MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

INSTITUTO MUNICIPAL DE CULTURA Y TURISMO DE CAJICÁ

2025

TABLA DE CONTENIDO

Contenido

1. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información – MSPI del Instituto Municipal de Cultura y Turismo de Cajicá (IMCTC) establece los lineamientos para proteger la información institucional, garantizar la privacidad de los datos y minimizar riesgos asociados al uso de tecnologías de la información.

El modelo se fundamenta en la Resolución 746 de 2022 del Ministerio TIC, que fortalece el MSPI como parte de la política de Gobierno Digital, y se articula con los estándares de la NTC-ISO/IEC 27001:2013, el CONPES 3854, la Ley 1581 de 2012 y la Ley 1712 de 2014.

El IMCTC, como entidad descentralizada del municipio, administra información cultural, turística, administrativa y comunitaria, por lo cual necesita mecanismos robustos para asegurar la confidencialidad, integridad y disponibilidad de sus activos de información.

2. JUSTIFICACIÓN

El presente documento compila los lineamientos del MSPI aplicados al Instituto Municipal de Cultura y Turismo de Cajicá con el fin de:

- Proteger datos personales, administrativos, financieros y culturales.
- Reducir riesgos tecnológicos y operativos.
- Cumplir con la normativa nacional de seguridad digital.
- Proporcionar confianza a servidores, contratistas, artistas, formadores, turistas y comunidad en general.
- Fortalecer la seguridad de la información como un proceso transversal del Instituto.

3. OBJETIVO GENERAL

Implementar el Modelo de Seguridad y Privacidad de la Información del Instituto Municipal de Cultura y Turismo de Cajicá, alineado con los estándares ISO/IEC 27001:2013, la Política de Gobierno Digital y la normativa sectorial vigente.

3.1 Objetivos Específicos

- Establecer los lineamientos para la gestión de la información física y digital del Instituto.
- Fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) del IMCTC.

- Garantizar la protección de datos personales y el cumplimiento del régimen de Habeas Data.
- Identificar y gestionar riesgos relacionados con la seguridad y privacidad.
- Fomentar la cultura institucional de seguridad digital.
- Mantener el cumplimiento de la normatividad vigente en materia de seguridad, protección de datos y transparencia.

4. MODELO DE SEGURIDAD MSPI

El Modelo de Seguridad y Privacidad de la Información MSPI, desde la Estrategia de Gobierno Digital contempla los siguientes ciclos de operación que contiene cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

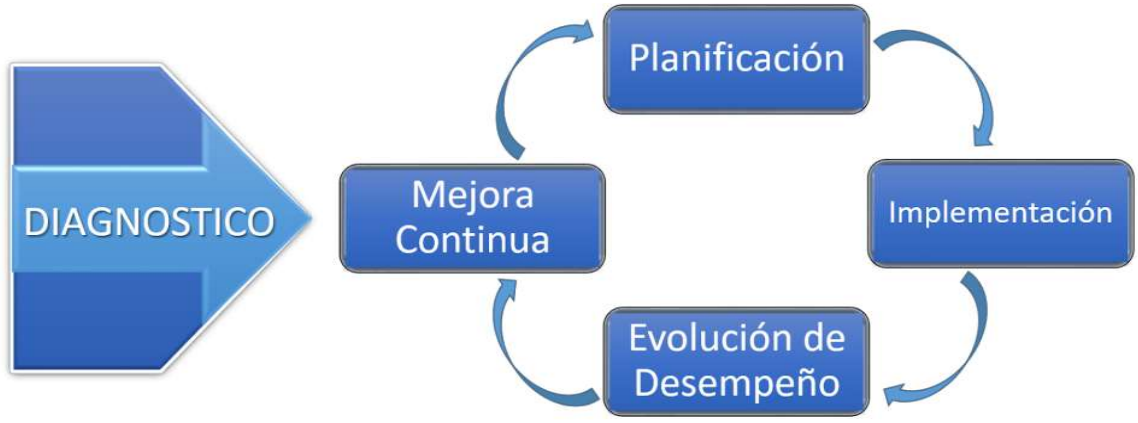


Figura 1 Ciclo de operación Modelo de Seguridad y Privacidad de la Información Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

El MSPI contempla cinco fases:

1. Diagnóstico
2. Planificación
3. Implementación
4. Evaluación

5. Mejora Continua

Estas fases permiten que el IMCTC gestione de manera integral la seguridad y privacidad de sus activos de información siguiendo los lineamientos de MinTIC.

5. FASE DE DIAGNÓSTICO

Esta Fase DIAGNOSTICO de acuerdo a la norma ISO 27001:2022 – Cláusula 4- Contexto de la organización, determina la necesidad de realizar un análisis de las cuestiones externas e internas de la Alcaldía municipal de Cajicá y su contexto, con el propósito de incluir los requisitos y expectativas de las partes interesadas en la organización para lograr el alcance del SGSI.

5.1 Estado Actual del Instituto Municipal de Cultura y Turismo de Cajicá

5.1.1 Conocimiento de la Entidad

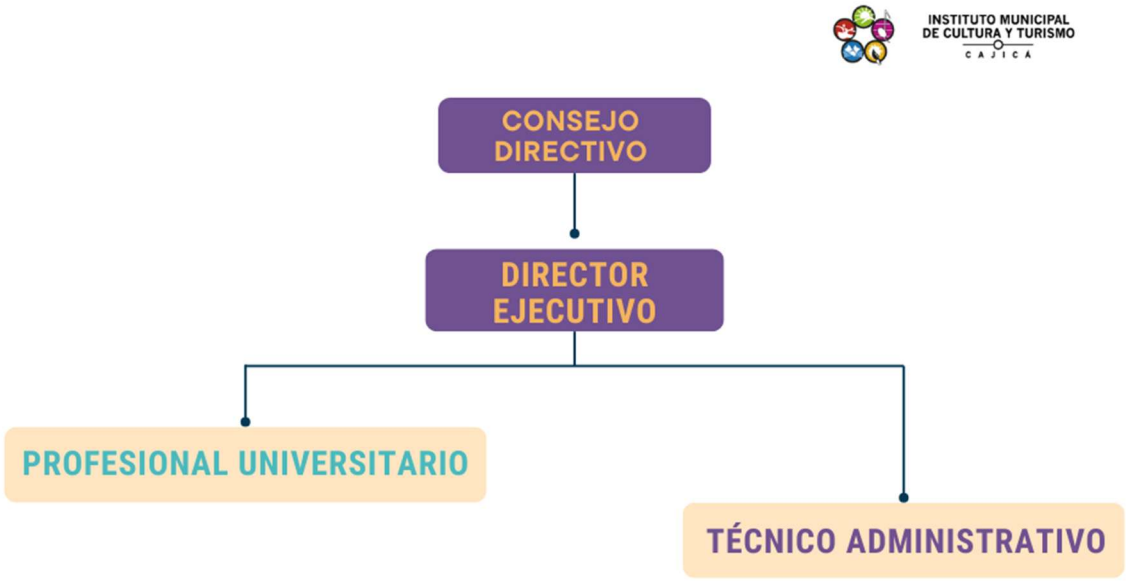
Misión

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 visibilizarían 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.

5.1.2 Organización del Instituto



El IMCTC cuenta con un organigrama institucional estructurado por áreas como:

- Dirección del Instituto
- Coordinación de Cultura
- Coordinación de Turismo
- Coordinación Administrativa
- Área TIC
- Escuelas de formación artística
- Programas comunitarios

5.2 Identificación del Nivel de Madurez

El Instituto utilizará la herramienta de evaluación MSPI del MinTIC para identificar su nivel de madurez en:

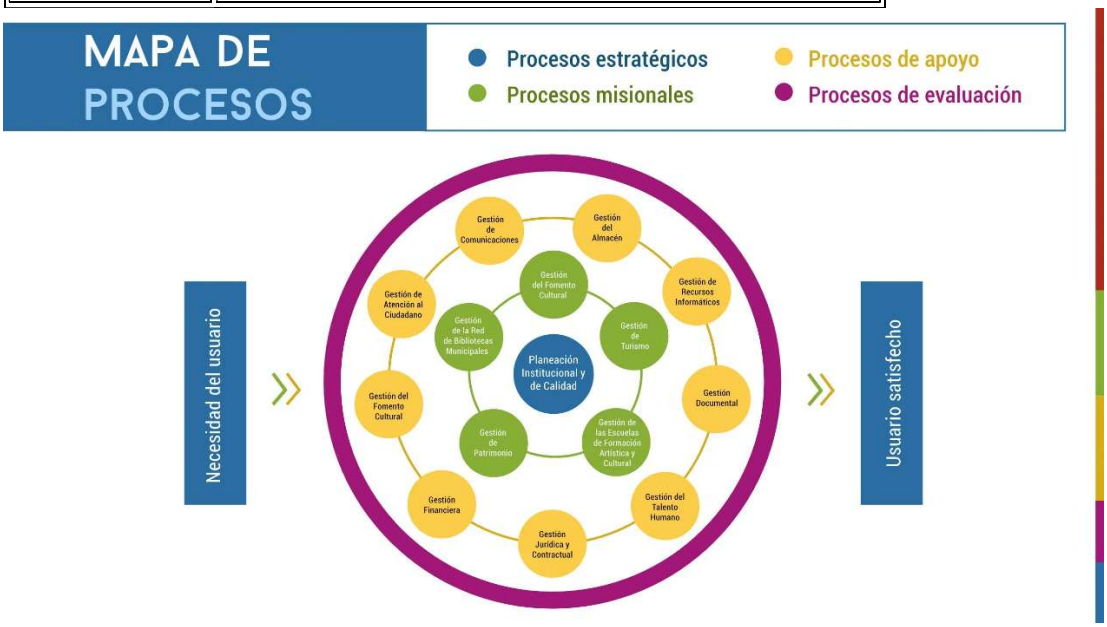
- Controles
- Procesos
- Gestión documental
- Seguridad digital
- Infraestructura tecnológica
- Cultura organizacional
- Protección de datos

5.3 Levantamiento de Información

Son partes interesadas de la Alcaldía Municipal de Cajicá, las entidades públicas y privadas

legalmente constituidas, que interactúan con la misma; teniendo presente los requisitos normativos internos, legales o reglamentarios y las obligaciones contractuales.

Parte interesada	Descripción
Gobierno	MinTIC, Secretaría TIC municipal, control interno.
Funcionarios	Servidores y contratistas del IMCTC.
Proveedores	Artistas, gestores, operadores turísticos y proveedores.
Comunidad	Usuarios de la oferta cultural y turística del Instituto.



Los activos de información incluyen:

- Bases de datos de programas culturales
- Registro de artistas, estudiantes y beneficiarios
- Información turística
- Bases de datos de eventos y convocatorias
- Infraestructura tecnológica
- Pagos, nómina, contratos y documentos administrativos

6. FASE DE PLANIFICACIÓN

Esta Fase de PLANIFICACIÓN de acuerdo a la norma ISO 27001:2013, en el capítulo 5 -Liderazgo, se fija las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad que tiene la Alta Dirección de establecer una política de seguridad de la información adecuada al propósito de la Alcaldía, que asegure la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen. En el capítulo 6 – Planificación, se establecen los requerimientos para la valoración y tratamiento de riesgos de seguridad, la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento. En el Capítulo 7 – Soporte, se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información.

6.1 Contexto del Instituto Municipal de Cultura y Turismo de Cajicá

6.1.1 Generalidades

El IMCTC desarrolla actividades culturales, artísticas y turísticas que implican manejo de información sensible y pública, por lo cual requiere adoptar el MSPI como componente estratégico para asegurar su operación.

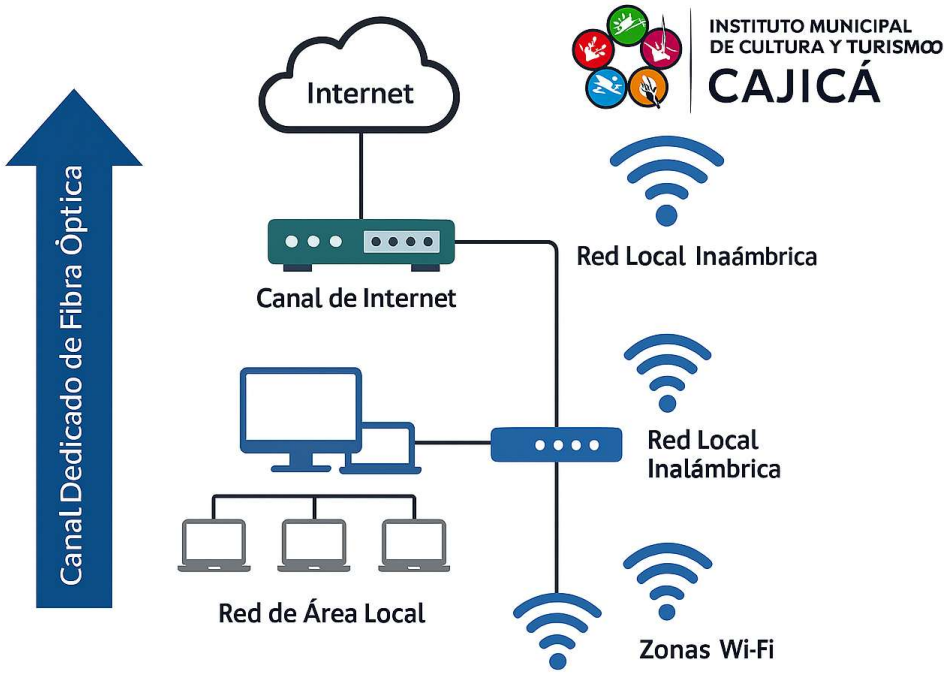
6.1.2 Contexto Tecnológico

Conectividad: La conectividad de la entidad está garantizada por un canal dedicado de Fibra Óptica. Esto permite que el canal de comunicación soporte las necesidades de la entidad del instituto municipal de cultura y turismo de Cajicá, tanto de planta como contratistas que allí laboran, requiere de una arquitectura de conectividad hibrida para su funcionamiento, es decir, debe disponer de conectividad por cable e inalámbrica; así mismo respecto del Wifi, se deben definir los tipos de perfil de acceso a esta red.

Red local: La red de área local (LAN), debe garantizar que al backbone llegue la conexión dedicada en fibra y pueda ser distribuida a través de cableado al menos en categoría 5e en cada una de las sedes. Se realizó un análisis de segmentación de acuerdo al número de sedes administrativas.

Red local inalámbrica: Se realiza una revisión de la red Wifi actual para optimizar la calidad de su diseño, dentro de los cuales se debe incluir la perfilación de usuarios para su utilización y manejo. Así mismo periódicamente se realiza el cambio de contraseña.

Canal de Internet: El servicio está dimensionado para ofrecer tráfico de salida y de entrada a Internet para toda la entidad, con un canal de Internet de 150Mbps distribuido para todas
El servicio está dimensionado para ofrecer tráfico de salida y de entrada a internet para las sedes, con un Ancho de banda de 1Gbps y para las Zonas Wifi 128 Mbps



Infraestructura del Instituto:

- Conexión a red municipal y enlaces dedicados.
- Equipos de cómputo administrativos y para formación artística.
- Red WiFi institucional para funcionarios.
- Sistemas de información como:
    - Bases de datos de inscrito a escuelas
    - Sistemas contables
    - Sistema de radicación
    - Páginas web y redes sociales institucionales

6.1.3 Expectativas de las Partes Interesadas

- Incluyen:
- Seguridad de la información
- Transparencia
- Protección de datos personales
- Accesibilidad
- Confiabilidad en plataformas y servicios digitales

6.1.4 Alcance del MSPI

El alcance del Modelo de Seguridad y Privacidad de la Información – MSPI del instituto municipal de cultura y turismo de Cajicá, es aplicable para todos los procesos, funcionarios, proveedores, contratistas, comunidad, y quienes, en cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, intercambien o consulten información, así como a los entes de control o entidades que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación; de esta forma buscamos proteger y preservar la integridad y disponibilidad de los activos de información.

El MSPI se aplica a:

- Todos los procesos del Instituto
- Funcionarios y contratistas
- Bases de datos y trámites
- Infraestructura tecnológica
- Información administrativa, cultural y turística

6.2 Liderazgo

6.2.1 Compromiso de la Dirección

La Dirección del IMCTC se compromete a garantizar recursos humanos, tecnológicos y financieros para implementar el MSPI.

6.2.2 Política de Seguridad

El IMCTC, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad. Para el instituto municipal de cultura y turismo de Cajicá la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición La política del Instituto incluye:

- Proteger activos de información
- Fomentar cultura de seguridad
- Gestionar riesgos
- Garantizar integridad, confidencialidad y disponibilidad
- Cumplir con la normativa vigente

6.2.3 Roles y Responsabilidades

Propuestos:

- Líder del SGSI: Coordinación TIC del Instituto
- Custodios de información: Coordinadores de áreas
- Responsable del tratamiento de datos: Dirección del IMCTC
- Usuarios: funcionarios, formadores y contratistas

Responsabilidades:

- Generar análisis y evaluación de riesgos.
- Identificación de riesgos realizada por los procesos.
- Incorporación de la gestión de riesgos.
- Identificación y evaluación de opciones para tratamiento de riesgos.
- Validar la implementación y operación del SGSI y MSPI.
- Identificación y controles para el tratamiento de riesgos.
- Implementación del plan de tratamiento de riesgos para lograr los objetivos de controles identificados.
- Verificar el diseño y definición de los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
- Generar estudios de los riesgos a intervalos planificados, y el nivel de riesgo residual y riesgo aceptable identificado.
- Definir y aplicar los procedimientos de seguimiento y revisión del SGSI.
- Generar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Generar revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes,

medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.

6.3 Planeación

Incluye:

- Identificación de riesgos
- Matriz de riesgos

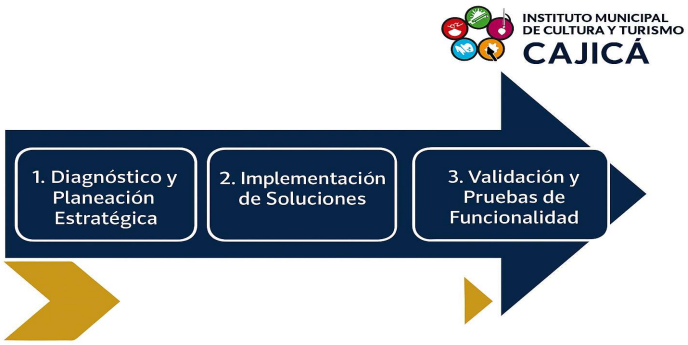
El instituto municipal de cultura y turismo de Cajicá realiza la identificación y evaluación de las amenazas de las vulnerabilidades relativas a los activos de información, ya sea sistemas de información, infraestructura y recurso humano, la probabilidad de ocurrencia y su impacto. Documento reservado por características de su naturaleza.

- Plan de tratamiento
- Plan de comunicaciones

Objetivo	Qué se Comunica	Frecuencia	Responsable	Estrategia de Comunicación	A quién se Comunica
Dar a conocer la Ley 1712 de 2014 (Transparencia y acceso a la información)	Ley 1712 de 2014: transparencia y acceso a la información pública y su reglamentación (1081 de 2015)	Anualmente	Funcionario asignado Área de Sistemas	Página web, redes sociales, institucional, banner web	Comunidad Cajiqueña y ciudadanía en general
Difundir el uso y beneficios de datos abiertos	Información relevante para la gestión cultural del municipio y apropiación de datos abiertos	Anualmente	Funcionarios asignados Área de Sistemas	Página web, redes sociales, institucional, banner web, datos.gov.co	Comunidad Cajiqueña y ciudadanía en general
Socializar procesos de gestión de recursos informáticos	Uso y apropiación de recursos informáticos	Anualmente / cuando se requiera	Funcionario designado Área de Sistemas	Inducciones, pantallas institucionales, correo institucional	Personal administrativo y prestadores de servicio
Socializar información relevante	Tipos de seguridad y seguimiento a la mejora	Trimestralmente / cuando se requiera	Secretario y funcionario asignado Área de Sistemas	Correo institucional, talleres,	Personal administrativo y prestadores de servicio

Objetivo	Qué se Comunica	Frecuencia	Responsable	Estrategia de Comunicación	A quién se Comunica
relacionada con MSP y SGSI				reuniones, redes sociales	

- Adopción de IPv6 (lineamientos MinTIC)



6.4 Soporte

Se asignarán recursos para:

- Infraestructura tecnológica
- Capacitación en seguridad digital
- Actualización de software
- Mantenimiento de equipos

7. IMPLEMENTACIÓN

Esta Fase IMPLEMENTACION en la norma ISO 27001:2013, capítulo 8 - Operación, indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

Incluye:

- Ejecución del plan de riesgos
- Controles operacionales

En la fase 5 del diagnóstico del MSPI se busca determinar el estado actual de la gestión de seguridad y privacidad de la información en la entidad, identificando el nivel de madurez institucional mediante el levantamiento de información y emisión del diagnóstico, evaluar el nivel de madurez de los controles de seguridad, identificar el avance en la implementación del ciclo de operación, verificar el cumplimiento con la legislación vigente sobre protección de datos personales y reconocer el uso de buenas prácticas en ciberseguridad. Para ello se recomienda utilizar los instrumentos disponibles en la página del Ministerio TIC: herramienta de diagnóstico, instructivo para su diligenciamiento y la Guía No. 1 sobre metodología de pruebas de efectividad. Esta fase implica recolectar información con la herramienta y aplicar la metodología de pruebas, para luego analizar los resultados, determinar el nivel de madurez y proceder a la fase de planificación. Los resultados del diagnóstico deben ser revisados y socializados con las partes interesadas antes de la implementación.

- Procedimientos internos
- Protocolos de seguridad

8. FASE DE EVALUACIÓN

La Fase EVALUACION DEL DESEMPEÑO en la norma ISO 27001:2013 descrita en el capítulo 9 - Evaluación del desempeño, define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

Incluye:

- Auditorías internas
- Revisión de indicadores
- Seguimiento a incidentes
- Revisión de madurez

9. FASE DE MEJORA CONTINUA

Esta Fase MEJORA CONTINUA en la norma ISO 27001:2013. En el capítulo 10 -Mejora, "se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información a partir de las no – conformidades que ocurran, las organizaciones deben establecer las acciones más efectivas para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan".

Implica:

- Acciones correctivas: El objetivo de estas acciones es eliminar la causa de problemas asociados con los requisitos del SGSI, con el fin de prevenir que ocurran nuevamente. Determinar y evaluar las causas de los problemas del SGSI e incidentes de seguridad de la información. Diseñar e implementar la acción correctiva necesaria. Revisar la acción correctiva tomada. Retroalimentación interna Actualización anual del MSPI

10. GLOSARIO

Activo de Información

Cualquier dato, documento, sistema, infraestructura tecnológica o recurso que tenga valor para el Instituto Municipal de Cultura y Turismo de Cajicá. Incluye información cultural, turística, administrativa, financiera y de atención al ciudadano.

Amenaza

Evento potencial que puede afectar negativamente un activo de información. Ejemplos: malware, accesos no autorizados, fallas eléctricas, errores humanos, pérdida de dispositivos, etc.

Autenticación

Proceso mediante el cual un usuario, funcionario o proveedor demuestra su identidad para acceder a sistemas del Instituto (correo institucional, aplicativos administrativos, plataformas culturales, etc.).

Autorización

Permisos otorgados a un usuario para acceder a determinados recursos. Se basa en roles institucionales (área cultural, área administrativa, turismo, comunicaciones, etc.).

Disponibilidad

Garantía de que los servicios, sistemas y la información del Instituto están accesibles cuando los funcionarios y ciudadanos los requieren. Incluye continuidad de portales culturales, agenda de eventos, y servicios al público.

Confidencialidad

Asegura que la información del Instituto solo sea accesible por personal autorizado. Ejemplo: datos personales de artistas, gestores, contratistas, funcionarios y ciudadanos.

Integridad

Garantiza que la información no ha sido alterada de forma no autorizada. Protege bases de datos culturales, calendarios de eventos y documentos administrativos.

Control

Medida implementada para reducir riesgos: políticas, firewalls, antivirus, respaldos, procedimientos, etc.

Dato Personal

Información que permite identificar a una persona. En el Instituto aplica especialmente a participantes de talleres, gestores culturales, contratistas, empleados y ciudadanos.

Dato Sensible

Información que afecta la intimidad de la persona. Su tratamiento en actividades culturales debe cumplir estrictamente con la Ley 1581 de 2012.

Evaluación de Riesgos

Proceso para identificar, analizar y valorar riesgos que afectan la seguridad de la información del Instituto.

Incidente de Seguridad

Cualquier evento que compromete la confidencialidad, integridad o disponibilidad de la información o los sistemas. Ejemplo: caída del portal web cultural, acceso no autorizado a bases de datos, malware en equipos institucionales.

Gestión de Incidentes

Conjunto de procesos para detectar, reportar, analizar y resolver incidentes de seguridad en el Instituto.

MSPI (Modelo de Seguridad y Privacidad de la Información)

Marco exigido por MinTIC para gestionar adecuadamente riesgos, seguridad y privacidad. Aplica a todos los procesos del Instituto y debe integrarse con cultura, turismo, administrativo y comunicaciones.

Política de Seguridad de la Información

Documento institucional que define objetivos, roles y compromisos en materia de seguridad y privacidad.

Privacidad

Derecho de los titulares de datos a controlar cómo se recolecta, usa y protege su información en las actividades culturales y turísticas.

Registro Nacional de Bases de Datos (RNBD)

Obligación ante la SIC para registrar las bases de datos administradas por el Instituto.

Respaldo (Backups)

Copia segura de información institucional que permite restaurar datos en caso de incidentes.

Riesgo

Probabilidad de que una amenaza explote una vulnerabilidad y afecte un activo del Instituto.

Seguridad de la Información

Conjunto de prácticas, políticas y controles destinados a proteger la información institucional.

Seguridad Digital

Aborda protección frente a ciberamenazas, ataques, vulnerabilidades, filtraciones y fallas tecnológicas que afecten actividades del Instituto.

Tratamiento de Datos Personales

Acciones como recolección, almacenamiento, uso y eliminación de datos de ciudadanos y actores culturales.

Vulnerabilidad

Debilidad que puede ser explotada por una amenaza. Ejemplos: sistemas sin actualización, contraseñas débiles, malas prácticas de almacenamiento de datos.

Encargado del Tratamiento

Persona o entidad que procesa datos por encargo del Instituto (p. ej., operador de plataformas culturales o turísticas).

Responsable del Tratamiento

El Instituto Municipal de Cultura y Turismo de Cajicá como entidad pública administradora de datos.

Ciclo PHVA (Planear – Hacer – Verificar – Actuar)

Metodología aplicada en el MSPI para la mejora continua.

11. REFERENCIAS

- Resolución 746 de 2022
- NTC-ISO/IEC 27001:2013
- Ley 1581 de 2012
- Ley 1712 de 2014
- Política de Gobierno Digital
- MSPI MinTIC
- Información institucional del IMCTC

INSTITUTO MUNICIPAL
DE CULTURA Y TURISMO
CAJICÁ