



**Superservicios**  
Superintendencia de Servicios  
Públicos Domiciliarios

---

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

---



## 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 los lineamientos establecidos 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 *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 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.
- **Ley 1955 de 2019.** Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad". Artículo 147. Transformación Digital Pública. Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. Artículo 148. Gobierno Digital como Política de Gestión y Desempeño Institucional. Todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones para la implementación de la política de Gobierno Digital.
- **CONPES 3995 DE 2019.** Política nacional de confianza y seguridad digital.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas V.5, diciembre de 2020, publicado por el DAFP.

#### 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 en razón del cumplimiento de sus funciones y las de la entidad compartan, utilicen, recolecten, procesen, intercambien o consulten cualquier activo de información de su propiedad.

#### 5. PLANIFICACIÓN DE ACTIVIDADES

TAREAS	RESPONSABLE	FECHA INICIO	FECHA FIN
Participar en las reuniones con el proveedor o los profesionales de calidad para la parametrización del módulo de riesgos e incluir las modificaciones establecidas por el DAFP en cuanto a seguridad digital.	Oficial de seguridad de la información	01/03/2021	31/12/2021
Actualizar el Instructivo de Gestión de Riesgos en lo referente a seguridad digital, de acuerdo con la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 de diciembre de 2020, publicado por el DAFP.	Oficial de seguridad de la información	01/03/2021 - 31/03/2021 01/10/2021 - 31/10/2021	
Socializar a los colaboradores de la entidad sobre la Gestión de Riesgos en lo referente a seguridad digital.	Oficial de seguridad de la información	01/02/2021	31/12/2021
Acompañar la identificación, administración y monitoreo de riesgos de seguridad digital.	Oficial de seguridad de la información	01/02/2021	31/12/2021
Verificar las evidencias publicadas por los líderes de proceso, tanto en el módulo de riesgos de seguridad digital como en el módulo de ACPM relacionadas con el tratamiento de riesgos.	Oficial de seguridad de la información	15/01/2021 - 31/03/2021 01/04/2021 - 30/06/2021 01/07/2021 - 30/09/2021 01/10/2021 - 20/12/2021	

**CONTROL DE CAMBIOS**

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	29/01/2021	Edición inicial
2	03/05/2021	<ul style="list-style-type: none"> <li>- Se incluyeron a los profesionales de calidad en la tarea de participar en las reuniones con el proveedor, para la parametrización del módulo de riesgos, de acuerdo con los nuevos lineamientos del DAFP.</li> <li>- Se ajustó la fecha de inicio y la fecha fin de la tarea: Actualizar el Instructivo de Gestión de Riesgos en lo referente a seguridad digital, de acuerdo con la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 de diciembre de 2020, publicado por el DAFP. Se establecieron las fechas 01/03/2021 - 31/03/2021 y 01/10/2021 - 31/10/2021.</li> <li>- Se amplió la fecha fin a 31/12/2021 para la tarea: Socializar a los colaboradores de la entidad sobre la Gestión de Riesgos en lo referente a seguridad digital.</li> </ul>