


	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN- SGSI



Diciembre de 2021

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

Control del Documento

Versión	Fecha	Autor	Páginas Afectadas	Referencia de Cambio
V1.0	03-01-2018	Fabio Rodrigo Pachón		Creación del Documento
V2.0	24-11-2021	Maryury Forero Bohorquez		Actualización Documento

Documentos Asociados

Nombre del Documento	Versión	Fecha
AGRI-SI-PO-002 POLITICA DE SEGURIDAD DE LA INFORMACIÓN.pdf	5	11-06-2020
NTC-ISO-IEC27001:2013		11-12-2013
GTC-ISO-IEC 27003		12-12-2012
SOA Canal Capital		20-10-2011
DOCUMENTO COMPES 3854 http://ticbogota.gov.co/sites/default/files/marco-legal/3854.pdf		11-04-2016

Aprobación del Documento

Versión	Autor	Referencia de Cambio
Autor	Fabio Rodrigo Pachón Arévalo	
Autor	Maryury Forero Bohorquez	
Aprobación	Mauris Antonio Avila	





	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

Tabla de contenido

1	Justificación	4
2	Objetivos.....	4
2.1	Objetivo General.....	4
2.2	Objetivos Específicos	4
3	Sistema de Seguridad de la Información - SGSI.....	5
3.1	Confidencialidad	5
3.2	Integridad	5
3.3	Disponibilidad	5
4	Para que sirve el SGSI	5
4.1	Vulnerabilidad.....	5
4.2	Riesgo	6
4.3	Amenaza	6
5	Que incluye el SGSI	6
5.1	Alcance y Limitaciones Preliminares del SGSI.....	6
5.2	Procedimientos y Mecanismos que soportan el SGSI.....	6
5.2.1	Política de Seguridad de la Información.....	6
5.2.2	Análisis de los Requisitos del SGSI	7
5.2.3	Determinar los Riesgos	7
5.2.4	Analizar los Riesgos	7
5.2.5	Valoración del Riesgo.....	8
5.2.6	Declaración de Aplicabilidad SOA	8
5.3	Diseño del SGSI	8
6	Implementación del SGSI	10
7	Tareas de la gerencia en el SGSI	11
7.1	Compromiso de la Dirección.....	11
7.2	Asignación de Recursos	11
7.3	Formación y Divulgación.....	11
7.4	Revisión del SGSI.....	11



	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

Índice de Tablas

Tabla 1 - Resumen de la Información Documentada para el SGSI	8
Tabla 2 - PDCA.....	10

Índice de Ilustraciones

Ilustración 1 - Análisis de Riesgos	7
Ilustración 2 - Ciclo PDCA.....	10

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

1 Justificación

Establecer un Sistema de Gestión de Seguridad de la Información permitirá que Canal Capital implemente los controles necesarios para garantizar la Confidencialidad, Integridad y Disponibilidad de la información, dando cumplimiento a la Norma NTC-ISO-IEC27001:2013 y los lineamientos dados por la Alta Consejería Distrital para las TIC establecidos en la Política Nacional de Seguridad Digital del Ministerio de Tecnologías de la Información y las Comunicaciones contenida en el documento CONPES 3854 versión aprobada el 11 de abril de 2016 y adoptando el Modelo de Seguridad y Privacidad de la Información – MSPI de la Política de Gobierno Digital, que se encuentra alineado con el Marco de Referencia de Arquitectura de TI.

La gestión de la seguridad de la información debe llevarse a cabo a través de un proceso documental y sistemático que debe ser transmitido a toda la organización.

2 Objetivos

2.1 Objetivo General



Proteger la información de Canal Capital preservando los criterios de Confidencialidad, Integridad y Disponibilidad.

2.2 Objetivos Específicos

- Apoyar el desarrollo de la seguridad de la información de Canal Capital coordinando los procesos de Gestión de Recursos Físicos y Tecnológicos.
- Identificar y llevar los riesgos sobre la seguridad de la información a niveles aceptables.
- Elaborar un plan de acción que permita mitigar el impacto de las amenazas, riesgos y vulnerabilidades valoradas en el análisis de riesgos y ofrecer las medidas pertinentes que permitan tener planes de acción y respuestas a los riesgos identificados.
- Realizar una auditoria con el fin de verificar el nivel de cumplimiento con la NTC-ISO-IEC27001:2013.

3 Sistema de Seguridad de la Información - SGSI

El Sistema de Gestión de Seguridad de la Información permite mantener la confidencialidad, integridad y disponibilidad de la Información, así como todos los sistemas involucrados en su tratamiento y divulgación dentro de Canal Capital.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

3.1 Confidencialidad

*La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.*¹

Atributo que deben tener los datos o la información, que garantiza la de esta para que sea divulgada únicamente por personas o entidades autorizadas por el Canal Capital, en el momento que se requiera.

3.2 Integridad

*Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.*²

Atributo que deben tener los datos o la información, para que no sean alterados ni destruidos por personas o entidades no autorizadas por el Canal Capital, garantiza la veracidad de la información entregada.

3.3 Disponibilidad

*Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.*³

Atributo que deben tener los datos o la información, para que sean consultados y tratados por personas o entidades autorizadas por el Canal Capital, en el momento que se requiera.

4 Para qué sirve el SGSI

El *Sistema de Gestión de Seguridad de la Información* ayuda a establecer políticas y procedimientos con el fin de minimizar los siguientes factores que pueden afectar la información y continuidad del negocio:



4.1 Vulnerabilidad

¹ http://www.iso27000.es/download/doc_sgsi_all.pdf

² http://www.iso27000.es/download/doc_sgsi_all.pdf

³ http://www.iso27000.es/download/doc_sgsi_all.pdf

Todas aquellas fallas, omisiones, o deficiencias de seguridad que pueden ser aprovechadas por cualquier individuo para poner en riesgo la información o la continuidad del negocio.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

4.2 Riesgo

Probabilidad que ocurra un hecho que afecte la información o la continuidad de negocio.

4.3 Amenaza

Potencial ocurrencia de que un hecho que afecte la información o la continuidad del negocio pueda manifestarse, es la materialización del riesgo

El Sistema de Gestión de Seguridad de la Información permite conocer los riesgos, vulnerabilidades y amenazas a las que está expuesta la entidad, así mismo se encarga de mitigar, minimizar y controlar.

5 Que incluye el SGSI

5.1 Alcance y Limitaciones Preliminares del SGSI

El alcance inicial preliminar del SGSI comprende la política de seguridad de la información, los procedimientos y controles para mantener los pilares de la información Confidencialidad, Integridad y Disponibilidad transmitida y procesado por funcionarios de Canal Capital, enfocado en la Norma NTC-ISO-IEC 27001:2013.

Las limitaciones preliminares del SGSI son las siguientes:

- Disponibilidad de tiempo.
- Recursos Económicos.
- Recursos Software y Hardware.
- Cambio continuo del personal a cargo.

5.2 Procedimientos y Mecanismos que soportan el SGSI

Los procedimientos describen de forma detallada las actividades y como se van a llevar a cabo, los recursos que se usan, los métodos y que alcance se pretende obtener, a través de unas etapas de trabajo enunciadas a continuación.



5.2.1 Política de Seguridad de la Información

Documento en el cual están establecidos los dominios y controles, que permiten la regulación de la Seguridad de la Información al interior del Canal Capital.

5.2.2 Análisis de los Requisitos del SGSI

De acuerdo con lo establecido en la Norma ISO/IEC 27003:2010 para establecer los requisitos de la seguridad de la información se deben tener en cuenta cinco elementos:⁴

- Identificar los activos de información importantes
- Visión de la Entidad y sus efectos sobre los requisitos futuros.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

- Aplicaciones, Redes, Recursos de TI.
- Requisitos Legales y reglamentarios.
- Conciencia sobre la seguridad de la información.

5.2.3 Determinar los Riesgos

En esta fase se debe realizar un estudio previo para determinar los riesgos, vulnerabilidades y amenazas para algunos de los sistemas que se encuentran en funcionamiento actualmente en Canal Capital. (Servidores, Red LAN, Estaciones de Trabajo, Software, Sistemas de Información).

Se deben llevar a cabo entrevistas, inventario de activos importantes de la entidad, visitas programadas por entidades externas con experticia en Seguridad de la Información y pruebas realizadas por los Profesionales en Sistemas de Canal Capital, donde se dan a conocer las debilidades o vulnerabilidades encontradas dentro de la entidad.

5.2.4 Analizar los Riesgos

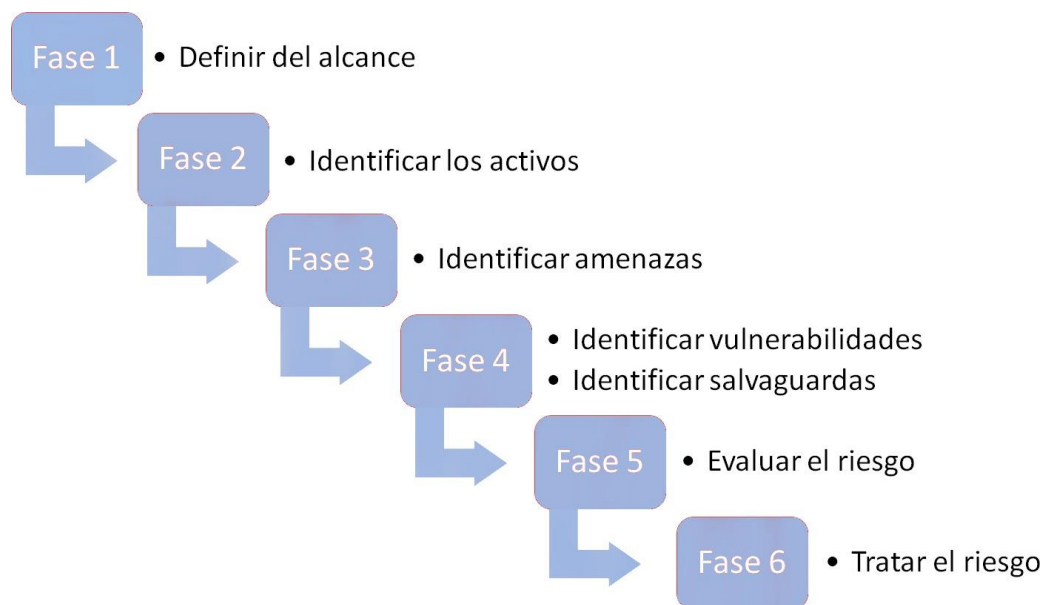




Ilustración 1 - Análisis de Riesgos

4

http://www.funcionpublica.gov.co/eva/admon/files/empresas/ZW1wcmVzYV83Ng==/imagenes/4495/Methodolog%C3%ADa_implementaci%C3%B3n_%20SGSI_basado_en_normas%20ISO:IEC%2027000.pdf

En esta etapa de implantación del SGSI se utiliza el método Magerit que permite valorar los riesgos, identificando el origen y permitiendo delimitar un sistema de control que ayude a disminuir el impacto que pueda tener alguno de estos sobre la entidad.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

La aplicación de listas de chequeo y cuestionarios permiten establecer la existencia de controles de seguridad, estos sirven como evidencia para confirmar los hallazgos y definir los controles que sean necesarios.⁵

5.2.5 Valoración del Riesgo

Eje principal del SGSI, se deben tener en cuenta los parámetros de probabilidad de ocurrencia, parámetros de impacto, vulnerabilidad y criterios de aceptación del riesgo.

5.2.6 Declaración de Aplicabilidad SOA

Documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

5.3 Diseño del SGSI

El diseño del SGSI se contempla en tres componentes:



1. Documentación del Sistema – Tabla 1⁶
2. Implementación de Controles del Plan de Tratamiento de Riesgos
3. Monitoreo constante de la Seguridad de la Información

Tabla 1 - Resumen de la Información Documentada para el SGSI

Numeral	ISO-TEC 27001	Documentación
4.3	Determinación del Alcance del SGSI	El alcance debe estar disponible como información documentada.
5.2	Política de Seguridad	La política de seguridad debe estar disponible como información documentada.
6.1.2	Valoración de riesgo de seguridad de la información	Información documentada acerca del proceso de valoración de riesgos de la seguridad de la información.
6.1.3	Tratamiento de riesgos de la seguridad de la información	Información documentada acerca del proceso de tratamiento de riesgos de la seguridad de la información.
6.1.3	Declaración de aplicabilidad	Declaración de aplicabilidad.
6.2	Objetivos de seguridad de la información y planes para lograrlos	Objetivos de la seguridad de la información.

⁵ <http://www.rte.espol.edu.ec/index.php/tecnologica/article/viewFile/456/321>

⁶ <<Revista Ibérica de Sistemas y Tecnologías de la Información>>, 2017, <http://www.funcionpublica.gov.co/eva/admon/files/empresas/> (Consultada el 4 de enero de 2018)

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

Numeral	ISO-TEC 27001	Documentación
7.2	Competencia	Evidencia de la competencia de las personas relacionadas con la seguridad de la información.
7.5	Información documentada	La que la entidad determine que es necesaria para el SGSI.
7.5.3	Control de la información documentada	La información documentada de origen externo.
8.1	Planificación y control operacional	Información documentada para tener confianza de que los procesos se han llevado a cabo de acuerdo con la planificación.
8.2	Valoración de la seguridad de la información	Resultados de las valoraciones de riesgos de la seguridad de la información.
8.3	Tratamiento de riesgos de la seguridad de la información	Resultados de los tratamientos de riesgos de la seguridad de la información.
9.1	Seguimiento, medición, análisis y evaluación.	Evidencia de los resultados del monitoreo y la revisión.
9.2	Auditoria interna	Conservar la información documentada como evidencia de la implementación del programa de auditoria y los resultados de esta.
9.3	Revisión por la dirección	Evidencia de los resultados de la revisión por la Dirección.
10.1	No conformidades y acciones correctivas	Naturaleza de las no conformidades y cualquier acción posterior tomada.
10.1	No conformidades y acciones correctivas	Resultados de cualquier acción correctiva.

6 Implementación del SGSI

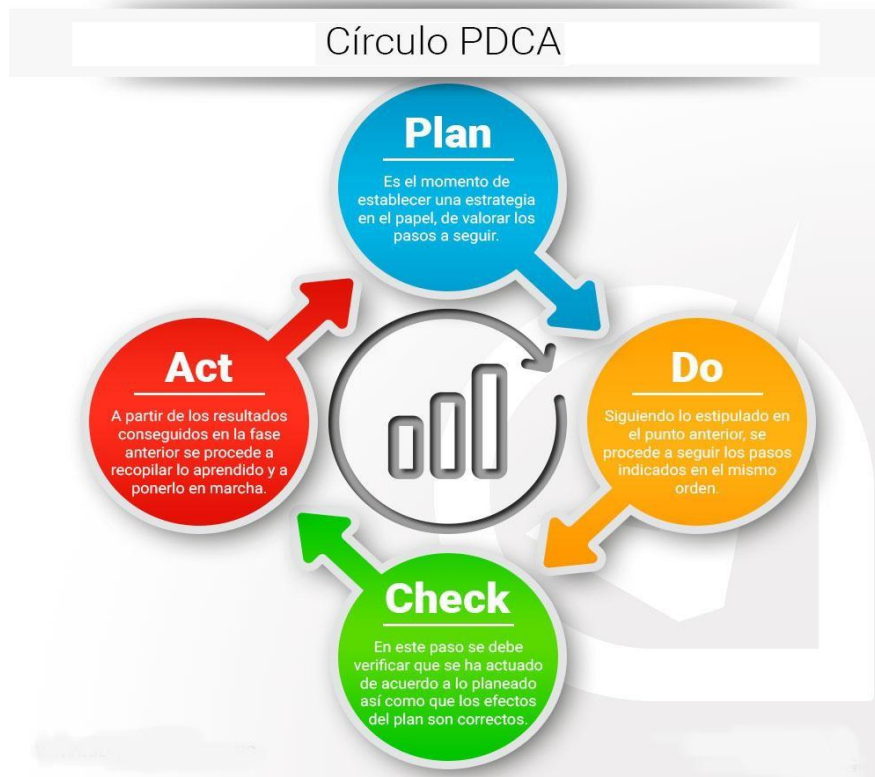




Ilustración 2 - Ciclo PDCA

Tabla 2 - PDCA

Plan (Planear) – Establecer el SGSI	Do (Hacer) – Implementar y Establecer el SGSI
<ul style="list-style-type: none"> Definir el alcance. Política SGSI. Análisis de Riesgos. Selección de Controles. Aceptación de los Riesgos Residuales. Autorización. SOA 	<ul style="list-style-type: none"> Tratamiento de Riesgos. Definir Métricas. Programas de Formación. Gestión de la operación. Plan de Respuesta a Incidentes.
Check (Verificar) – Monitorear el SGSI	Act (Actuar) – Mantener y Mejorar el SGSI
<ul style="list-style-type: none"> Supervisar. Revisar Eficacia del SGSI. Auditorías Internas. Actualizar Planes de Seguridad. Mantenimiento de Registros. 	<ul style="list-style-type: none"> Implementar Mejoras. Aplicar Medidas Correctivas y Correctivas. Comunicar las Acciones. Asegurar el Cumplimiento de Objetivos.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

7 Tareas de la gerencia en el SGSI

7.1 Compromiso de la Dirección

Es parte fundamental en la implantación de un SGSI y su mejora continua, el apoyo de la Alta Dirección de Canal Capital, ya que repercute directamente en el cumplimiento de la misión de la entidad.

- Asegurarse de que se establecen objetivos y planes del SGSI.
- Establecer roles y responsabilidades de seguridad de la información.
- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas.

7.2 Asignación de Recursos

- Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.
- Garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.
- Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
- Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.
- Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de estas.
- Mejorar la eficacia del SGSI donde sea necesario.

7.3 Formación y Divulgación

- Intranet.
- Campañas de expectativa.
- Capacitaciones por parte del área de sistemas.
- Correos Corporativos.

7.4 Revisión del SGSI

- Auditorias.
- Informes de estado de las acciones correctivas y preventivas.
- Recomendaciones de mejora.
- Cambios que afecten el SGSI.
- Actualización de Riesgos.