**INSTITUTO MUNICIPAL DE CULTURA Y TURISMO DE TENJO – CUNDINAMARCA**

# SEGUIMIENTO MATRIZ DE RIESGOS

**OFICINA DE CONTROL INTERNO**

**2024**

# MATRIZ DE RIESGOS IMCTT

| Área o Proceso | Tipo de Riesgo | Descripción del Riesgo | Posibles Consecuencias | Probabilidad | Impacto | Responsable | Controles Actuales | Acciones de Mitigación | Seguimiento 2024 |
|---|---|---|---|---|---|---|---|---|---|
| **Dirección general, gestión financiera, gestión jurídica, gestión administrativa y las demás dependencias que se le asignen recursos públicos** | Riesgo fiscal | Posible conducta irregular en procesos administrativos y financieros. | Sanciones legales, pérdida de credibilidad y recursos económicos. | Media | 60% moderado | Líder de proceso y control interno | Políticas anticorrupción, auditorías internas, reportes periódicos de control. | Capacitación continua en ética pública, fortalecer mecanismos de transparencia y reportes de denuncias. | Se realiza auditoria interna, a corte 31 de diciembre no se evidencia materialización de riesgo |
| **Gestión talento humano** | Riesgo fiscal | Incumplimiento de normativas de contratación laboral y seguridad social. | Multas, sanciones, y deterioro de la imagen institucional. | Muy bajo | 20% leve | talento humano | Revisiones periódicas de contratos, seguimiento a normativas laborales. | Actualizar políticas de contratación, capacitaciones sobre normatividad laboral. | Proceso transición secop I a secop II, mejora normativa institucional, sin materialización de riesgo. |
| **Gestión financiera** | Riesgo fiscal | Realizar pagos sin cumplimiento de requisitos legales para el pago de actas parciales y/o liquidación de contratos. | Sanciones legales, detrimento patrimonial, retraso en ejecución de proyectos. | Media | 60% moderado | tesorería | Verificación de requisitos legales y procesos internos. | Implementar revisión doble de pagos y auditorías mensuales. | Se verifico e incluyo en la auditoria interna los riesgos de tesorería, sin evidenciar materialización de riesgos. |
| **Gestión administrativa** | Riesgo fiscal | Realizar pagos sin verificación de aportes parafiscales | Multas a la entidad, incumplimiento de la normativa laboral y fiscal. | Media | 60% moderado | Supervisores | Solicitud de soportes antes del pago. | Fortalecer controles mediante sistemas | Desde el área se seguridad y salud en el trabajo se hace de manera |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | por parte de los contratistas. | | | | | | automatizados y alertas. | mensual la verificación de pago de aportes. |
| **Gestión financiera** | Riesgo fiscal | No presentar los informes del área financiera en los tiempos y términos establecidos por la ley. | Sanciones legales, pérdida de credibilidad, afectación a la planeación financiera. | Media | 60% moderado | Tesorería | Cronograma de reportes y seguimiento periódico. | Implementar alertas automatizadas y control de entregas con responsables. | Se da cumplimiento a los informes de ley en los tiempos establecidos por las entidades reguladoras. |
| **Gestión administrativa** | Corrupción | Adjudicación de contratos a proveedores sin cumplir requisitos legales. | Sobreprecios, pérdida de recursos públicos, demandas legales. | Alta | 60% moderado | Dirección general | Comité de contratación, verificación de requisitos y licitaciones. | Fortalecer auditorías externas e implementar software de control. | El comité de contratación verifica el cumplimiento de requisitos en los procesos de evaluación de los procesos de la manera más adecuada. |
| **Tesorería** | Corrupción | Malversación de fondos públicos mediante pagos a cuentas no autorizadas. | Pérdida de fondos, afectación de proyectos institucionales, sanciones. | Media | 40% menor | Tesorería | Conciliaciones periódicas y doble verificación de pagos. | Implementar mecanismos de alertas automáticas y auditorías. | Existe plan anual de adquisiciones donde las dependencias solicitan los insumos, materiales y equipos necesarios para el desarrollo de sus actividades. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Gestión administrativa** | Corrupción | Manipulación en los procesos de contratación pública para favorecer a un proveedor específico. | Sanciones legales, pérdida de recursos públicos, daño reputacional. | Media | 60% moderado | Dirección general | Verificación y auditoría de procesos de contratación. | Implementar mecanismos de transparencia, uso de pliegos estandarizados y participación de veedurías ciudadanas. | No se evidencia direccionamiento de contratos. |
| **Gestión archivo** | Corrupción | Manipulación o destrucción de documentos para evitar transparencia. | Pérdida de confianza pública, sanciones legales, falta de trazabilidad. | Media | 60% moderado | Responsable de archivo | Implementación de gestión documental y sistema digital de archivos. | Realizar copias de seguridad y monitoreo regular. | Se esta fortaleciendo el proceso de gestión documental, se realiza back ups en los equipos y existe área de conservación de expedientes físicos con un responsable de la cadena de custodia. |
| **Gestión financiera** | Corrupción | Solicitud de dinero o beneficios personales para acelerar pagos. | Sanciones legales, pérdida de recursos, daño reputacional. | Media | 60% moderado | Tesorería | Auditorías periódicas y control en procesos de pagos. | Implementar denuncias anónimas y mecanismos anticorrupción. | No se evidencia no se conocen denuncias en los canales establecidos por la entidad sobre este tipo de riesgo. |
| **Gestión administrativa** | Seguridad de información | Pérdida de información sensible o ataque cibernético en sistemas de la entidad. | Interrupción de servicios, pérdida de datos, daño a la reputación. | Alta | 80% mayor | Ingeniero de sistemas | Uso de antivirus, copias de seguridad, y control de accesos. | Mejorar sistemas de seguridad, realizar simulacros de ciberseguridad, capacitar al personal | La entidad cuenta con micrositio pago y el nivel de seguridad lo garantiza el proveedor del hosting. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | sobre manejo de datos. | |
| **Gestión turismo** | Seguridad de información | Insatisfacción en los visitantes por mala atención en los puntos de información turística (pit). | Reducción de visitantes y de ingresos, mala percepción de Tenjo. | Muy bajo | 20% leve | Coordinador de turismo | Capacitación en atención al cliente, protocolos de atención en pit. | Implementar encuestas de satisfacción, mejorar capacitación en servicio al cliente. | Existe puntos de atención al usuario con perfiles y capacidades idóneas. |
| **Gestión administrativa** | Seguridad de la información | Pérdida de datos críticos debido a la falta de respaldo periódico de la información. | Pérdida de información, interrupción de procesos, sanciones legales. | Media | 60% moderado | Ingeniero de sistemas | Respaldos parciales manuales. | Implementar políticas de respaldo automático y periódico de la información. | Se cuenta con soporte en el área de sistemas, personal encargado de la custodia y vigilancia de los datos del imctt. |
| **Gestión administrativa** | Seguridad de la información | Acceso no autorizado a la red interna por falta de controles de autenticación robustos. | Robo de información sensible, ciberataques, daño reputacional. | Alta | 60% moderado | Ingeniero de sistemas | Contraseñas básicas y controles de acceso limitados. | Implementar autenticación multifactorial y monitoreo constante de accesos. | Se cuenta con accesos permitidos solo al encargado de soporte del área de sistemas |
| **Gestión administrativa** | Seguridad de la información | Filtración de datos personales de empleados o usuarios por manejo inadecuado de archivos físicos o digitales. | Vulneración de la privacidad, sanciones legales, pérdida de confianza. | Media | 60% moderado | Dirección general | Controles parciales en acceso físico a la información. | Capacitación sobre manejo seguro de la información y uso de encriptación. | Solo se brinda la información exigida por el sigep, de los hojas de vida y declaraciones de renta del personal del imctt. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Gestión administrativa** | Seguridad de la información | Instalación de software no autorizado en equipos de la entidad. | Malware, robo de información, daño a la infraestructura tecnológica. | Media | 60% moderado | Ingeniero de sistemas | Políticas de uso básico de software. | Implementar software de control de instalación y auditorías periódicas. | Se cuenta con software legal en los equipos y esta restringido el acceso a descargas de software no permitido por la entidad. |

Elaboro:

Original firmado

Ing. Alexander Núñez
Oficina de Control interno