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

2025

Dirección: Calle 1A # 0-40
Cajicá - Cundinamarca
Teléfonos: (57+1) 310 584 4637 - 310 205 6145
Correo electrónico: pqrs@culturacajica.gov.co
Página web: www.culturacajica.gov.co

Tabla de contenido

1. INTRODUCCIÓN

La gestión de los riesgos de seguridad y privacidad de la información es el proceso mediante el cual se busca reducir la pérdida y protección de la información, permitiendo conocer las debilidades que afectan el ciclo de vida de los datos.

Cualquier sistema de información es susceptible de riesgos a la seguridad y privacidad de los datos y es de gran importancia que toda entidad u organización cuente con un plan de gestión de riesgos para garantizar la continuidad de los servicios. Por este motivo, el Instituto Municipal de Cultura y Turismo de Cajicá (IMCTC) se ha visto en la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado a sus procesos.

Este plan permite identificar el nivel de riesgo en que se encuentran los activos de información mediante la valoración de la seguridad existente a nivel de Hardware y Software, y la permanente capacitación al personal para seguir las normas y procedimientos referentes a la seguridad de la información.

2. CONTEXTO ESTRATEGICO INSTITUCIONAL

Misión

Somos una entidad descentralizada que planea, direcciona, ejecuta y evalúa las políticas, planes, programas y proyectos culturales, bibliotecarios, patrimoniales y turísticos del Municipio de Cajicá, desde el reconocimiento y visibilización de la diversidad cultural del municipio, el fortalecimiento de las prácticas de lectura, escritura y oralidad, la salvaguarda, protección, conservación y divulgación del patrimonio material e inmaterial y la promoción de Cajicá como destino turístico, a partir de procesos de planeación, articulación, desarrollo y evaluación encaminados al reconocimiento del Instituto a nivel regional y nacional por la calidad de los servicios y el impacto en la comunidad.

Visión

Liderar la formulación, ejecución y evaluación de políticas, planes, programas y proyectos culturales, bibliotecarios, patrimoniales y turísticos a nivel municipal, departamental, nacional e internacional, por medio de procesos innovadores de la gestión pública de la cultura a través del fomento de las prácticas culturales, el impulso de las prácticas de la lectura, escritura y oralidad, el rescate y apropiación de los bienes y manifestaciones de interés cultural y la promoción de Cajicá como destino turístico, contribuyendo a la transformación

cultural y el desarrollo social, económico y comunitario de la población.

3. ALCANCE

Que los funcionarios y contratistas del IMCTC comprendan los riesgos inherentes al uso de herramientas informáticas aplicadas a la administración de la información institucional.

Todas las plataformas y herramientas con las cuales el IMCTC, en el desarrollo de sus actividades, recopila, almacena y procesa información.

4. OBJETIVO GENERAL

Desarrollar un plan de gestión de riesgos de seguridad y privacidad de la información que permita minimizar la probabilidad de pérdida de activos de la información en el IMCTC.

5. OBJETIVOS ESPECÍFICOS

Objetivo 1: Promover la centralización de datos a través del uso de las herramientas informáticas institucionales implementadas y/o controladas por el IMCTC, para facilitar los procesos de backup y restauración de datos.
Objetivo 2: Registrar, clasificar, cuantificar y evaluar el reporte de incidentes que involucren riesgos de seguridad a la información, e identificar los puntos críticos que se deben atender con mayor prioridad.
Objetivo 3: Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo de información.
Objetivo 4: Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el Plan de Tratamiento de Riesgos y Privacidad de la Información.

6. DEFINICIONES BÁSICAS

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
Impacto: son las consecuencias que genera un riesgo una vez se materialice.
Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de

objetivos de los procesos de una entidad.

7. MARCO NORMATIVO

- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 1266 de 2008. Disposiciones generales Habeas Data.
- Ley 1581 de 2012. Disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014.Transparencia y Acceso a la información Pública Nacional.
- Decreto 4170 de 2011. Creación de la ANCP-CCE.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 1083 de 2015. Único Reglamentario del Sector Función Pública, con las modificaciones y adiciones introducidas a partir de su fecha de su expedición.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo con las modificaciones y adiciones introducidas a partir de su fecha de su expedición

8. PLAN DE ACCIÓN

ESTRATEGIA: Llevar a cabo acciones de mitigación de riesgos de seguridad informática.

META: Garantizar la mitigación de riesgos de seguridad y privacidad de la información.

INDICADOR: Número de actividades enfocadas en la mitigación de riesgos.

9. CRONOGRAMA:

ACTIVIDAD	RESPONSABLE	ENTREGABLE	FECHA DE INICIO	FECHA DE FINALIZACIÓN	PERIODICIDAD
Actividades de mitigación de riesgos	Contratista Área de tecnología	Informe de resultados	01/02/2025	28/12/2025	Mensual
Identificación de los riesgos	Contratista Área de tecnología	Informe de resultados	01/02/2025	28/12/2025	Mensual

10. SEGUIMIENTO Y MONITOREO

El seguimiento de los planes institucionales se realizará de acuerdo con el formato EST-PIC-MN-002-FM-003, correspondiente al seguimiento

de planes, programas y proyectos. Trimestralmente, se deberá reportar el estado de avance de cada plan.
Mapa de riesgos -

11. REFERENCIAS

Guía de Gestión de riesgos -Seguridad y Privacidad de la información https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf