



Superservicios



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

Oficina Asesora de Planeación e Innovación Institucional
Enero, 2026 V.1

1. OBJETIVO

Establecer las actividades orientadas a tratar de manera integral los riesgos de Seguridad y Privacidad de la Información a los cuales la entidad puede estar expuesta; con el fin de alcanzar sus objetivos institucionales y el cumplimiento de su misión y visión, protegiendo y preservando la integridad, confidencialidad y disponibilidad de la información.

1.1. OBJETIVOS ESPECÍFICOS

- Gestionar los riesgos de Seguridad y Privacidad de la Información, teniendo en cuenta los activos de información identificados y las directrices establecidas en el documento DE-I-004 Instructivo para la Gestión de Riesgos establecido por la entidad.
- Socializar y sensibilizar a los colaboradores de la entidad, los lineamientos establecidos para la gestión de riesgos de Seguridad y Privacidad de la Información.
- Realizar el seguimiento a las acciones correctivas y preventivas que se generen para mitigar los riesgos residuales que se encuentren en zonas moderada, alta y extrema.
- Dar cumplimiento a los requisitos legales y normativos en materia de riesgos de seguridad y privacidad de la información.

2. DEFINICIONES

- **Activo de información:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización

del riesgo.

- **Integridad:** Propiedad de exactitud y completitud.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Seguridad de la información:** Conjunto de medidas que toman las personas y las organizaciones, que les permiten resguardar y proteger los activos de información, preservando su confidencialidad, integridad y disponibilidad.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

3. MARCO LEGAL

- **Ley 527 de 1999.** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del *Habeas 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 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia. Parte 1 - Disposiciones reglamentarias generales. Título 1 - Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional.
- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1008 del 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.
- **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. Artículos 1 y 2 relacionados con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información.
- **CONPES 3975 de 2019.** Política nacional para la transformación digital e inteligencia artificial.
- **CONPES 3995 DE 2020.** Política nacional de confianza y seguridad digital.
- **Resolución 500 de 2021.** Por la cual 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.

- **Directiva Presidencial 03 de 2021.** Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- **Decreto Presidencial 88 de 2022.** Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
- **Resolución 460 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones.** Por la cual se expide el Plan Nacional de Infraestructura de Datos y Su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
- **Circular 01 de 2022 - Departamento Administrativo de la Presidencia de la República.** Recomendaciones de uso de servicios en la nube como medida para mitigar riesgos de seguridad digital.
- **Decreto 255 de 2022 - Ministerio de Comercio, Industria y Turismo.** Por el cual se adiciona la Sección 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.
- **Directiva 02 de 2022 - Presidencia de la República.** Reiteración de la política pública en materia de seguridad digital.
- **Decreto 338 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones.** Por el cual se adiciona el Título 21 a la Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.

- **Resolución 746 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones.** Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
- **Resolución 01117 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones.** Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital.
- **Decreto 767 de 2022 - Presidencia de la República.** 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.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas V.7, 2025, publicado por el DAFP.
- **Ley 2294 de 2023 – Plan Nacional de Desarrollo 2022- 2026 “Colombia potencia mundial de la vida”.** Artículo 143. Transformación digital como motor de oportunidades e igualdad. Numeral 4. Promover estrategias para la identificación, prevención y control de todo tipo de violencias en entornos digitales, en coordinación con el Ministerio de Educación Nacional, con énfasis en mujeres, grupos étnicos y niñas, niños y adolescentes. Numeral 5. Implementar iniciativas de transformación digital como herramienta para la productividad, la generación de empleo, la dinamización de la economía en las regiones y la potencialización de la economía popular. Numeral 6. Fortalecer el Gobierno Digital para tener una relación eficiente entre el Estado y el ciudadano, que lo acerque y le solucione sus necesidades, a través del uso de datos y de tecnologías digitales para mejorar la calidad de vida.
- **Resolución 02277 de 2025 - Ministerio de Tecnologías de la Información y las Comunicaciones.** Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 asociado con el fortalecimiento del Modelo de Seguridad y Privacidad de la Información y se derogan otras disposiciones relacionadas con la materia.

4. ALCANCE

El alcance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica para todos los procesos identificados en el modelo de operación institucional, a todos sus funcionarios, contratistas, proveedores y aquellas personas o terceros que para el cumplimiento de sus funciones y las de la entidad, compartan, utilicen, recolecten, procesen, intercambien o consulten cualquier activo de información de su propiedad.

5. METODOLOGÍA DE IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

El Instructivo para la Administración de Riesgos de la Entidad (DE-I-004) establece las directrices metodológicas para la identificación, análisis, evaluación, tratamiento, monitoreo, revisión y seguimiento de los riesgos de gestión, integridad, fiscales y seguridad de la información en la Superintendencia de Servicios Públicos Domiciliarios (Superservicios), los últimos de particular relevancia para el presente plan, el cual está orientado a proteger los activos de información.

6. PLANIFICACIÓN DE ACTIVIDADES

| ACTIVIDADES | RESPONSABLE ¹ | FECHA INICIO | FECHA FIN |
|--|--|--|------------|
| Acompañar los ejercicios de evaluación y tratamiento de riesgos en la entidad asociados a seguridad de la información. | Oficial de seguridad de la información | 01/02/2026 | 31/03/2026 |
| Verificar la eficacia de los controles asociados a seguridad de la información, de acuerdo con las evidencias publicadas por los líderes de proceso, en el módulo de riesgos de seguridad digital. | Oficial de seguridad de la información | 30/05/2026 31/09/2026 31/12/2026 | |

¹ El rol de Oficial de Seguridad de la Información fue asignado al jefe de la Oficina Asesora de Planeación e Innovación Institucional, de acuerdo con la Resolución No. SSPD – 20211000576955 del 12/10/2021.

| | | |
|--|--|--|
| Realizar socialización del cumplimiento del plan de tratamiento de riesgos | Oficial de seguridad de la información | 30/05/2026 31/09/2026 31/12/2026 |
|--|--|--|

7. SEGUIMIENTO.

El informe consolidado de seguimiento al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026 se realizará con una frecuencia cuatrimestral, en concordancia con el cronograma del numeral 6. Asimismo, se llevará a cabo un seguimiento mensual cuyas evidencias serán registradas en SISGESTION.

Este documento se articula con el Plan de Acción Institucional; por consiguiente, los productos y entregables generados en dicho marco acreditan también el cumplimiento de las actividades aquí descritas.

8. ACCIONES DE MEJORA

En caso de presentarse desviaciones en la ejecución y desarrollo del plan de ejecución y monitoreo de riesgos de seguridad y privacidad de la información, se aplicarán acciones de mejora concertadas con los líderes de los procesos y el personal de las dependencias responsables, las cuales se registran en el sistema de información SIGME (Sistema Integrado de Gestión y Mejora).

CONTROL DE CAMBIOS

| VERSIÓN | FECHA | DESCRIPCIÓN DEL CAMBIO |
|---------|------------|------------------------|
| 1 | 30/01/2026 | Edición inicial |