



Agencia Nacional de Contratación Pública



Colombia Compra Eficiente

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA - COLOMBIA  
COMPRAS EFICIENTES

## Director General

José Andrés O'Meara Riveira

## Secretaria General

Claudia Ximena López Pareja

### Subdirector de Negocios

Andrés Ricardo Mancipes González

### Subdirector de Gestión Contractual

Jorge Augusto Tirado Navarro

### Subdirectora de Estudios de Mercado y Abastecimiento Estratégico (EMAE)

Catalina Pimienta Gomez

### Subdirector de Información y Desarrollo Tecnológico (IDT)

Rigoberto Rodríguez Peralta

### Asesor Económico

Steven Orozco Rodríguez

### Asesor Jurídico

Juan David Marín López

### Asesora Comunicaciones

Fabiana de la Espriella Salcedo

### Asesor Subdirección IDT

Juan Camilo Arango Medina

### Asesora Planeación

Karina Blanco Marín

### Asesora Control Interno

Judith Gómez Zambrano

## CONTENIDO

INTRODUCCIÓN .....	1
1 OBJETIVO GENERAL .....	2
2 OBJETIVOS ESPECÍFICOS .....	2
3 DEFINICIONES.....	2
4 Marco Legal.....	3
5 Alcance y aplicabilidad.....	3
6 Establecimiento y Gestión.....	4
7 Plan de Seguridad y Privacidad de la Información.....	4
a) Fase de Diagnóstico.....	4
b) Fase de Planeación y/o Planificación.....	4
c) Fase de Implementación.....	5
d) Fase de Evaluación del Desempeño.....	5
e) Fase de Mejora Continua.....	5
8 Plan Operativo del Modelo de Privacidad y Seguridad de la Información.....	5
9 Control de documentos.....	14
10 Seguimiento y actualización.....	15
11 FICHA TÉCNICA DE DOCUMENTO Y CONTROL DE CAMBIOS.....	15

## INTRODUCCIÓN

La Agencia Nacional de Contratación Pública-Colombia Compra Eficiente (en adelante, ANCP-CCE) en el desarrollo, cumplimiento y fortalecimiento de su Modelo

de Seguridad y Privacidad de la Información [en adelante, MSPI] que es establecido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones-MintIC, elabora el presente Plan de Seguridad y Privacidad de la información en el desarrollo de sus objetivos estratégicos y el cumplimiento normativo y regulatorio aplicable.

## 1 OBJETIVO GENERAL

Trazar y planificar las acciones tendientes a fortalecer la Seguridad y Privacidad de la información de la ANCP-CCE acorde a la estrategia de seguridad y privacidad de la información del MSPI adoptado y la Política Nacional de Gobierno Digital.

## 2 OBJETIVOS ESPECÍFICOS

- o Elaborar el Plan de Seguridad y Privacidad de la información de la ANCP-CCE para la vigencia 2022<sup>1</sup>.
- o Incrementar y fortalecer el nivel de madurez en la gestión de la Seguridad y Privacidad de la información dentro de la ANCP-CCE.
- o Dar cumplimiento a lo establecido por el Decreto 612 de 2018, la Ley 1581 de 2012, Decreto 1377 de 2013, Decreto 886 de 2014 y demás normatividad vigente de Privacidad y Protección de Datos Personales que sea aplicable.

## 3 DEFINICIONES.

**Activo de información:** Es toda aquella información o elemento que reside en medio electrónico o físico, que tiene un significado y valor para la Entidad y por ende necesita ser protegido.

**Confidencialidad:** es el principio de la Seguridad de la información que busca asegurar que la información de la Entidad sea accedida únicamente por el personal autorizado.

<sup>1</sup> El instrumento de Evaluación MSPI, es una herramienta creada por el Ministerio de las 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, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Política de Gobierno Digital en su componente de Seguridad y Privacidad de la Información. <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

**Disponibilidad:** Es el principio de la Seguridad de la información que busca asegurar que la información de la Entidad sea accesible y utilizable cuando sea requerida.

**Integridad:** Es el principio de la Seguridad de la información que busca asegurar que la información esté protegida contra modificaciones no autorizadas, con el fin de garantizar su constancia, exactitud y completitud.

**MSPI:** Es el Modelo de Seguridad y Privacidad de la Información, establecido por el Ministerio de las Tecnologías de la Información y las Comunicaciones-MinTIC, el cual está determinado por las necesidades objetivas, los requisitos de Seguridad, los procesos, el tamaño y la estructura de la Entidad con el objetivo de preservar la Confidencialidad, Integridad y Disponibilidad de los activos de información, garantizando su buen uso y la Privacidad de los datos.

**Seguridad de la información:** Es el conjunto de medidas que buscan preservar la Confidencialidad, Integridad y Disponibilidad de la información de la Entidad.

#### 4 MARCO LEGAL.

**Decreto 612 de 2018.** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.

**Decreto 1008 de 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

**Guías-Modelo de Privacidad y Seguridad de la Información MSPI-** Ministerio de Tecnologías de la información y las comunicaciones -MinTIC.

**Resolución 500 de 2021** se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital

#### 5 ALCANCE Y APLICABILIDAD.

El alcance del presente Plan Operativo del Modelo de Seguridad y Privacidad de la Información aplica todos los procesos de la Entidad en concordancia con el alcance del Modelo de Seguridad y Privacidad de la Información- MSPI.

## 6 ESTABLECIMIENTO Y GESTIÓN.

El grupo de Seguridad y Privacidad de la Información de la ANCP-CCE, por medio del uso de la herramienta “*Instrumento de Evaluación MSPI*”, creada por el MinTIC, ejecutó el auto diagnóstico con el fin de identificar el nivel de madurez en la implementación del MSPI en la Entidad, permitiéndole evidenciar y establecer el estado de la gestión y de los riesgos en la Seguridad y Privacidad de la Información dentro en la ANCP-CCE y posibilitándole fijar metas y objetivos a desarrollar por medio del presente Plan Operativo del Modelo de Seguridad y Privacidad de la Información de acuerdo con la estructura interna y los Activos de información de la Entidad.

Las funciones del comité de Seguridad de la Información son asumidas por el Comité Institucional de Gestión y Desempeño.

## 7 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

A continuación, se listan las fases establecidas por parte del grupo de Seguridad y Privacidad de la información de la ANCP-CCE como marco de referencia del presente Plan, teniendo en cuenta las fases definidas en el ciclo de operación del Modelo de Seguridad y Privacidad de la Información [MSPI]<sup>2</sup>:

### a) Fase de Diagnóstico.

Se debe ejecutar el Diagnóstico del MSPI por medio de la herramienta del “Instrumento de Evaluación MSPI” del MinTIC, con el fin de, realizar el reconocimiento, valoración y el nivel de cumplimiento y madurez de los requisitos de Seguridad y Privacidad de la Información en la Entidad. Así mismo, en esta fase se debe definir el enfoque para la valoración, análisis, evaluación y tratamiento de los riesgos que le permita a la ANCP-CCE: identificar los activos de información dentro del alcance del MSPI, los propietarios de los activos, los riesgos, amenazas y las vulnerabilidades.

### b) Fase de Planeación y/o Planificación.

En esta fase se establecen los objetivos a alcanzar y las actividades del proceso

<sup>2</sup> Modelo PHVA: Planificar, Hacer, Verificar y Actuar. <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

susceptibles de mejora. El resultado de la fase de planeación le permite a la ANCP-CCE establecer desde el nivel de madurez del Modelo de Seguridad de la Información y de los riesgos identificados, fijar el mapa de ruta y establecer las actividades que deben desarrollarse para el avance y monitoreo del MSPI.

#### c) Fase de Implementación.

Esta fase le permite a la ANCP-CCE ejecutar e implementar las acciones y actividades a corto, mediano y largo plazo que fueron establecidas e identificadas en la fase de planificación, con el fin de incrementar el nivel de madurez del MSPI.

#### d) Fase de Evaluación del Desempeño.

Esta fase le permite a la Entidad, una vez implementadas las actividades planeadas en el presente plan, establecer un periodo de prueba para verificar la eficacia de las acciones propuestas.

#### e) Fase de Mejora Continua.

Debido a que la información no es estática, esta fase le permite a la Entidad analizar los resultados de las acciones implementadas, así como, identificar las acciones correctivas y preventivas que sean pertinente de acuerdo con los objetivos previstos en la implementación del MSPI. Las acciones de esta fase solo podrán ejecutarse una vez implementadas las anteriores fases y teniendo en cuenta los resultados de los incidentes, retroalimentaciones y/o autoevaluaciones realizadas de forma periódica en la Entidad.

## 8 PLAN OPERATIVO DEL MODELO DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

Una vez culminada las actividades del MSPI de la fase de Planificación, se llevó a cabo la revisión de la implementación de los controles, con el fin de dar cumplimiento con los requisitos y objetivos del MSPI.

La fase de implementación del MSPI permitió a la ANCP-CCE validar los requisitos presentados tanto por la Política como el Manual de Seguridad y Privacidad de la Información; de igual manera, los controles de Seguridad de la información, que por normativa o por resultado de la valoración de riesgos se deberían implementar. En la fase de preparación se establecerá las actividades y la programación para la implementación tanto de los requisitos, controles y buenas prácticas de seguridad y

privacidad de la información en la ANCP-CCE. Como estrategia interna para la orientación de los propósitos de seguridad y privacidad de la información, se definen e implementan políticas y directrices que guíen las prácticas de protección de la información en cuanto a su confidencialidad, integridad y disponibilidad.

La operación del Modelo de Seguridad y Privacidad de la Información – MSPI tiene los siguientes pilares:

- Gestión de los activos de información
- Gestión de riesgos de seguridad de la información – Riesgos digitales
- Gestión de incidentes de seguridad
- Gestión en la continuidad de la operación [BCP – Seguridad Operativa - Vulnerabilidades]
- Cumplimiento normativo y legal – Gobierno Digital
- Plan de capacitación y sensibilización
- Protección de datos personales
- Mejora continua



## Situación actual

EL SGSI es aplicable a los activos de información de todos los procesos de la ANCP-CCE, verificándolo y aplicándolo, comprende las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con la declaración de aplicabilidad de la ejecución de los controles de la ISO 27002, a los siguientes grupos de controles a la fecha no están adoptados en su totalidad en la ANCP-CCE:

- A 6.2 Dispositivos móviles y teletrabajo
- A 14.2.6 Ambiente de desarrollo seguro
- A 14.2.8 Pruebas de seguridad de sistemas

La ANCP-CCE ha realizado actividades tendientes a la adopción del Modelo de Seguridad y Privacidad de la Información, para lo cual se tiene aprobada por la alta dirección la Política y el Manual de Seguridad y Privacidad de la Información, obteniendo

la adopción de controles en diferentes áreas dentro de la Agencia alineándose con los siguientes frentes:

- Selección de personal.
- Terminación o cambio de responsabilidades de empleo.
- Devolución de Activos.
- Cancelación o ajuste de los derechos de acceso.
- Seguridad de oficinas, salones e instalaciones.

Acorde al plan de implementación del MSPI se debe documentar e implementar los siguientes controles mediante su incorporación en los procedimientos de seguridad:

- Procedimiento de monitoreo y capacidad de recursos tecnológicos.
- Procedimiento Borrado seguro de medios
- Procedimiento gestión de medios removibles.
- Procedimiento cambios estándares de los recursos tecnológicos.
- Actualizar Política de control de acceso.
- Procedimiento control de acceso remoto.
- Actualizar Política y herramienta de cifrado
- Procedimiento para activar factores múltiples de autenticación [MFA] en las cuentas de correo y otros sistemas



- Procedimiento cifrado de contraseña
- Procedimiento para enmascarar datos personales o confidenciales en ambientes pre - productivos.

Teniendo en cuenta la política y manual de seguridad y privacidad de la información aprobado y el resultado del análisis del estado actual de la implementación de seguridad y privacidad de la información, para la vigencia 2022 se establece el siguiente Plan Operativo del Modelo de Seguridad y Privacidad de la Información:

Gestión	Descripción de las Actividades	Meta	Fechas de programación	
			Primer Semestre	Segundo Semestre
Activos	Actualizar los lineamientos para el levantamiento de activos de información	Metodología levantamiento de activos de información		X
	Identificar los activos de la información y la evaluación de su criticidad	Formato de activos de información		X
	Identificar el Índice de Información Clasificada y Reservada	Formato con el Índice de Información Clasificada y Reservada		X
	Publicación en la página WEB de los Activos de Información y del Índice de Información Clasificada y Reservada.	Formato de activos de información y Formato con el Índice de Información Clasificada y Reservada		X



Gestión	Descripción de las Actividades	Meta	Fechas de programación	
			Primer Semestre	Segundo Semestre
Riesgo	Actualización, valoración, evaluación de los riesgos de seguridad digital; identificación de los controles establecidos para mantener la confidencialidad, integridad y disponibilidad de la información en la ACNP-CCE conforme a la actualización realizada a los activos de información en la vigencia 2021.	Matriz de Riesgos Digitales	X	
	Formulación de planes de tratamiento de riesgo de seguridad digital	Matriz de Riesgos Digitales	X	
	Seguimiento a la implementación de los planes de tratamiento de riesgos de seguridad digital	Matriz de Riesgos Digitales	X	
	Actualización Guía Gestión de Riesgos Seguridad de la información, alineada a las actualizaciones de la metodología aprobada en la entidad	Gestión Tratamiento de riesgos digitales	X	
Sensibilización	Realizar sesiones de sensibilización de seguridad de la información.	Enterates, Capacitaciones	X	X



Gestión	Descripción de las Actividades	Meta	Fechas de programación	
			Primer Semestre	Segundo Semestre
	Participar en la inducción y reinducción de los funcionarios de la entidad con charlas en materia de seguridad de la información y protección de datos personales.	Capacitaciones	X	X
	Socialización de la documentación, controles y herramientas del MSPI	Capacitaciones	X	X
Ciberseguridad	Validar y dar cumplimiento a lo definido en el Plan Nacional de Protección de Infraestructuras Críticas Cibernéticas	Informe		X
	Servir como punto de Contacto con el CSIRT ColCERT para realizar la gestión de eventos e incidentes de seguridad de la información que afecten los servicios o la infraestructura de la Agencia	Informe	X	X
Incidentes	Acompañar en la gestión de acciones de respuesta frente a eventos e incidentes de seguridad de la información	Informe	X	X



Gestión	Descripción de las Actividades	Meta	Fechas de programación	
			Primer Semestre	Segundo Semestre
	Revisión, actualización y publicación del procedimiento de incidentes de seguridad de la información.	Procedimiento de Incidentes de Seguridad		X
Seguridad operativa	Documentar los controles de seguridad de la información que permiten el cumplimiento de los requisitos legales en materia de seguridad de la información obligatorios para la Entidad	Matriz de Riesgos Digitales		X
	Establecer los niveles de acceso, limitar y monitorear el acceso a los datos, código fuente, equipos y demás componentes tecnológicos requeridos por el personal técnico para el desarrollo, mantenimiento, administración, operación y soporte de la ANCP-CCE	Matriz de Roles y perfiles		X
BCP	Definir los marcos de tiempo aceptables para recuperar la información	Prueba del DRP		X



Gestión	Descripción de las Actividades	Meta	Fechas de programación	
			Primer Semestre	Segundo Semestre
	y sistemas críticos de la ANCP-CCE			
	Establecimiento de planes de contingencia, continuidad del negocio y requerimientos de recuperación en caso de desastre.	BCP - DRP		X
Mejora Continua	Hacer seguimiento a las observaciones o recomendaciones de las Acciones Correctivas y Oportunidades de Mejora	Informe	X	X
	Realizar revisiones periódicas de seguridad y privacidad de la información en la infraestructura y sistemas de la ANCP-CCE, para verificar el cumplimiento de las Políticas y normas de seguridad y privacidad de la información.	Informe	X	X
	Realizar la evaluación de la efectividad de los controles de seguridad de la información adoptados por la Entidad para el	Informe	X	X

Gestión	Descripción de las Actividades	Meta	Fechas de programación	
			Primer Semestre	Segundo Semestre
	tratamiento de los riesgos de seguridad Digital			
	Acompañar la elaboración de los componentes del plan estratégico de gestión de seguridad de la información de la Entidad	Informe	X	X
	Actualizar los indicadores de eficacia, eficiencia y efectividad del Sistema de Seguridad y privacidad de la información	Informe	X	X
Gobierno digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Informe		X
	Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Informe		X
Protección de datos personales	Inventario de bases de datos personales de acuerdo con los	Inventario	X	



Gestión	Descripción de las Actividades	Meta	Fechas de programación	
			Primer Semestre	Segundo Semestre
	estándares emitidos por la SIC			
	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Inventario	X	
	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Inventario	X	
Vulnerabilidades	Coordinar el análisis de vulnerabilidades en la entidad y la realización de sus informes.	Informe	X	
	Apoyar el desarrollo de pruebas de ingeniería social para evaluar el nivel de conciencia en seguridad de la información de los colaboradores de la Entidad	Informe	X	

## 9 CONTROL DE DOCUMENTOS.

Los documentos que sean proyectados y/o elaborados por el grupo de Seguridad



de la Información de la Subdirección IDT de la ANCP-CCE en el ejercicio y desarrollo del presente Plan de Seguridad y Privacidad de la información, se deben proteger y controlar de acuerdo con los lineamientos internos estipulados por la Entidad y, por lo tanto, pasar por el ciclo de revisión, aprobación y publicación definido, por la misma.

## 10 SEGUIMIENTO Y ACTUALIZACIÓN.

El grupo de Seguridad y Privacidad de la Información de la Subdirección de IDT de la ANCP-CCE es el encargado de ejecutar, revisar y hacer seguimiento al avance del Plan Operativo del Modelo de Seguridad y Privacidad de la información, así como de su correcto cumplimiento.

## 11 FICHA TÉCNICA DE DOCUMENTO Y CONTROL DE CAMBIOS

FICHA TECNICA DE DOCUMENTO: 1. IDENTIFICACIÓN Y UBICACIÓN	
Título del documento:	Plan de Seguridad y Privacidad de la Información
Fecha de aprobación:	25 de noviembre de 2022
Resumen / Objetivo de contenido:	Trazar y planificar las acciones tendientes a fortalecer la Seguridad y Privacidad de la información en la Entidad, en el desarrollo y la ejecución del MSPI y la Política Nacional de Gobierno Digital en los procesos, servicios, infraestructura y en general en los activos de información de la ANCP-CCE.
Area / Dependencia de autoría:	Subdirección de Información y Desarrollo Tecnológico
Código de estandarización:	CCE-SGI-PL-01
Categoría / Tipo de documento:	Plan
Aprobación por:	CIGD
Información adicional:	
Serie documental según TRD	DG.SIDT.30.4 Manuales de Seguridad de la Información





Link de ubicación original del documento (especifique donde se aloja o reposa el documento)	<a href="https://cceeficiente.sharepoint.com/:f:/r/cce/Documentos%20compartidos/SIDT/GESTI%C3%93N%20SEGURIDAD%20DE%20LA%20INFOR/2021/DG.SIDT.30.4%20Manuales%20de%20Seguridad%20de%20la%20Informaci%C3%B3n?csf=1&amp;web=1&amp;e=dReSFZ">https://cceeficiente.sharepoint.com/:f:/r/cce/Documentos%20compartidos/SIDT/GESTI%C3%93N%20SEGURIDAD%20DE%20LA%20INFOR/2021/DG.SIDT.30.4%20Manuales%20de%20Seguridad%20de%20la%20Informaci%C3%B3n?csf=1&amp;web=1&amp;e=dReSFZ</a>
--	---

**FICHA TECNICA DE DOCUMENTO: 2. AUTORES Y RESPONSABLES DE REVISIÓN Y APROBACIÓN**

ACCIÓN	NOMBRE	CARGO/ PERFIL	FECHA	FIRMA
Elaboró	Milena Cabrales	Contratista Líder de Seguridad	09/11/2021	Milena Cabrales
Revisó	Rigoberto Rodríguez Peralta	Subdirector de IDT	19/11/2021	Rigoberto Rodríguez
Aprobó	CIGD	CIGD	25/11/2021	Acta del 25 de noviembre del 2021

**Nota:** Si la aprobación se realizó mediante acta de alguno de los comités internos considerados en la resolución número 173 de 2020 por favor especificar acta y mes del desarrollo de esta.

3. CONTROL DE CAMBIOS DE DOCUMENTO			Versión vigente del documento:		01
VERSIÓN	FECHA	DESCRIPCIÓN DE AJUSTES	ELABORÓ	REVISÓ	APROBÓ
3	25/11/2021	Actualización del documento; y se hace modificación del código del proceso de seguridad al Macroproceso de GTI, dado	Milena Cabrales	Rigoberto Rodríguez	Comité Institucional de Gestión y Desempeño



# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CCE-GTI-PL-01

V.03 25 de noviembre de 2021



		que todos los procesos de tecnología fueron agrupados en este macroproceso.			
2	22/12/2020	Actualización del documento	Ana Cárdenas	Rigoberto Rodríguez	Comité Institucional de Gestión y Desempeño
1	8/02/2019	Creación del documento	Frederick Ferro Mojica Luis Alejandro Ruiz	Dana Pineda Marin	Comité Institucional de Gestión y Desempeño

-----  
**Nota:** El control de cambios en el documento, se refiere a cualquier ajuste que se efectúe sobre el documento que describe ficha técnica del presente documento.



**Colombia Compra Eficiente**

Tel. (+57 1)7956600 • Carrera 7 No. 26 - 20 Piso 17 • Bogotá - Colombia



[www.colombiacompra.gov.co](http://www.colombiacompra.gov.co)