Agencia Nacional
de Contratación Pública
Colombia Compra Eficiente

PLAN DE TRATAMIENTO DE RIESGOS 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 formulado un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, con el propósito de fortalecer y cumplir con el Modelo de Seguridad y Privacidad de la Información (MSPI). Este modelo, definido conforme a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), tiene como objetivo proteger los activos de información de la Entidad y garantizar su adecuada gestión, en línea con la normativa vigente en seguridad de la información.

El presente plan se enfoca en la identificación y análisis de riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información. A través de un proceso sistemático, se identifican amenazas y vulnerabilidades que puedan impactar los activos críticos de la Entidad, permitiendo determinar su nivel de riesgo y establecer acciones concretas para mitigar su impacto y probabilidad de ocurrencia.

Como parte de la estrategia de tratamiento de riesgos, se implementarán medidas de mitigación y control orientadas a reducir los riesgos detectados, a través de controles técnicos, administrativos y físicos que buscan prevenir incidentes de seguridad y garantizar la capacidad de respuesta oportuna ante posibles brechas o amenazas. Estas acciones serán complementadas con un monitoreo constante y revisiones periódicas, permitiendo ajustar las estrategias a nuevos riesgos emergentes y mantener la eficacia de las medidas adoptadas. Adicionalmente, el plan incluye acciones de capacitación y sensibilización dirigidas al personal de la Entidad, fomentando una cultura de seguridad de la información y minimizando los riesgos derivados de errores humanos o negligencias.

Como infraestructura crítica, la ANCP-CCE debe robustecer sus sistemas y procesos para garantizar la resiliencia y continuidad operativa. La ejecución adecuada de este Plan busca asegurar la protección de la información, al igual que la estabilidad del sistema de contratación pública, fortaleciendo la confianza de los diferentes grupos de interés y contribuyendo al cumplimiento de los objetivos estratégicos y misionales de la Entidad.

2. OBJETIVO

General:

Definir, desarrollar y planificar las acciones y actividades necesarias para implementar medidas y controles específicos para la identificación, evaluación, tratamiento y monitoreo de los riesgos de seguridad de la información en la ANCP-CCE para la vigencia 2025, garantizando la protección de los activos críticos, el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) y el fortalecimiento continuo de la confidencialidad, integridad y disponibilidad de la información.

Específicos:

- Realizar un análisis exhaustivo, alineado a la metodología de riesgos de la ANCP-CCE, para identificar y evaluar los riesgos que puedan afectar la seguridad de la información.
- Desarrollar e implementar controles técnicos, administrativos y físicos adecuados para mitigar los riesgos identificados, asegurando la protección de los activos de información frente a amenazas internas y externas.
- Diseñar e implementar actividades de capacitación y concientización dirigidas a los colaboradores de la ANCP-CCE, promoviendo prácticas seguras en el manejo de la información y la prevención de incidentes.
- Establecer mecanismos de monitoreo continuo y evaluación periódica de los controles implementados, garantizando su efectividad y la adopción de medidas correctivas cuando sea necesario.
- Asegurar el cumplimiento de las políticas internas, el MSPI y la normativa vigente en seguridad de la información, promoviendo la mejora continua a través de auditorías y revisiones periódicas del plan.

3. ALCANCE

Este Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información aplica a todas las actividades, procesos, sistemas, aplicaciones, redes, bases de datos y documentos físicos o digitales que contengan información gestionada por la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE). Incluye la identificación, análisis, evaluación, tratamiento y monitoreo de riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información, así

como la protección de datos personales, en conformidad con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la normativa vigente.

El Plan abarca todos los sistemas informáticos, redes, bases de datos, aplicaciones y cualquier otro medio que contenga información relevante para la Entidad. Es aplicable a todos los funcionarios, contratistas, proveedores y demás partes interesadas con acceso a la información gestionada por la ANCP-CCE, comprendiendo todas las Áreas, Subdirecciones y Grupos Internos de Trabajo, para garantizar que estos actores comprendan y apliquen las medidas y controles definidos para mitigar los riesgos identificados.

Asimismo, el Plan adopta un enfoque integral, considerando la seguridad y privacidad de la información tanto en su forma digital como física. Su cumplimiento es obligatorio y estará sujeto a auditorías y revisiones periódicas para evaluar su efectividad, identificar oportunidades de mejora y asegurar que la gestión de riesgos mantenga la protección de la información en niveles aceptables, alineada con los objetivos estratégicos y operativos de la Entidad.

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.

- **Riesgo Emergente:** Amenaza nueva o en evolución que surge debido a cambios en el entorno, tecnología, regulaciones, o dinámicas sociales y económicas, y que no ha sido completamente identificado o comprendido, lo que dificulta su gestión.

- **Riesgo de Seguridad/Privacidad de la Información:** Es la posibilidad de que ocurra un evento que afecte la confidencialidad, integridad o disponibilidad de la información, causando un impacto negativo en la Agencia.

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

- **Tratamiento de Riesgos:** Es el proceso mediante el cual se implementan medidas y acciones específicas para gestionar los riesgos identificados. Incluye

decisiones para mitigar, aceptar, transferir o eliminar los riesgos, con el objetivo de reducir su impacto o probabilidad de ocurrencia. El tratamiento de riesgos implica la implementación de controles adecuados, asignación de responsabilidades y monitoreo continuo para garantizar la protección de los activos y la mejora de la seguridad.

- **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.

- **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.

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 objetivo de evaluar y fortalecer la implementación del Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información, la ANCP-CCE utilizará el "Instrumento de Evaluación MSPI" como herramienta de autodiagnóstico, junto con las guías y lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). A través de este instrumento, se llevará a cabo una evaluación interna para medir el nivel de madurez en la gestión de los riesgos de seguridad de la información y analizar el estado actual de los controles y prácticas implementadas.

La gestión del Plan incluirá la revisión y actualización periódica de políticas, procedimientos y controles existentes, con el fin de identificar y abordar áreas de mejora. En este sentido, se establecerán metas a corto, mediano y largo plazo para el fortalecimiento continuo de la seguridad de la información. Estas metas estarán enfocadas en garantizar la protección efectiva de los activos de información, asegurar el cumplimiento de las normativas vigentes y ajustar el Plan a las necesidades organizacionales y riesgos emergentes, manteniendo una postura proactiva frente a posibles vulnerabilidades.

7. PLAN OPERATIVO DE TRATAMIENTO DE RIESGOS

Tabla 1 : Plan Operativo de Tratamiento de riesgos

No.	Componente	Descripción de las Actividades	Meta	Responsable	Fechas de programación			
					1Q	2Q	3Q	4Q
1	Análisis de Riesgos de Seguridad de la Información identificados en la matriz integral de riesgos de la Entidad	Realizar un análisis de los riesgos actuales de seguridad y privacidad de la información en todos los sistemas, procesos y recursos existentes.	Contar con dos evaluaciones de riesgos formales durante el año y generar un informe de resultados y recomendaciones (acciones correctivas)	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	X		X	

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

No.	Componente	Descripción de las Actividades	Meta	Responsable	Fechas de programación			
					1Q	2Q	3Q	4Q
2	Análisis de riesgos emergentes (Ciberdefensa)	Realizar una evaluación de los riesgos emergentes, incluyendo amenazas cibernéticas y nuevas vulnerabilidades que podrían afectar los sistemas de información.	Asegurar la ejecución de analítica de datos que permita tomar decisiones oportunas frente a las amenazas externas, internas y demás riesgos emergentes, especialmente en materia de ciberseguridad. Entregable: informe de resultados y recomendaciones	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	X	X	X	X
3	Consolidación de riesgos	Consolidar los riesgos actuales y emergentes en un único análisis integral, priorizando aquellos con mayor impacto en la seguridad y privacidad de la información., además de contemplar los riesgos asociados al tratamiento de la privacidad y la protección de los datos personales Presentar los resultados de la consolidación de riesgos a los diferentes responsables de los procesos de la ANCP-CCE	Contar con un análisis consolidado y priorizado de los riesgos relevantes. Entregable: Matriz Integral de Riesgos de Seguridad y Privacidad de la Información actualizada. Informe de cambios, en caso de aplicar.	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	X		X	

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

No.	Componente	Descripción de las Actividades	Meta	Responsable	Fechas de programación			
					1Q	2Q	3Q	4Q
4	Evaluación de Controles	Evaluar los controles actuales de seguridad de la información para determinar su efectividad en la mitigación de riesgos.	Evaluar el nivel de madurez de los controles existentes. Entregable: Informe de Resultados de la Medición.	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT		X		X
5	Capacitación y sensibilización	Ejecutar las actividades de sensibilización establecidas en el Plan de Capacitación, Sensibilización y Comunicación en materia seguridad de la información y protección de datos personales.	Verificar que los funcionarios y contratistas comprendan y apliquen las políticas de seguridad. Entregables: Dos capacitaciones por trimestre en materia de: a) riesgos de seguridad/privacidad de la información; b) amenazas cibernéticas; c) roles y responsabilidades en cuanto a la gestión de riesgos se refiere; d) la gestión de riesgos como un componente del MSPI. Divulgación de destacados o piezas web para la protección de la información y protección ante nuevas amenazas.	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	X	X	X	X

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

No.	Componente	Descripción de las Actividades	Meta	Responsable	Fechas de programación			
					1Q	2Q	3Q	4Q
6	Implementación de medidas de seguridad	Implementar controles adicionales para mitigar riesgos identificado. Dichos controles surgen de la analítica realizada a los riesgos actuales (matriz integral de riesgos) y a los riesgos emergentes.	Implementar el 100% de los controles de seguridad necesarios para reducir los riesgos críticos identificados en los análisis de vulnerabilidad, dentro de los 45 días siguientes a la aprobación del plan de acción, asegurando su efectividad mediante planes de remediación y seguimiento. Entregables: Plan de Acción frente a los resultados obtenidos Planes de Remediación.	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 control adicional que se requiera para la mitigación de un riesgo emergente en la ANCP-CCE			
7	Gestión de vulnerabilidades	Realizar evaluación de vulnerabilidades en las diferentes plataformas Planear y solucionar vulnerabilidades identificadas en las diferentes plataformas	Entregables: Informe de vulnerabilidades Plan de solución de vulnerabilidades y evidencia de su solución	Líder de Seguridad y Privacidad de la Información de la Subdirección de IDT	X	X	X	X
8	Mejora Continua	Hacer seguimiento a las observaciones o recomendaciones de los Informes de Vulnerabilidades.	Entregable: Informe de Resultados de Eficacia de Acciones Correctivas.	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 Tratamiento de Riesgos 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, trimestres de ejecución de la actividad, 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 Tratamiento de Riesgos en Materia 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 Tratamiento de Riesgos en Materia 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	Ejecución del Plan de Tratamiento de Riesgos
Cálculo	(Número de actividades completadas / Total de actividades planificadas) x 100
Descripción y Tecnología de Apoyo Recomendada	Medir el porcentaje de cumplimiento de las actividades del Plan de Tratamiento de Riesgos, permitiendo identificar desviaciones y tomar acciones correctivas.
Objetivo de Medición	≥ 90%
Umbrales Esperados Óptimos (%)	90% - 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 Tratamiento de Riesgos 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 gestión de riesgos en de Seguridad y Privacidad 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) y la metodología de riesgos de la Entidad, procurando la correcta identificación de riesgos, la implementación de controles adecuados y la protección de los activos críticos.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código de estandarización:	CCE-GTI-PL-07
Categoría / Tipo de documento:	Plan
Aprobación por:	Comité Institucional de Gestión y Desempeño - CIGD.
Información adicional:	No aplica
Serie documental según TRD	Planes - 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-07_Plan_Tratamiento_Riesgos

2. AUTORES Y RESPONSABLES DE REVISIÓN Y APROBACIÓN				
ACCIÓN	**NOMBRE**	**CARGO/ PERFIL**	**FECHA**	**FIRMA**
Elaboró	Oscar Fernando Sanabria Camargo	Contratista / Subdirección de Información y Desarrollo Tecnológico	01/12/2025	Original Firmado
Revisó	William Efrén Pardo Garzón	Analista T2 – G6 / Subdirección de Información y Desarrollo Tecnológico	02/12/2025	Original Firmado
	COASIC	Comité de Apoyo de Seguridad de la Información y Ciberseguridad	09/12/2025	Acta de la IV Sesión del COASIC -con fecha de 09/12/2025
Aprobó	CIGD	Comité Institucional de Gestión y Desempeño	15/12/2025	Acta de la IV sesión del CIGD
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.				

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

3. CONTROL DE CAMBIOS DEL DOCUMENTO					
VERSION	**AJUSTES**	**FECHA**	**VERSIÓN VIGENTE DEL FORMATO**		**03**
01	Creación del documento	05/04/2019	**Elaboró:**	Luís Alejandro Ruíz	Contratistas IDT
			Revisó:	Diana Pineda Marín	Subdirector de Información y Desarrollo Tecnológico
			Aprobó:	Comité Institucional de Gestión y Desempeño CIGD	Comité Institucional de Gestión y Desempeño
02	Actualización del documento	22/12/2020	**Elaboró:**	Milena Patricia Cabrales	Contratistas IDT
			Revisó:	Rigoberto Rodríguez Peralta	Subdirector de Información y Desarrollo Tecnológico
			Aprobó:	Comité Institucional de Gestión y Desempeño CIGD	Acta de Comité Institucional de Gestión y Desempeño
03	Actualización del documento	2/11/2022	**Elaboró:**	Wilson Eduardo Coronado Becerra	Contratistas IDT
			Revisó:	Rigoberto Rodríguez Peralta	Subdirector de Información y Desarrollo Tecnológico
			Aprobó:	Acta de Comité Institucional de Gestión y Desempeño	Acta de Comité Institucional de Gestión y Desempeño
04		31/01/2024	**Elaboró**	Alexis Linares	Contratistas IDT

	Actualización del Documento		**Revisó**	Luis Reyes William Pardo Carlos Toledo	Gestor T1-15 Analista T2 G6 Subdirector IDT
			Aprobó	Comité Institucional de Gestión y Desempeño CIGD	Acta de Comité Institucional de Gestión y Desempeño
05	Actualización del numeral 7. Plan operativo de tratamiento de riesgos, en el cual se definen las actividades a ejecutar durante la vigencia 2025	13/01/2025	**Elaboró**	Cevallos & Holguín Consultores S.A.S	Contratistas IDT
			Revisó	Comité Asesor en materia de seguridad de la información COASIC	COASIC
			Aprobó	Comité Institucional de Gestión y Desempeño CIGD	Acta de Comité Institucional de Gestión y Desempeño
06	Actualización del documento en el cual se definen las actividades a ejecutar durante la vigencia 2026 además se incluye el alcance	02/12/2025	**Elaboró**	Oscar Fernando Sanabria Camargo	Contratista IDT
			Revisó	Comité Asesor en materia de seguridad de la información COASIC	COASIC
			Aprobó	Comité Institucional de Gestión y Desempeño CIGD	Acta de 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