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

Instituto de Cultura y Turismo del Departamento de Bolívar – ICULTUR

GOBERNACIÓN DE BOLÍVAR

Vigencia 2026

Documento Institucional – Versión Estructurada según Índice Oficial

INTRODUCCIÓN

Este documento corresponde al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto de Cultura y Turismo del Departamento de Bolívar – ICULTUR para la vigencia 2026.

El Plan se formula como complemento del Plan Estratégico de Seguridad y Privacidad de la Información y desarrolla de manera detallada las acciones orientadas a reducir los riesgos identificados a niveles aceptables.

Su estructura respeta de manera estricta el índice institucional aprobado por Control Interno y se articula con el Modelo Integrado de Planeación y Gestión – MIPG, el Sistema de Control Interno y los lineamientos de Gobierno Digital.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Establecer el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de ICULTUR para la vigencia 2026, definiendo acciones, controles, responsables e indicadores que permitan reducir los riesgos identificados.

1.2 OBJETIVOS ESPECÍFICOS

Definir estrategias de tratamiento de riesgos alineadas con los objetivos institucionales.

Asignar responsabilidades claras para la implementación de controles.

Establecer mecanismos de seguimiento y evaluación del riesgo.

Fortalecer la cultura de gestión del riesgo en seguridad de la información.

2. JUSTIFICACIÓN

La información constituye uno de los activos estratégicos más relevantes del Instituto de Cultura y Turismo del Departamento de Bolívar – ICULTUR, en tanto soporta la planeación, ejecución y control de los procesos misionales, estratégicos y de apoyo de la entidad.

En este sentido, la adecuada gestión de los riesgos asociados a la seguridad y privacidad de la información se convierte en un elemento esencial para garantizar la continuidad institucional, la transparencia administrativa y la confianza de la ciudadanía.

La creciente dependencia de las tecnologías de la información, el incremento en el volumen de datos tratados por la entidad y la interacción permanente con terceros y ciudadanos, incrementan la exposición de ICULTUR a riesgos relacionados con accesos no autorizados, pérdida de información, divulgación indebida, indisponibilidad de los sistemas y afectaciones a la integridad de los datos. Estos riesgos pueden generar impactos operativos, legales, reputacionales y financieros que comprometen el cumplimiento de los objetivos institucionales.

En este contexto, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se formula como un instrumento técnico y operativo que permite traducir el análisis del riesgo en acciones concretas, controles definidos y responsabilidades claramente asignadas. Este Plan fortalece el Sistema de Control Interno al incorporar un enfoque preventivo y sistemático, alineado con el Modelo Integrado de Planeación y Gestión – MIPG y los lineamientos de Gobierno Digital.

Asimismo, la implementación de este Plan contribuye al cumplimiento de la normatividad vigente en materia de protección de datos personales, seguridad de la información y control interno, y se constituye en un soporte fundamental para los procesos de auditoría interna, evaluación independiente y reporte de información a través del FURAG. De esta manera, ICULTUR avanza hacia una gestión institucional basada en el riesgo, orientada a la mejora continua y a la protección efectiva de la información pública.

3. MARCO NORMATIVO

Constitución Política de Colombia.

Ley 1581 de 2012 – Protección de Datos Personales.

Decreto 1074 de 2015.

Decreto 1078 de 2015.

Modelo Integrado de Planeación y Gestión – MIPG.

Política de Gobierno Digital.

Sistema de Control Interno – MECI.

4. RESPONSABLES

Alta Dirección.

Área de Tecnologías de la Información.

Líderes de Proceso.

Control Interno.

Servidores públicos y contratistas.

4. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a la totalidad de los procesos, activos de información, sistemas de información, bases de datos, archivos físicos y digitales, infraestructura tecnológica y recursos de apoyo que hacen parte del funcionamiento del Instituto de Cultura y Turismo del Departamento de Bolívar – ICULTUR.

El alcance del Plan comprende tanto la información generada internamente como aquella recibida de terceros, ciudadanos, proveedores y entidades públicas o privadas, independientemente de su formato, medio de almacenamiento o canal de transmisión. En este sentido, el Plan cubre información en formato físico, digital, audiovisual y cualquier otro medio utilizado por la entidad.

Así mismo, el Plan aplica a todos los servidores públicos, contratistas, pasantes y terceros que, en desarrollo de sus funciones o actividades contractuales, tengan acceso, manejen, custodien o administren información institucional. Cada uno de estos actores deberá cumplir las acciones de tratamiento, controles y responsabilidades definidas en el presente documento.

El alcance del Plan se extiende a todas las etapas del ciclo de vida de la información, incluyendo su creación, procesamiento, almacenamiento, transmisión, consulta, conservación y disposición final, garantizando un enfoque integral de seguridad y privacidad de la información durante la vigencia 2026.

5. TÉRMINOS Y DEFINICIONES

Activo de información: Elemento que tiene valor para la organización.

Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad.

Riesgo residual: Riesgo remanente después de aplicar controles.

Tratamiento del riesgo: Proceso para modificar el riesgo.

6. PROCESO DE GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN

El proceso de gestión del riesgo de seguridad de la información en ICULTUR se desarrolla como un proceso sistemático, continuo y estructurado, orientado a identificar, analizar, evaluar, tratar y realizar seguimiento a los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

Este proceso inicia con la identificación del contexto institucional y de los activos de información, continúa con la identificación de amenazas y vulnerabilidades, y permite determinar los riesgos asociados a cada activo. Posteriormente, se realiza la valoración del riesgo, considerando la probabilidad de ocurrencia y el impacto potencial, lo que facilita su priorización.

Con base en los resultados de la valoración, se definen las acciones de tratamiento del riesgo, las cuales pueden orientarse a mitigar, aceptar, transferir o evitar el riesgo, según el nivel de tolerancia institucional y la viabilidad técnica, operativa y financiera de las acciones propuestas.

El proceso de gestión del riesgo incorpora mecanismos de monitoreo y revisión permanente, que permiten evaluar la efectividad de los controles implementados, identificar cambios en el contexto institucional y ajustar oportunamente las acciones de tratamiento. Este enfoque garantiza la mejora continua del Plan y su articulación con el Sistema de Control Interno y el Modelo Integrado de Planeación y Gestión – MIPG.

7. CONTEXTO ESTRATÉGICO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El contexto estratégico de riesgos de seguridad de la información comprende el análisis de los factores internos y externos que influyen en la gestión del riesgo en ICULTUR. Este análisis permite comprender las condiciones bajo las cuales la entidad desarrolla sus funciones y cómo estas condiciones pueden incidir en la exposición a riesgos de seguridad y privacidad de la información.

Dentro de los factores internos se consideran los objetivos institucionales, la estructura organizacional, los procesos misionales y de apoyo, el nivel de madurez en la gestión de tecnologías de la información, la cultura organizacional y los recursos disponibles. Estos elementos permiten identificar activos críticos y determinar su nivel de exposición al riesgo.

Por su parte, los factores externos incluyen el entorno normativo, los lineamientos de política pública, los avances tecnológicos, las amenazas cibernéticas emergentes y las relaciones con terceros y ciudadanos. El análisis de este contexto facilita la identificación de riesgos estratégicos y la definición de acciones de tratamiento alineadas con la misión institucional.

El contexto estratégico constituye la base para la toma de decisiones informadas en materia de seguridad de la información y permite articular el Plan de Tratamiento de Riesgos con los objetivos estratégicos del Instituto y del Departamento de Bolívar.

8.1 IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

La identificación de activos de seguridad de la información es una etapa fundamental del proceso de gestión del riesgo, en tanto permite reconocer aquellos elementos que tienen valor para ICULTUR y que requieren protección frente a amenazas internas y externas.

Los activos de información incluyen, entre otros, bases de datos, sistemas de información, aplicaciones, archivos físicos y digitales, documentos, infraestructura tecnológica, servicios de red, así como el conocimiento institucional generado por los servidores públicos y contratistas. Cada uno de estos activos cumple una función específica en el logro de los objetivos institucionales.

La identificación de activos se realiza considerando su relación con los procesos institucionales, el tipo de información que contienen, su nivel de criticidad y las consecuencias que podría generar su afectación. Este análisis permite priorizar los activos más relevantes y orientar las acciones de tratamiento del riesgo de manera eficiente.

La adecuada identificación de activos facilita la asignación de responsabilidades, la definición de controles y el seguimiento efectivo de los riesgos asociados, fortaleciendo la gestión integral de la seguridad y privacidad de la información.

La identificación de activos permite priorizar la protección de la información crítica para ICULTUR.

8.1.1 Análisis de los objetivos estratégicos

Se analizan los objetivos estratégicos institucionales para identificar activos críticos asociados.

8.1.2 Análisis de los objetivos de proceso

Se analizan los objetivos de cada proceso para identificar riesgos asociados a la operación.

8. IDENTIFICACIÓN DE RIESGOS

La identificación de riesgos de seguridad y privacidad de la información consiste en reconocer los eventos potenciales que podrían afectar negativamente los activos de información de ICULTUR. Este proceso considera la interacción entre amenazas, vulnerabilidades y activos, permitiendo identificar riesgos de manera estructurada y coherente.

Las amenazas pueden ser de origen interno o externo e incluyen acciones humanas, fallas tecnológicas, eventos naturales y situaciones operativas que puedan comprometer la información. Las vulnerabilidades corresponden a debilidades en los controles, procesos o tecnologías que pueden ser explotadas por una amenaza.

La identificación de riesgos se apoya en el análisis de procesos, la revisión de incidentes previos, entrevistas con responsables, evaluación de controles existentes y el análisis del contexto institucional. Este ejercicio permite consolidar un inventario de riesgos que sirve como base para la valoración, el tratamiento y el seguimiento.

El resultado de esta etapa es un conjunto de riesgos claramente definidos, documentados y alineados con los activos de información, lo cual facilita la toma de decisiones y el fortalecimiento del Sistema de Control Interno en materia de seguridad y privacidad de la información

9.1 TIPOS DE RIESGOS

Riesgos tecnológicos.

Riesgos operativos.

Riesgos legales.

Riesgos reputacionales.

9.2 TÉCNICAS PARA LA IDENTIFICACIÓN DE RIESGOS

1. Análisis de procesos

El análisis de procesos consiste en la revisión detallada y sistemática de las actividades que conforman un proceso, con el fin de identificar puntos críticos donde puedan generarse riesgos operativos, tecnológicos, administrativos o de control.

Esta técnica permite evaluar la secuencia de tareas, los responsables, los insumos, los controles existentes y los resultados esperados, identificando posibles fallas, cuellos de botella o dependencias excesivas.

A través del análisis de procesos se pueden detectar riesgos asociados a errores humanos, fallas tecnológicas, deficiencias en los controles internos o interrupciones en la prestación del servicio.

2. Entrevistas

Las entrevistas son una técnica cualitativa que permite identificar riesgos a partir del conocimiento y la experiencia de los funcionarios, contratistas o actores involucrados en los procesos evaluados.

Mediante preguntas estructuradas o semiestructuradas, se recopila información sobre situaciones recurrentes, debilidades operativas, incidentes no documentados y posibles escenarios de riesgo.

Esta técnica resulta especialmente útil para identificar riesgos que no se encuentran formalmente registrados en la documentación, pero que se presentan en la operación diaria de la entidad o del sistema evaluado.

3. Revisión documental

La revisión documental consiste en el análisis de documentos internos y externos relacionados con los procesos, tales como manuales, procedimientos, contratos, informes, actas, políticas, normatividad vigente y registros históricos.

Esta técnica permite identificar riesgos derivados de inconsistencias normativas, vacíos procedimentales, incumplimientos contractuales o desactualización de la documentación. A través de la revisión documental se puede evaluar si los procesos cuentan con lineamientos claros y si estos se encuentran alineados con los objetivos institucionales y los requisitos legales aplicables.

4. Análisis de incidentes históricos

El análisis de incidentes históricos se basa en la revisión de eventos ocurridos en el pasado que hayan generado fallas, interrupciones, pérdidas o afectaciones a los procesos, sistemas o servicios.

Esta técnica permite identificar patrones recurrentes, causas raíz y áreas vulnerables, facilitando la anticipación de riesgos similares en el futuro. El estudio de incidentes históricos es fundamental para fortalecer los controles existentes y establecer acciones preventivas, correctivas o de mejora continua, orientadas a reducir la probabilidad de ocurrencia o el impacto de eventos adversos.

9. VALORACIÓN DE RIESGOS

La valoración permite priorizar los riesgos y definir su tratamiento.

10.1 ANÁLISIS DE IMPACTO
Se evalúan las consecuencias de la materialización del riesgo sobre la operación, la legalidad y la reputación.

10.2 EVALUACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN
La evaluación considera probabilidad e impacto.

10.2.1 Análisis Preliminar del Riesgo Inherente
El riesgo inherente corresponde al riesgo sin controles.

10.2.2 Valoración de los Controles
Se evalúa la efectividad de los controles existentes.

10.2.3 Nivel de riesgo (Riesgo residual)
Corresponde al riesgo después del tratamiento.

10.3 MONITOREO Y REVISIÓN
El monitoreo permite verificar la efectividad del tratamiento.

10.3.1 Línea Estratégica
Define directrices institucionales.

10.3.1.1 Primera Línea de Defensa
Responsables directos de los procesos.

10.3.1.2 Segunda Línea de Defensa
Funciones de control y seguimiento.

10.3.1.3 Tercera Línea de Defensa
Auditoría interna.

10.3.2 Matriz de Responsabilidad
Define roles y responsabilidades en la gestión del riesgo.

10.4 SEGUIMIENTO AL RIESGO
Permite verificar el avance de las acciones de tratamiento.

10.4.1 Reportes Periódicos
Informes periódicos a la Alta Dirección y Control Interno.

10. COMUNICACIÓN Y CONSULTA

La comunicación y consulta constituyen un componente fundamental del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto de Cultura y Turismo del Departamento de Bolívar – ICULTUR. Este componente garantiza la apropiación institucional del enfoque de gestión del riesgo, la articulación entre áreas y la toma de decisiones informadas.

La comunicación se realizará mediante circulares internas, correos institucionales, comités técnicos, informes periódicos y espacios de socialización, asegurando que los responsables conozcan sus obligaciones y los avances del Plan.

La consulta permitirá recoger observaciones de líderes de proceso, Área TIC y Control Interno, promoviendo la mejora continua y la efectividad del tratamiento del riesgo.

11. CRONOGRAMA DE ACTIVIDADES

El cronograma de actividades constituye el instrumento operativo que permite planificar, ejecutar y controlar las acciones de tratamiento de riesgos de seguridad y privacidad de la información durante la vigencia 2026.

Este plan de tratamiento de riesgos define las **acciones de control** orientadas a mitigar los principales riesgos identificados en los procesos tecnológicos, administrativos y de control interno. Cada actividad se encuentra asociada a un riesgo específico, un proceso responsable y un tipo de control (técnico o administrativo), permitiendo asegurar la trazabilidad y el seguimiento de su implementación.

Los **indicadores y metas** establecidos facilitan la medición objetiva del nivel de cumplimiento, mientras que las **evidencias** permiten soportar documentalmente la ejecución de los controles, en concordancia con los principios de autocontrol, autorregulación y mejora continua exigidos en los modelos de control interno y gestión del riesgo.

Este instrumento sirve como base para el **seguimiento periódico**, la toma de decisiones preventivas y la reducción de la probabilidad e impacto de los riesgos institucionales.

Cronograma General de Implementación – Vigencia 2026

Actividad	Riesgo Asociado	Proceso	Tipo de Control	Responsable	Fecha Inicio	Fecha Fin	Indicador	Meta	Evidencia
Implementar control de accesos y autenticación	Acceso no autorizado	Gestión TIC	Técnico	Area TIC	01/02/2026	30/06/2026	% accesos controlados	100%	Registros de acceso
Implementar copias de seguridad automáticas	Pérdida de información	Gestión TIC	Técnico	Area TIC	01/02/2026	31/12/2026	% backups realizados	100%	Logs de respaldo
Firmar acuerdos de confidencialidad	Divulgación indebida de información	Gestión Humana	Administrativo	Gestión Humana	01/01/2026	31/03/2026	% acuerdos firmados	100%	Contratos firmados
Capacitación en seguridad de la información	Errores humanos	Todos los procesos	Administrativo	Area TIC / Talento Humano	01/04/2026	30/09/2026	% funcionarios capacitados	90%	Listados de asistencia
Seguimiento trimestral a riesgos	Materialización del riesgo	Control Interno	Administrativo	Control Interno	01/03/2026	31/12/2026	Informes realizados	4 informes	Informes de seguimiento

Actividad	Nombre	Cargo / Dependencia
Proyecto	Mario Imbett	Gestion TIC
Revisó	Irina de Guzmán Herrera	Directora administrativa y financiera
Revisó	Vaneza Daguer Tamayo	Director General
Aprobó	Comité Institucional de gestión y desempeño	Comité Institucional de gestión y desempeño