PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026



INSTITUTO MUNICIPAL DE CULTURA Y TURISMO DE TENJO

ALCALDÍA DE TENJO

CONTENIDO

1. INTRODUCCIÓN 3
   1.1. Objetivo principal 3
   1.2. Objetivos específicos 3
2. MARCO NORMATIVO 3
3. GLOSARIO Y ABREVIATURAS 4
   3.1 Glosario 4
   3.2 Abreviaturas 4
4. ALCANCE 4
5. METODOLOGÍA 5
6. EVALUACION DE RIESGOS 6
7. INDICADORES CLAVE 9
8. SEGUIMIENTO 9

1. INTRODUCCIÓN

El Instituto Municipal de Cultura y Turismo de Tenjo (IMCTT) es una entidad pública que maneja información sensible. La seguridad y privacidad de esta información es fundamental para la entidad y sus usuarios.

El objetivo de este plan es identificar, analizar y mitigar los riesgos de seguridad y privacidad de la información del IMCTT. El plan se basa en los principios de enfoque basado en riesgos, enfoque holístico y enfoque continuo.

El IMCTT se compromete a implementar este plan para garantizar la seguridad y privacidad de la información que maneja.

1.1. Objetivo principal

Garantizar la seguridad y privacidad de la información del Instituto Municipal de Cultura y Turismo de Tenjo (IMCTT).

1.2. Objetivos específicos

- Identificar y analizar los riesgos de seguridad y privacidad de la información del IMCTT.
- Implementar medidas de mitigación de riesgos para reducir la probabilidad e impacto de los riesgos identificados.

2. MARCO NORMATIVO

NORMA	AÑO	DESCRIPCIÓN
Ley 527 de 1999	1999	Define y reglamenta el acceso y el uso de los mensajes de datos.
Ley 594 de 2000	2000	Dicta la Ley General de Archivo y dicta otras disposiciones.
Ley 603 de 2000	2000	Modifica el artículo 47 de la Ley 222 de 1995.
Ley 1581 de 2012	2012	Dicta disposiciones generales para la Protección de Datos

Decreto 1078 de 2015	2015		Reglamenta el sector de Tecnologías de la Información y las Comunicaciones, y establece el componente de seguridad y privacidad de la información como parte integral de la estrategia GEL.

3. GLOSARIO Y ABREVIATURAS

3.1 Glosario

- Activo de Información: Todo recurso de datos, información o sistemas que tiene valor para la organización y requiere protección.
- Mitigación: Medidas tomadas para reducir la probabilidad o el impacto de un riesgo.
- Riesgo de Seguridad: Posible evento que puede comprometer la confidencialidad, integridad o disponibilidad de la información.
- Privacidad: Derecho de los individuos a controlar el uso de su información personal.

3.2 Abreviaturas

- IMCTT: Instituto Municipal de Cultura y Turismo de Tenjo.
- TIC: Tecnologías de la Información y las Comunicaciones.
- KPI: Indicador Clave de Desempeño (por sus siglas en inglés). ISO: Organización Internacional de Normalización.

4. ALCANCE

El plan de tratamiento de riesgos de seguridad y privacidad de la información del Instituto Municipal de Cultura y Turismo de Tenjo (IMCTT) se aplica a todos los activos de información del IMCTT, independientemente de su formato, ubicación o estado. Esto incluye información sensible, como datos personales, información financiera y datos de propiedad intelectual.

El alcance del plan se define de esta manera para garantizar que todos los activos de información del IMCTT estén protegidos contra los riesgos de seguridad y privacidad. La información sensible es la más importante para el IMCTT, ya que su pérdida o divulgación podría tener consecuencias graves para la entidad. El plan incluye medidas de mitigación específicas para proteger esta información.

5. METODOLOGÍA

El IMCTT implementará el plan de tratamiento de riesgos de seguridad y privacidad de la información utilizando la siguiente metodología:

Etapa de planificación

- Definición de los objetivos del plan.
- Establecimiento del alcance y el cronograma.
- Asignación de las responsabilidades.
- Etapa de ejecución.

Implementación de las medidas de mitigación de riesgos

- Etapa de monitoreo y seguimiento.
- Monitoreo de los riesgos de seguridad y privacidad de la información.

Seguimiento de la efectividad de las medidas de mitigación

- Identificación de oportunidades de mejora.

Mejora continua

- Revisión periódica del plan.
- Identificación de oportunidades de mejora.
- Implementación de las mejoras identificadas.



El gráfico muestra que el proceso de mejora continua es un ciclo continuo que se repite a lo largo del tiempo. El IMCTT debe revisar el plan de tratamiento de riesgos de seguridad y privacidad de la información de forma periódica para identificar oportunidades de mejora. Estas oportunidades de mejora pueden incluir la actualización de las medidas de mitigación de riesgos, la adición de nuevos riesgos al plan, o el cambio de la metodología utilizada.

6. EVALUACION DE RIESGOS

La evaluación de riesgos se realiza de manera cualitativa mediante una comparación que analiza la probabilidad de ocurrencia de un riesgo frente a su impacto potencial. Este proceso da como resultado la creación de una herramienta conocida como “Matriz de Calificación, Evaluación y Respuesta a los Riesgos”.

Esta matriz permite clasificar y calificar los riesgos según los niveles de impacto y probabilidad previamente establecidos, además de identificar las zonas de riesgo. Con base en esta clasificación, se definen las posibles formas de tratamiento para mitigar cada riesgo identificado. A continuación, se presenta un ejemplo de cómo se lee esta matriz:

IMPACTO	VALOR
Insignificante	5% - 19%
Baja	20% - 49%
Alta	50% - 90%
Extremo	91% - 100%

PROBABILIDAD	RANGO
Frecuencia Extrema	1 vez al día
Frecuencia Alta	1 vez al mes
Frecuencia Media	1 vez cada 6 meses
Frecuencia Baja	1 vez al año

La evaluación de riesgos identificó los siguientes riesgos de seguridad y privacidad de la información del IMCTT:

NO	ACTIVO	NOMBRE DEL RIESGO	DESCRIPCIÓN DEL RIESGO	TIPO DE RIESGO	CAUSAS	EFECTOS	PROBABILIDAD	IMPACTO DISPONIBILIDAD	IMPACTO INTEGRIDAD	IMPACTO CONFIDENCIALIDAD	CONTROLES
1	Equipos de cómputo de funcionarios	Pérdida de equipos de cómputo	Robo o pérdida de los equipos de cómputo de los funcionarios	Físico	Robo físico o negligencia en el cuidado de los equipos	Pérdida de datos confidenciales e interrupción en el trabajo de los funcionarios	Moderado	Extremo	Extremo	Extremo	Implementar control de inventario, marcado de activos y políticas de seguridad física
		Malware	Infección de equipos por malware	Técnico	Uso de software no autorizado	Pérdida o corrupción de datos	Alta	Extremo	Extremo	Extremo	Usar antivirus y políticas de uso
		Acceso no autorizado	Acceso indebido por usuarios no autorizados	Técnico	Contraseñas débiles	Violación de datos personales	Alta	Extremo	Extremo	Extremo	Implementar autenticación MFA
		Pérdida de datos	Borrado accidental o fallos de hardware	Operativo	Sin respaldo periódico de información	Interrupción de actividades operativas	Moderado	Extremo	Extremo	Extremo	Realizar copias de seguridad periódicas
		Uso indebido	Uso personal indebido que compromete la seguridad	Operativo	Falta de monitoreo de actividades	Exposición de la red corporativa	Moderado	Alta	Alta	Alta	Políticas de uso aceptable
2	Televisores	Acceso no controlado a televisores	Configuración insegura que permite accesos remotos no autorizados	Ciberseguridad	Uso de contraseñas débiles o configuraciones predeterminadas	Posibles ataques o mal uso de los dispositivos para divulgación de información	Baja	Baja	Baja	Baja	Configuración segura y controles de acceso

		Configuración incorrecta	Configuraciones mal realizadas que afectan la calidad de imagen	Técnico	Errores humanos	Baja eficiencia en la comunicación visual	Baja	Baja	Baja	Baja	Capacitación al personal
		Riesgo de robo	Hurto de televisores debido a accesos no controlados	Físico	Falta de vigilancia adecuada	Pérdida de activos valiosos	Moderado	Baja	Baja	Baja	Instalación de anclajes o alarmas
		Sobrecarga eléctrica	Daños causados por fluctuaciones de energía	Ambiental	Falta de protectores eléctricos	Pérdida de equipos	Moderado	Baja	Baja	Baja	Uso de estabilizadores de voltaje
		Uso no autorizado	Utilización indebida por personal no autorizado	Operativo	Falta de restricciones de uso	Mal uso de los recursos corporativos	Baja	Baja	Baja	Baja	Actualizar políticas de uso para funcionarios y contratistas
3	Rack de comunicaciones	Falla en rack de comunicaciones	Fallo o desorganización en el rack de comunicaciones	Operacional	Mala gestión de cableado o componentes antiguos	Caída de la red interna y lentitud en los servicios	Baja	Alta	Alta	Alta	Organización del cableado y monitoreo de equipos
		Riesgo de incendio	Incendio en el cuarto donde se encuentra el rack por sobrecalentamiento	Ambiental	Falta de sistemas de ventilación	Daño completo a la infraestructura de red	Baja	Alta	Alta	Extremo	Sistemas de detección de incendios
		Acceso físico no autorizado	Ingreso indebido al rack por personal no autorizado	Físico	Falta de candados o control de acceso físico	Manipulación no autorizada de equipos	Moderado	Alta	Alta	Alta	Implementar cerraduras
		Sobrecarga eléctrica	Sobrecarga en los dispositivos del rack	Operativo	Falta de distribución adecuada de energía	Interrupción del servicio de red	Moderado	Alta	Alta	Extremo	Uso de UPS y distribuidores eléctricos
		Daño por humedad	Afectación de los equipos por condiciones ambientales	Ambiental	Falta de control de humedad en el cuarto	Pérdida de funcionalidad de los dispositivos	Baja	Alta	Alta	Alta	Control de temperatura y humedad
4	Base de datos SQL	Exposición de la base de datos SQL	Explotación de vulnerabilidades en la base de datos	Ciberseguridad	Configuración insegura o falta de cifrado	Robo o alteración de datos confidenciales	Media	Extremo	Extremo	Extremo	Implementar cifrado de datos y auditorías regulares

		Ataques de inyección SQL	Explotación de vulnerabilidades en las consultas	Técnico	Falta de validación de entradas	Compromiso de los datos almacenados	Alta	Extremo	Extremo	Extremo	Implementar validación de consultas
		Acceso no autorizado	Ingreso indebido a la base de datos	Técnico	Contraseñas débiles o configuraciones inseguras	Exposición de datos sensibles	Alta	Extremo	Extremo	Extremo	Control estricto de accesos
		Pérdida de datos	Eliminación accidental o malintencionada de registros	Operativo	Errores humanos	Interrupción en las operaciones del negocio	Media	Extremo	Extremo	Extremo	Políticas de respaldo
		Fallos de disponibilidad	Caída del servicio por sobrecarga o errores de configuración	Técnico	Sobrecarga de consultas o errores técnicos	Interrupción de las operaciones	Media	Extremo	Extremo	Extremo	Balanceo de carga y optimización

7. INDICADORES CLAVE

Para evaluar la efectividad del plan, se establecerán los siguientes indicadores clave:

- Número de incidentes de seguridad reportados: Evaluación mensual.
- Tasa de éxito en pruebas de recuperación de datos: Revisión trimestral.
- Nivel de cumplimiento normativo: Auditorías semestrales.

Satisfacción del personal capacitado: Encuestas después de cada capacitación.

8. SEGUIMIENTO

El seguimiento es la actividad de monitorear y evaluar el progreso de un plan o proyecto. En el contexto de la gestión de riesgos, el seguimiento se utiliza para garantizar que las medidas de mitigación de riesgos sean efectivas y que los riesgos se mantengan controlados.

El seguimiento de los riesgos de seguridad y privacidad de la información debe incluir las siguientes actividades:

- Monitoreo de los riesgos: El IMCTT debe monitorear los riesgos de seguridad y privacidad de la información para identificar cualquier cambio en su probabilidad o impacto.

- Seguimiento de la efectividad de las medidas de mitigación: El IMCTT debe evaluar la efectividad de las medidas de mitigación de riesgos para garantizar que están reduciendo la probabilidad e impacto de los riesgos.
- Identificación de oportunidades de mejora: El IMCTT debe identificar oportunidades de mejora en el plan de tratamiento de riesgos para garantizar que sea efectivo y que siga siendo adecuado para las necesidades de la entidad.

Dado en Tenjo, Cundinamarca el 30 de enero de 2026.

DIANA CAROLINA ROJAS GUTIÉRREZ

DIRECTORA GENERAL DEL INSTITUTO MUNICIPAL DE CULTURA Y TURISMO DE TENJO