Agencia Nacional
de Contratación Pública
Colombia Compra Eficiente

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA -COLOMBIA COMPRA EFICIENTE – 2026

TABLA DE CONTENIDO

LISTADO DE TABLAS

1. INTRODUCCIÓN

La Subdirección de Información y Desarrollo Tecnológico (SIDT) de la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente (ANCP-CCE), ha elaborado el presente Plan de Seguridad y Privacidad de la Información con el fin de avanzar, fortalecer y cumplir con su Modelo de Seguridad y Privacidad de la Información (MSPI). Este modelo ha sido establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y se enmarca en el desarrollo de los objetivos misionales y estratégicos de la ANCP-CCE, orientados a la protección de los activos de información y al cumplimiento de la normativa vigente en materia de Seguridad de la Información.

El presente Plan se alinea con las Políticas de Seguridad y Privacidad de la Información de la ANCP-CCE, en cumplimiento de las disposiciones establecidas en la normativa vigente y aplicable en seguridad de la información, incluyendo los lineamientos del MSPI. Dichas políticas regulan la responsabilidad de la ANCP-CCE en la gestión y protección de la información de la Entidad, garantizando la confidencialidad, integridad y disponibilidad de los activos de información, así como la implementación de medidas para prevenir y mitigar los riesgos asociados a la seguridad de la información.

Como infraestructura crítica del Estado, la ANCP-CCE debe garantizar la capacidad y fortalecimiento de sus sistemas y procesos para proteger la información. La eficacia en la seguridad de la información no sólo respalda la integridad del sistema de contratación pública, sino que también asegura la estabilidad de los diferentes objetivos misionales y funciones clave de la Entidad en relación con sus diferentes grupos de interés.

2. OBJETIVO

General

Definir, desarrollar y planificar las acciones y actividades necesarias para fortalecer el componente de Seguridad de la Información de la ANCP-CCE, en desarrollo y cumplimiento de sus políticas internas y del Modelo de Seguridad y Privacidad de la Información (MSPI). Lo anterior, garantizando que las actividades operativas se encuentren alineadas con identificación y evaluación de riesgos de seguridad de la

información, la implementación de controles adecuados y la protección de los activos críticos.

Específicos

- Establecer el Plan de Seguridad y Privacidad de la Información de la ANCP-CCE.
- Incrementar y fortalecer el nivel de madurez en la gestión de la seguridad de la información dentro de la ANCP-CCE.
- Garantizar la ejecución de análisis de riesgos y brechas para identificar amenazas y vulnerabilidades en los sistemas de información.
- Implementar estrategias de ciberdefensa para proteger contra ataques cibernéticos y riesgos emergente, con el fin de mejorar la resiliencia frente a amenazas digitales.
- Establecer mecanismos de monitoreo y auditoría continua para evaluar la efectividad del Plan de Seguridad y Privacidad de la Información y asegurar el cumplimiento constante con las normativas aplicables.
- Identificar y aplicar las acciones correctivas necesarias para optimizar la gestión de seguridad de la información en la Entidad.
- Fomentar la cultura de seguridad de la información dentro de la ANCP-CCE mediante la capacitación y concienciación continua de todos los colaboradores sobre las mejores prácticas en privacidad y seguridad de la información.

3. ALCANCE

Este Plan de Seguridad y Privacidad de la Información aplica a todas las actividades, procesos, sistemas, aplicaciones, redes, bases de datos, documentos físicos y digitales que involucren el manejo, almacenamiento, procesamiento y transmisión de información dentro de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE).

Su aplicación incluye a todos los funcionarios, contratistas, proveedores y terceros que tengan acceso a los activos de información de la Entidad, abarcando todas las áreas, subdirecciones y grupos internos de trabajo. Asimismo, contempla la protección integral de la información en sus formas digital y física, garantizando la confidencialidad, integridad y disponibilidad, en cumplimiento de las normativas vigentes y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).

El cumplimiento del Plan es obligatorio para todos los actores mencionados y será objeto de auditorías periódicas con el fin de evaluar su efectividad, identificar oportunidades de mejora y asegurar que la seguridad de la información se mantenga en niveles óptimos.

4. 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.

- **Amenaza:** Cualquier circunstancia o evento que tenga el potencial de causar daño a los activos de información, ya sea de forma accidental o intencionada.

- **Base de datos:** Conjunto estructurado de datos personales que se encuentran almacenados en un soporte electrónico, documental o en otro formato que permita su consulta y procesamiento.

- **Control de Seguridad:** Medida o mecanismo diseñado para prevenir, detectar, corregir o minimizar el impacto de amenazas y vulnerabilidades en los activos de información.

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

- **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.

- **Evento de seguridad:** Es cualquier situación o incidente que pueda afectar la seguridad de una red de computadoras o de un sistema. Puede ser una señal de una posible amenaza a la seguridad o un comportamiento inusual.

- **Incidente de Seguridad:** Cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información, y que requiera una respuesta o intervención para mitigarlo.

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

- **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.

- **Vulnerabilidad:** Cualquier debilidad en los sistemas, procedimientos o controles que pueda ser explotada por una amenaza para comprometer la seguridad de la información.

5. MARCO NORMATIVO

- **Ley 1266 de 2008:** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 1273 de 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **Ley Estatutaria 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.

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

6. ESTABLECIMIENTO Y GESTIÓN

Con el propósito de evaluar y fortalecer la implementación del Plan de Seguridad y Privacidad de la Información, la ANCP-CCE contempla la herramienta de autodiagnóstico denominada "Instrumento de Evaluación MSPI", así como las diferentes guías y lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Se empleará una evaluación interna utilizando el referido instrumento de diagnóstico para medir el nivel de madurez en la gestión de la seguridad de la información y evaluar el estado actual de los controles y prácticas establecidas.

El proceso de establecimiento y gestión del Plan incluirá la revisión de políticas, procedimientos y controles existentes, así como la identificación de áreas de mejora. Se establecerán metas a corto, mediano y largo plazo para fortalecer continuamente la seguridad de la información. Estas metas estarán orientadas a mejorar la protección de los activos de información, asegurar el cumplimiento de las normativas vigentes y adaptar el Plan a las necesidades y riesgos emergentes.

7. PLAN OPERATIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tabla 1 - Plan Operativo de Seguridad y Privacidad de la Información.

No.	Componente	Descripción de las Actividades	Meta	Responsable	Fechas de programación			
					1Q	2Q	3Q	4Q
1	Análisis del estado en materia de Seguridad de la Información	Aplicar la herramienta de autodiagnóstico para medir el nivel de madurez del MSPI en la agencia	Contar con evaluaciones trimestrales (4 al año) que muestren el avance en la madures de los controles del sistema y poder generar acciones de mejora en caso de requerirlo	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	X	X	X	X

			Entregable: Herramienta de autodiagnóstico					
2	Implementación de controles Administrativos, Personales, Físicos y Tecnológicos	Ejecución del Plan de trabajo de implementación de controles definidos	Verificar la implementación de todos los controles definidos mediante los informes trimestrales (4 al año) de seguimiento a nivel administrativo, físicos, personales y tecnológicos Entregable: Informe de Seguimiento y Resultados de los Controles de Seguridad de la Información.	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	X	X	X	X
3	Monitoreo Continuo de Incidentes	Implementar herramientas y controles de monitoreo continuo que permitan la identificación temprana de eventos de seguridad, asegurando una respuesta rápida y efectiva ante cualquier incidente. Lo anterior, con el fin de permitirá detectar comportamientos inusuales en los sistemas de información, activando los procedimientos de gestión de incidentes establecidos.	Garantizar la cobertura total de los sistemas críticos y generar informes sobre incidentes en menos de 24 horas tras su detección. Entregable: Informe de Gestión de Incidentes. Reporte ante autoridades (de aplicar). Informe de Monitoreo	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	Esta actividad será ejecutada en aquellas ocasiones en donde se presente e identifique un incidente de seguridad en la ANCP-CCE			

4	Revisión y Actualización de Políticas de Seguridad	Realizar revisiones periódicas de las políticas internas de seguridad de la información para asegurar que estén alineadas con las normativas vigentes y las mejores prácticas aplicables.	Actualizar el 100% de las Políticas de Seguridad y Privacidad de la Información y publicarlas en el documento CCE-GTI-MA – Manual Operativo de Seguridad de la Información, conforme al Sistema Integrado de Gestión. Entregable: Manual Operativo de Seguridad de la Información actualizado con todas las políticas vigentes y alineadas al MSPI.	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT				X
5	Actualización e Innovación de la Infraestructura Tecnológica	Evaluar de manera periódica las tecnologías implementadas para identificar oportunidades de mejora, así como la adopción de nuevas soluciones que permitan fortalecer la protección de los activos de información y mejorar el rendimiento de los sistemas.	Validar las actualizaciones de la infraestructura tecnológica a través de: Entregable: informe de seguridad, asegurando que la seguridad y eficiencia operativa estén alineados a todos los componentes de seguridad que apliquen.	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	Esta actividad será ejecutada en aquellas ocasiones en donde se presente e identifique una actualización a la infraestructura de la ANCP-CCE			
6	Gestión de incidentes y/o brechas de seguridad	Identificar, analizar, gestionar y resolver de manera oportuna los incidentes de seguridad o brechas en los sistemas, implementando acciones correctivas para mitigar riesgos y	Gestionar cualquier incidente y/o brecha de seguridad de la información bajo este esquema: Identificar, clasificar, priorizar, contener, analizar, erradicar, recuperar, reportar, remediar. Entregable: Informe de Gestión de Incidentes, junto con su respectiva documentación.	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	Esta actividad será ejecutada en aquellas ocasiones en donde se presente e identifique un incidente y/o brecha de seguridad y/o privacidad de la información al interior de la ANCP-CCE			

		prevenir su repetición.	Entregable: Planes de Remediación.		
7	Despliegue de las acciones correctivas	Planificar, coordinar e implementar de manera oportuna las acciones correctivas necesarias para resolver las vulnerabilidades o problemas detectados, asegurando la mitigación de riesgos y evitando su recurrencia.	Planificar, coordinar e implementar el 100% de las acciones correctivas derivadas de vulnerabilidades detectadas, asegurando su ejecución dentro de los 60 días siguientes a la identificación, y verificar su efectividad para evitar recurrencias. Entregable: - Cronograma de Implementación de Acciones Correctivas. - Plan de Monitoreo de las Acciones Correctivas. - Informe de Efectividad de las Acciones Correctivas.	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	Esta actividad será ejecutada en aquellas ocasiones en donde se presente e identifique un incidente y/o brecha de seguridad y/o privacidad de la información al interior de la ANCP-CCE
8	Apoyo y asesoría técnico-jurídica en los lineamientos para la respuesta a PQRSD aplicables y asociadas a la seguridad y privacidad de la información	Proporcionar apoyo técnico y jurídico para definir y aplicar de manera oportuna los lineamientos en la respuesta a PQRSD relacionadas con la seguridad y privacidad de la información, garantizando el cumplimiento de normativas y mejores prácticas en ambos ámbitos, en el marco del MSPI.	Proporcionar el 100% del apoyo técnico y jurídico requerido para definir y aplicar lineamientos en la respuesta a PQRSD relacionadas, dentro de un plazo máximo de 5 días hábiles posteriores a la recepción de cada solicitud, en el marco del MSPI. Entregables: Conceptos técnicos y/o lineamientos en materia de seguridad/privacidad de la información, continuidad de negocio y tratamiento/protección de datos personales.	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	Esta actividad será ejecutada en aquellas ocasiones en donde se presente e identifique una PQRSD aplicable al área de seguridad de la información de la ANCP-CCE

9	Evaluación de desempeño	Evaluar la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación	Entregables: Hoja de vida de indicadores, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el Decreto 612 de 2018.	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT		X		X
10	Indicadores de seguridad de la información	Realizar el reporte de los Indicadores de seguridad de la información	Entregable: Informe de Indicadores de seguridad de la información	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	X	X	X	X
11	Actualización de los documentos del componente de seguridad de la información	Actualizar los documentos del componente de seguridad de la información	Entregables: Documentos del componente de seguridad de la información actualizados	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT		X		X
12	Gestión de la continuidad de negocio	Planear y ejecutar planes de pruebas del Plan de continuidad del Negocio y Plan de recuperación de desastre de las aplicaciones de la ANCP-CCE	Entregables: Planes de ejecución de pruebas de Plan de continuidad del Negocio y Plan de recuperación de desastre Informes de pruebas de Plan de continuidad del Negocio y Plan de recuperación de desastre	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT		X		X

Fuente: Elaboración propia

8. ACTUALIZACIÓN DEL PLAN

A continuación, se presenta la estrategia de seguimiento y monitoreo del cumplimiento del Plan de Seguridad y Privacidad de la Información, la cual incluye los elementos clave para asegurar la correcta ejecución de cada actividad contemplada en el Plan. La siguiente herramienta contempla el diligenciamiento de los roles de los responsables específicos para cada tarea, fechas de inicio y fin, así como indicadores de porcentaje de cumplimiento por trimestre, lo que permitirá un

seguimiento sistemático y preciso, con el fin de tomar las acciones correctivas a las que haya lugar. El monitoreo se realizará de manera continua, con revisiones trimestrales y auditorías internas, garantizando que se implementen las acciones correctivas necesarias para cumplir con las metas establecidas.
Adicionalmente, el Plan de Seguridad y Privacidad de la Información deberá ser actualizado una vez al año, con el fin de garantizar que el mismo permanezca alineado con las normativas vigentes, las necesidades tecnológicas, y las nuevas amenazas o riesgos identificados. De esta manera, se asegura que las estrategias y acciones definidas continúen siendo efectivas y pertinentes para la protección de los activos de información de la organización.

Al finalizar la vigencia anual del Plan de Seguridad y Privacidad de la Información, se debe emitir un Informe Anual que resuma el estado de cumplimiento del plan, los logros alcanzados, las desviaciones identificadas y las acciones correctivas implementadas. Este informe servirá para evaluar la efectividad de las estrategias implementadas y garantizar que los objetivos del plan se hayan cumplido en su totalidad, proporcionando una base sólida para las actualizaciones y mejoras necesarias en la siguiente vigencia.

9. SEGUIMIENTO Y MEDICIÓN

Los indicadores de seguimiento son herramientas clave para evaluar el progreso y la efectividad de las estrategias implementadas. Estos indicadores permiten medir el rendimiento en relación con los objetivos establecidos, facilitando la toma de decisiones informadas y la identificación de áreas de mejora.

A continuación, se detalla las características del indicador:

Tabla 2 - Indicador de Cumplimiento y Seguimiento del Plan

Indicador	Detalle
Nombre del Indicador	Seguimiento del Plan de Seguridad y Privacidad de la Información
Cálculo	(Número de actividades ejecutadas del plan / Total de actividades programadas del plan) x 100
Descripción y Tecnología de Apoyo Recomendada	Evaluar el avance y cumplimiento de las actividades planificadas en el Plan de Seguridad y Privacidad de la Información para garantizar su correcta implementación

Objetivo de Medición	≥ 95%
Umbrales Esperados Óptimos (%)	95% - 100%
Responsable de la Medición	Subdirección de IDT
Frecuencia de Medición	Trimestral
Clasificación	Operativo

Fuente: Elaboración Propia

10. FICHA TÉCNICA DEL DOCUMENTO Y CONTROL DE CAMBIOS

1. IDENTIFICACIÓN Y UBICACIÓN	
Título del documento:	Plan de Seguridad y Privacidad de la Información
Fecha de aprobación:	15/12/2025
Área / Dependencia de autoría:	Subdirección de Información y Desarrollo Tecnológico
Resumen / Objetivo de contenido:	Fortalecer la Seguridad de la Información de la ANCP-CCE mediante la implementación de acciones alineadas con sus políticas internas y el Modelo de Seguridad y Privacidad de la Información (MSPI), procurando la correcta identificación de riesgos, la implementación de controles adecuados y la protección de los activos críticos.
Código de estandarización:	CCE-GTI-PL-01
Categoría / Tipo de documento:	Plan
Aprobación por:	Comité Institucional de Gestión y Desempeño
Información adicional:	No aplica
Serie documental según TRD	Planes de Seguridad y Privacidad de la información
Enlace de ubicación original del documento (especifique donde se aloja o reposa el documento)	CCE-GTI-PL-01_Plan_Seguridad_Privacidad

2. AUTORES Y RESPONSABLES DE REVISIÓN Y APROBACIÓN				
ACCIÓN	**NOMBRE**	**CARGO/ PERFIL**	**FECHA**	**FIRMA**
Elaboró	Oscar Fernando Sanabria Camargo	Contratista	03/12/2025	Original firmado
Revisó	William Efrén Pardo Garzón	Analista T2 – G6 / Subdirección de Información y Desarrollo Tecnológico	03/12/2025	Original firmado
	COASIC	Comité de Apoyo de Seguridad de la Información y Ciberseguridad	09/12/2025	Acta de la IV Sesión del COASIC
Aprobó	CIGD	Comité Institucional de Gestión y Desempeño	15/12/2025	Acta de la IV sesión del CIGD

3. CONTROL DE CAMBIOS DEL DOCUMENTO					
VERSION	**AJUSTES**	**FECHA**	**VERSIÓN VIGENTE DEL FORMATO**		**07**
01	Creación del documento	08/02/2019	**Elaboró**	Frederick Ferro Mojica Luis Alejandro Ruiz	Contratistas IDT
			Revisó	Dana Pineda Marín	Subdirector de Información y Desarrollo Tecnológico
			Aprobó	CIGD	Comité Institucional de Gestión y Desempeño
02		13/01/2025	**Elaboró**	Ana María Cárdenas	Contratistas IDT

	Actualización del Documento		**Revisó**	Rigoberto Rodríguez	Subdirector de Información y Desarrollo Tecnológico
			Aprobó	Comité Institucional de Gestión y Desempeño	CIGD
03	Actualización del documento; y se hace modificación del código del proceso de seguridad al Macroproceso de GTI, dado que todos los procesos de tecnología fueron agrupados en este macroproceso.	25/11/2021	**Elaboró**	Milena Cabrales	Contratistas IDT
			Revisó	Rigoberto Rodríguez	Subdirector de Información y Desarrollo Tecnológico
			Aprobó	Comité Institucional de Gestión y Desempeño	CIGD
04	Actualización del Documento	13/10/2022	**Elaboró**	Milena Cabrales	Contratistas IDT
			Revisó	Rigoberto Rodríguez	Subdirector de Información y Desarrollo Tecnológico
			Aprobó	Comité Institucional de Gestión y Desempeño	CIGD
05	Actualización y ajustes al documento	31/01/2024	**Elaboró**	Javier Peralta Alexis Linares	Contratistas IDT
			Revisó	Luis Reyes William Pardo Carlos Toledo	Gestor T1-15 Analista T2 G6 Subdirector IDT

			Aprobó	Javier Peralta Alexis Linares	Contratistas IDT
06	Actualización general del documento	03/01/2025	**Elaboró**	Cevallos & Holguín Consultores S.A.S	Contratista IDT
			Revisó	COASIC	Comité Asesor en materia de seguridad de la información
			Aprobó	CIGD	Comité Institucional de Gestión y Desempeño SESIÓN DEL 12-12-2024
07	Actualización del documento en el cual se definen las actividades a ejecutar durante la vigencia 2026 además se incluye el alcance	03/12/2025	**Elaboró**	Oscar Fernando Sanabria Camargo	Contratista / Subdirección de Información y Desarrollo Tecnológico
			Revisó	William Efrén Pardo Garzón	Analista T2 – G6 / Subdirección de Información y Desarrollo Tecnológico
				Comité de Apoyo de Seguridad de la Información y Ciberseguridad	COASIC
			Aprobó	Comité Institucional de Gestión y Desempeño CIGD	Comité Institucional de Gestión y Desempeño SESIÓN DEL 15-12-2025

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