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

VIGENCIA
2026

CONTENIDO

1. INTRODUCIÓN

INDEPORTES CAUCA es consciente de la importancia del tratamiento de los riesgos de seguridad digital, frente a los activos de información generados por la entidad, por lo anterior es de vital importancia evaluar las acciones a tomar para mitigar los riesgos existentes teniendo en cuenta los criterios definidos anteriormente por la entidad, en la medida que se tengan plenamente identificados los riesgos que afecten la seguridad de la información, INDEPORTES CAUCA establecer los respectivos controles y medidas viables, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información.

2. OBJETIVOS

- **GENERAL**

  - Presentar el plan de tratamiento de riesgos de riesgos de la información de INDEPORTES CAUCA, con el fin de implementar los controles adecuados que permitan proteger los activos de la información.

- **ESPECIFICO**

  - Crear o actualizar si es necesario el mapa de riesgos de seguridad de la información.
  - Definir los principales acticos a proteger.
  - Identificar los riesgos de seguridad de la información.
  - Realizar el seguimiento a los controles establecidos.

3. NORMATIVIDAD

- Decreto 1008 del 14 de junio de 2018, Política de Gobierno Digital.
- Decreto 1078 de 2015 Articulo 2.2.17.7.1, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1499 de 2017 Artículo 2.2.22.2.1., Políticas de institucional.
- Decreto 2693 de 2012.
- Decreto 1499 de 2017 se crea el nuevo Modelo Integrado de Planeación y Gestión.
- Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
- Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

- ➢ Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- ➢ Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
- ➢ NTC 27001:2006: Sistema de Gestión de Seguridad de la Información (SGSI).
- ➢ ISO 27002:2005: Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información.

4. ALCANCE

El alcance del Plan de Tratamiento de Riesgos de Seguridad de la Información se aplica en todos los procesos asociados a INDEPORTES CAUCA, por lo cual es de estricto cumplimiento para contratistas y funcionarios de planta de la entidad.

5. RESPONSABILIDADES

- ➢ Jefe de oficina de planeación.
- ➢ Apoyo de área de sistemas de la información.

6. TÉRMINOS Y DEFINICIONES

- ➢ **Seguridad de la información:** Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.
- ➢ **Activo de la información**: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Administración Municipal y, en consecuencia, debe ser protegido. Se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- ➢ **Confidencialidad:** garantiza que la información solo sea accesible para las personas autorizadas a tener dicho acceso.
- ➢ **Integridad:** garantiza la exactitud y veracidad de la información, asegurando que la información no se encuentra alterada, destruida o perdida.
- ➢ **Disponibilidad:** garantiza que los usuarios autorizados para el uso y conocimiento de esta información tengan acceso a la misma y a los activos asociados.

- **Riesgos de seguridad de la información:** posibilidad de que ocurran eventos o situaciones que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos y sistemas informáticos de una organización. Este riesgo está relacionado con amenazas que pueden aprovechar vulnerabilidades en los sistemas, tecnologías, procesos o personas para acceder, modificar, destruir o robar información sensible.

7. DESARROLLO

El presente plan será desarrollado por medio del análisis de los riesgos que actualmente se tienen en cuanto a los activos de la información, de acuerdo a la matriz de riesgos realizada en la vigencia 2024, se contemplan medidas de respuesta las cuales se implementaran en la entidad de acuerdo a los recursos que se dispongan para el 2025.

ANALISIS DEL RIESGO					
	CLASIFICACION			EVALUACION	
RIESGO (R1)	PROBABILIDAD	IMPACTO	TIPO DE IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA
Pérdida, robo o fuga de Información.	5	5	Disponibilidad, confidencialidad e integridad de la informacion.	Extremo	Licenciamiento de Software.

ANALISIS DEL RIESGO					
	CLASIFICACION			EVALUACION	
RIESGO (R2)	PROBABILIDAD	IMPACTO	TIPO DE IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA
Correos electronicos no seguros	3	4	confidencialidad de la informacion.	Alto	Capacitacion al personal del uso correcto del correo electronico.

ANALISIS DEL RIESGO					
	CLASIFICACION			EVALUACION	
RIESGO (R3)	PROBABILIDAD	IMPACTO	TIPO DE IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA
Daño en los equipos tecnologicos	4	4	Disponibilidad de la informacion.	Alto	Mantenimientos preventivos. Actualizacion de software.

ANALISIS DEL RIESGO					
	CLASIFICACION			EVALUACION	
RIESGO (R4)	PROBABILIDAD	IMPACTO	TIPO DE IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA
Perdida de conexión	3	3	Disponibilidad de la informacion.	Alto	Mejora en la infraestructura de red. Mantenimientos preventivos. Actualizacion de software.

ANALISIS DEL RIESGO					
	CLASIFICACION			EVALUACION	
RIESGO (R5)	PROBABILIDAD	IMPACTO	TIPO DE IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA
Ataques Ciberneticos	3	5	Disponibilidad, confidencialidad e integridad de la informacion.	Alto	Implementacion de herramientas de seguridad de la informacion.

8. SEGUIMIENTO Y EVALUACIÓN

El seguimiento al documento tiene como propósito monitorear permanentemente el avance o cumplimiento de los entregables y productos propuestos, de acuerdo con las fechas establecidas.

9. ANEXOS

- Política de Gobierno Digital.
- Política de Seguridad Digital.

10. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
01	2026/01/26	Elaboración Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

ELABORÓ		REVISÓ		APROBÓ	
Nicolás A. Díaz Martínez Contratista Sistemas		**Mónica Margoth Mera Cerón** Jefe Oficina de Planeación		**Comité de Gestión y Desempeño Institucional.** Acta N° 01-2026	
Fecha	2026/01/26	Fecha	2026/01/26	Fecha	2026/01/26