4.7 Lineamientos generales de operación y mantenimiento del SGSI

- Todos los servidores públicos y/o contratistas de la SIC deben velar por la planeación, implementación, revisión y mejora continua del SGSI, y así mismo deben capacitarse adecuadamente para velar por la integridad, confidencialidad y disponibilidad de los activos de información que administran, gestionan y/o custodian.

- Todos los servidores públicos y/o contratistas de la SIC deben conocer y apoyar la gestión los riesgos a los que están expuestos los activos de información que maneja su dependencia.

5. RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

1. Se realiza una actualización general del documento en cuanto a numeración y contenido, incluyendo el cambio de nombre del documento. Se realizan ajustes a la política y el alcance del Sistema de Gestión de Seguridad de la Información. Se incluye información de contexto de la entidad, objetivos del SGSI, roles y responsabilidades.

_____

Fin documento