ALCALDÍA DE SOLEDAD | TRÁNSITO DE SOLEDAD

# Plan de Tratamiento del Riesgo TIC

# IMTTRASOL



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

**Director Instituto Municipal de Tránsito y Transporte de Soledad**
**IMTTRASOL**
Especialista GERSON JUNIOR BALZA CORRALES

**Jefe Oficina de Sistema y Telecomunicaciones**
Ingeniero RAMSÉS ESCORCIA MAYA

# Plan de Tratamiento del Riesgo TIC

**Instituto Municipal de Tránsito y Transporte de Soledad**
**IMTTRASOL**

**jefesistemas@transitosoledad.gov.co**

**2024**



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

## TABLA DE CONTENIDO

Contenido





**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

## INTRODUCCION

Sin duda como parte de la Seguridad de la Información, es necesario para la entidad hacer una adecuada gestión de riesgos, que le permita saber cuáles son las principales vulnerabilidades de sus activos de información y muy importante, saber cuáles son las amenazas que podrían explotar dichas vulnerabilidades, en la medida que la organización tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

El objetivo fundamental del Plan de tratamiento de riesgos de Seguridad de la Información es evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes teniendo en cuenta los criterios de aceptación de riesgos definidos por la Entidad. Dichas acciones deben ser conocidas, tratadas y ejecutadas por la Entidad de una forma documentada, sistemática, estructurada y eficiente.

En la medida que se tenga una visión de los riesgos que pueden afectar la seguridad de la información, la Entidad puede establecer controles y medidas efectivas, viables y transversales, con el propósito de preservar la disponibilidad, integridad y confidencialidad de su información, para lo cual es necesario definir los lineamientos que se deben seguir para el análisis y evaluación de los riesgos de Seguridad de la Información de la Entidad.

Es responsabilidad del Instituto Municipal de Tránsito y Transporte de Soledad, implementar medidas que permitan mitigar y tratar los riesgos de seguridad y privacidad de la información.

El personal del IMTTRASOL, contratistas, funcionaros y terceros, en cumplimiento de sus funciones, están sometidos a riesgos que pueden ocasionar el no cumplimiento de los objetivos misionales y administrativos del instituto; por lo tanto, es indispensable tomar los controles necesarios, para identificar las causas y consecuencias de la materialización de dichos riesgos.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información del Instituto Municipal de Tránsito y Transporte de Soledad, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo en la entidad, de manera que, al comprender el concepto de riesgo, así como el contexto, a través de este instrumento se planean las acciones que reduzcan la afectación a la entidad en caso de materialización de estos, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el mundo en el Entorno Digital.



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

# 1. OBJETIVOS

## 1.1. Objetivo General:

Desarrollar el Plan de Tratamiento del riesgo al interior del Instituto Municipal de Tránsito y Transporte de Soledad, siguiendo los lineamientos de la metodología de gestión de riesgos de seguridad y privacidad de la información, a través de la identificación de activos de información, amenazas, vulnerabilidades, riesgos y controles, los niveles aceptables y tratamiento de riesgo, con el propósito de maximizar la probabilidad de alcanzar los objetivos organizacionales perseguidos por IMTTRASOL.

## 1.2. Objetivos Específicos:

- Identificar y tratar los riesgos en todos los niveles del Instituto Municipal de Tránsito y Transporte de Soledad.
- Proteger la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte del Instituto.
- Comprometer a todos los servidores de la Entidad, en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos.
- Establece una base confiable para la toma de decisiones y la planificación.
- Mejora la eficacia y la eficiencia operativa del Instituto Municipal de Tránsito y Transporte de Soledad.
- Mejora el aprendizaje y la flexibilidad organizacional.



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

## 2. ALCANCE DEL DOCUMENTO

Los lineamientos contenidos en el presente documento son aplicables a todos los niveles del Instituto Municipal de Tránsito y Transporte de Soledad, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del IMTRASOL compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los entes de control, entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación.

De igual manera aplica para el Plan de Tratamiento del riesgo del Instituto Municipal de Tránsito y Transporte de Soledad.

## 3. DEFINICIONES

**Activo:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.

**Activo crítico:** Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectarán el cumplimiento de los objetivos estratégicos de la entidad.

**Administración de Riesgos:** Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

**Análisis de Riesgos:** Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de determinar su aceptación y manejo.

**Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

**Análisis de Impacto al Negocio (BIA):** Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.

**Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

**Características de la Información:** las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

**Causas:** (internas o externas): Aquello que se considera como fundamento u origen de algo.

**Compromiso de la Dirección:** Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

**Control:** Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

**Control correctivo:** Es el control que se realiza para eliminar la (s) causa (s) de una no conformidad detectada u otra situación indeseable.

**Control preventivo:** Es el control que se realiza para eliminar la (s) causa (s) de una no conformidad potencial u otra situación potencialmente indeseable.

**Confiabilidad de la Información:** Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

**Confidencialidad:** Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

**Consecuencia:** resultado, efecto o impacto de un riesgo o un evento.

**Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

**Evento:** Es el suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

**Evento de seguridad de la información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

**Evaluación del Riesgo:** Proceso utilizado para determinar las prioridades de la administración del riesgo, comparando el nivel de un determinado riesgo con respecto a un estándar determinado, es decir, calificar el riesgo de acuerdo a su impacto con respecto a la probabilidad.



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

**Frecuencia:** Es el número de veces que se repite un evento o un hecho en el tiempo.

**Impacto:** Efecto positivo o negativo producido por un acontecimiento, evento o riesgo.

**Identificación del Riesgo:** Proceso para determinar las causas internas y/o externas (debido a…), evento (lo que puede suceder…riesgo) y la consecuencia (lo que podría ocasionar que…).

**Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

**Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

**Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

**Legalidad:** Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.

**Mesa de Servicios:** Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que la Oficina de Sistemas y Telecomunicaciones recolecta las necesidades que tienen dependencias en cuanto a los recursos tecnológicos.

**No repudio:** El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.

**Partes interesadas:** Persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

**Plan de Continuidad de Negocio:** Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

**Propietario de la información (titular):** Es la unidad organizacional o proceso donde se crean los activos de información.



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

**Probabilidad:** Cualidad de probable, que puede suceder.

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

**Riesgo Residual:** Riesgo remanente después de la implementación del tratamiento del riesgo.

**Riesgo Estratégico:** Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

**Riesgos Operativos:** Comprende los riesgos relacionados tanto con la parte operativa como con la técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos y la ejecución de los procedimientos en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

**Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad, que incluye la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, así como de su interacción con las demás áreas, dependerá en gran parte el éxito o fracaso de toda entidad.

**Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

**Riesgos de Tecnología:** Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga sus necesidades actuales, futuras y soporte el cumplimiento de la misión.

**Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso.

**Terceros:** Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.

**Valoración del Riesgo:** Es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados en el elemento de control.

**Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

## 4. MARCO NORMATIVO

A continuación, se relaciona la normatividad que soporta el diseño y ejecución de la Metodología de Gestión de Riesgos del Instituto Municipal de Tránsito y Transporte de Soledad, el cual se encuentra fundamentado en el marco legal y las políticas establecidas para el uso de las tecnologías de la información y la seguridad digital en las entidades públicas del Estado.

**Ley 87 de 1993**. "por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones"

**Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

**Ley 527 de 1999.** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

**Ley 850 de 2003.** Por medio de la cual se reglamentan las veedurías ciudadanas.

Ley 872 de 2003. Por el cual se crea el Sistema de Gestión de la Calidad en la rama ejecutiva del poder público y en otras prestadoras de servicio.

**Ley 962 de 2005.** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos Administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

**Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

**Ley 1273 de 2009.** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

**Ley 1341 de 2009**. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones.

**Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

**Ley 1474 de 2011.** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

**Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

**Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.

**Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

**Ley 1978 de 2019.** Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones.

**Decreto 1747 de 2000.** Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con: "Las entidades de certificación, los certificados y las firmas digitales".

**Decreto 19 de 2012.** Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

**Decreto 2609 de 2012.** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

**Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.

**Decreto 2573 de 2014.** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

**Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.

**Decreto 943 de 2014.** Por el cual se adopta la actualización del Modelo Estándar de Control Interno.

**Decreto 1078 de 2015.** Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y las comunicaciones – Título 9 – Capítulo I.

**Decreto 415 de 2016**. Por el cual se adiciona el Decreto Único Reglamentario del Sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

**Decreto 1499 de 2017**. Modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública

**Decreto 1008 de 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

**Conpes 3854 de 2016.** Política Nacional de Seguridad Digital.

**Conpes 3920 de 2018.** Política Nacional de Explotación de Datos.



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

## 5. IDENTIFICACIÓN DEL RIESGO

Riesgo es la probabilidad de ocurrencia de un hecho que no permita cumplir con el propósito definido en el proceso.

La identificación del riesgo se realiza determinando las causas, con base en los factores internos y/o externos analizados, y que pueden afectar el logro de los objetivos del proceso.

Se deben considerar las causas y eventos posibles que pueden inducir al riesgo, para ello prima el conocimiento de los procesos por parte de los responsables, el conocimiento del medio, los análisis estratégicos que se definen, los factores que inducen el riesgo resultante de la experiencia de quien los trabaja diariamente.

Para identificar un riesgo, se debe pensar en las clases de factor de riesgo que pueden generarlo como son:

<table>
<tr><th colspan="2">FACTORES INTERNOS Y EXTERNOS DE RIESGO</th></tr>
<tr><th>Externos</th><th>Internos</th></tr>
<tr><td>Económicos: Disponibilidad de capital, emisión de deuda o no pago de la misma, liquidez, mercados financieros, competencias.</td><td>Infraestructura: Disponibilidad de activos, capacidad de los activos, acceso al capital.</td></tr>
<tr><td>Ambientales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.</td><td>Personal: Capacidad del personal, salud, seguridad.</td></tr>
<tr><td>Políticos: Cambios de gobierno, legislación, políticas públicas.</td><td>Procesos: Capacidad, diseño, ejecución, proveedores, entradas, salidas, conocimientos.</td></tr>
<tr><td>Sociales: Demografía, responsabilidad social, terrorismo.</td><td rowspan="2">Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento.</td></tr>
<tr><td>Tecnológicos: Interrupciones, comercio electrónico, datos externos, tecnología emergente.</td></tr>
</table>

El Objetivo de la identificación de riesgos es desarrollar una completa lista de fuentes de riesgo y eventos que puedan tener un impacto en el logro de los objetivos críticos identificados en el contexto.

Con base en el análisis de los riesgos de los activos de la información a continuación se relacionan los riesgos más susceptibles en el Instituto Municipal de Tránsito y Transporte de Soledad:



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

| RIESGOS IMTTRASOL | |
|---|---|
| **ID Riesgo** | **Escenario de Riesgo** |
| **R1** | Acceso no autorizado de personas a equipos y servidores por mala gestión de configuraciones de seguridad y ausencia de mecanismos de identificación y autenticación de usuario. |
| **R2** | Daño a los equipos y servidores parte de funcionarios y/o terceros debido a exposición de temperaturas extremas y uso incorrecto de los mismos. |
| **R3** | Fallas parciales o totales de equipos debido a no realizar jornadas de mantenimiento |
| **R4** | Pérdida parcial o total del servicio o equipo causado por inundaciones, incendio y movimientos telúricos. |
| **R5** | Indisponibilidad en la prestación de servicio tanto a usuarios internos como externos debido a problemas o cortes en los servicios públicos primarios |
| **R6** | Divulgación de información por falta de procedimientos para manejo de medios y devolución de activos TI. |
| **R7** | Degradación y/o problemas en la prestación del servicio y fallos o mal funcionamiento de aplicaciones o activos de gestión de red, por configuración errónea, manipulación del software o aplicativo de manera indebida, debido a falta de gestión de versiones, actualizaciones y mala gestión de contraseñas. |
| **R8** | Descarga, instalación y uso de Software no licenciado o no autorizado en los equipos de computo |
| **R9** | Daño, perdida de datos e información de la base de datos debido a falta de controles de acceso, copias de seguridad, documentación y por no contar con controles ante infecciones de malware |
| **R10** | Falla, interferencia en el servicio de datos e Internet debido a conexión deficiente en el cableado y falta de mantenimiento de los dispositivos por parte del proveedor. |
| **R11** | Hurto y manipulación de la información de manera indebida, causado por la ausencia de controles de acceso de usuarios, conexiones de red desprotegidas, falta de protección de código malicioso, mala gestión de contraseñas, falta de procedimientos para baja de usuarios y uso de medios removibles no controlado |
| **R12** | Ataques a los portales de la entidad y publicación de contenidos o correos con información confidencial o no autorizada, debido a configuraciones de seguridad débiles. |
| **R13** | Error de acceso a sistemas bancarios y financieros debido a perdida de conectividad de Intranet y/o red |
| **R14** | Por no contar con una adecuada instalación eléctrica, se podría presentar el daño de los equipos tecnológicos en general. |
| **R15** | Errores en el uso del sistema debido a la ausencia de un eficiente control de cambios en la configuración, entrenamiento insuficiente del personal, falta de conciencia acerca de seguridad de la información. |
| **R16** | Errores en el uso de hardware y software debido a falta de capacitación técnica de personal de soporte técnico. |
| **R17** | Incumplimiento de compromisos debido a acciones deliberadas de los funcionarios causada por el inconformismo laboral, ausentismo y/o por contar con funcionarios sin la competencia requerida. |
| **R18** | Suplantación o uso de personal no autorizado a los sistemas debido a gestión de acceso ineficiente y política de puestos de trabajo. |
| **R19** | Hurto, fraude o sabotaje de equipos, medios, información o documentos, debido a la falta de protección de cables y dispositivos, una inadecuada protección de la información en lugares no apropiados y por no contar con una práctica de clasificación de información que proponga los niveles de protección de esta. |
| **R20** | Accesos no autorizados a oficinas debido a uso inadecuado o descuidado del control de acceso físico a oficinas y áreas protegidas. |



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

## 6. ANALISIS Y EVALUACION DEL RIESGO

El Riesgo Inherente, es la evaluación del riesgo en ausencia de cualquier acción que la administración pueda tomar encaminada a minimizar la posibilidad de ocurrencia o impacto del riesgo, es la exposición al riesgo sin controles. La medición del riesgo consiste en evaluar dos criterios, la probabilidad de ocurrencia del riesgo y el impacto que pueda generar su materialización. La probabilidad, es la posibilidad de ocurrencia de un evento teniendo en cuenta la frecuencia en que éste se dé o pueda darse, de acuerdo con los hechos históricos que se han presentado en IMTTRASOL. El impacto, es el resultado de un evento expresado cualitativa o cuantitativamente en pérdida, perjuicio, desventaja o ganancia. Para establecer la probabilidad de ocurrencia y el impacto se utilizarán la siguiente tabla

**Probabilidad de Ocurrencia:**

| NIVEL | DESCRIPTOR | DESCRIPCION | FRECUENCIA |
|---|---|---|---|
| 1 | Raro | El evento puede ocurrir solo en circunstancias excepcionales | No se ha presentado en los últimos 5 años |
| 2 | Improbable | El evento puede ocurrir en algún momento | Al menos de una vez en los últimos 5 años |
| 3 | Posible | El evento podría ocurrir en algún momento | Al menos de una vez en los últimos 2 años |
| 4 | Probable | El evento probablemente ocurrirá en la mayoría de las circunstancias | Al menos de una vez en el último año |
| 5 | Casi Seguro | Se espera que el evento ocurra en la mayoría de las circunstancias | Mas de una vez al año |

**Impacto:**

| NIVEL | DESCRIPTOR | DESCRIPCION |
|---|---|---|
| 1 | Insignificante | Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad |
| 2 | Menor | Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad |
| 3 | Moderado | Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad |
| 4 | Mayor | Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad |
| 5 | Catastrófico | Si el hecho llegara a presentarse, tendría desastrosos efectos o consecuencias sobre la entidad. |

Los impactos de mayor ocurrencia en las entidades del Estado son:

-Impacto de confidencialidad en la información
-Impacto legal
-Impacto de credibilidad o imagen
-Impacto operativo

La combinación entre la probabilidad y el impacto, da como resultado la severidad del riesgo el cual puede ser clasificado como: bajo, moderado, alto o extremo, como resultado de esta medición se determina el Riesgo Inherente del proceso evaluado.

| | | IMPACTO | | | | |
|---|---|---|---|---|---|---|
| | | 1. Insignificante | 2. Menor | 3. Moderado | 4. Mayor | 5. Catastrófico |
| PROBABILIDAD | 5. Casi Seguro | | | | | |
| | 4. Probable | | | | | |
| | 3. Posible | | | | | |
| | 2. Improbable | | | | | |
| | 1. Raro | | | | | |

| ZONA DE RIESGO | Bajo | Moderado | Alto | Extremo |
|---|---|---|---|---|
| RESPUESTA | Asumir | Asumir - Reducir | Reducir – Evitar - Transferir | Reducir – Evitar - Transferir |



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

| ANALISIS Y EVALUACION DEL RIESGO | | | | | |
|---|---|---|---|---|---|
| **PROCESO:** GESTION DE LAS TECNOLOGÍAS DE LA INFORMACION | | | | | |
| **OBJETIVO:** Dirigir, planear, coordinar y controlar el diseño, la implementación, seguimiento y evaluación, de los sistemas de información requeridos por el Instituto Municipal de tránsito y transporte de Soledad, aplicando métodos cuantitativos y heurísticos en la interacción con las diferentes dependencias, para fortalecer de forma ágil, oportuna y eficiente los procesos. | | | | | |
| **No.** | **RIESGO** | **CALIFICACION** | | **TIPO IMPACTO** | **EVALUACION** |
| | | **Probabilidad** | **Impacto** | | **Zona de Riesgo** |
| **R1** | Acceso no autorizado de personas a equipos y servidores por mala gestión de configuraciones de seguridad y ausencia de mecanismos de identificación y autenticación de usuario. | Posible | Moderado | Confidencialidad de la información | **Alto** |
| **R2** | Daño a los equipos y servidores parte de funcionarios y/o terceros debido a exposición de temperaturas extremas y uso incorrecto de los mismos. | Posible | Menor | Operativo | **Moderado** |
| **R3** | Fallas parciales o totales de equipos debido a no realizar jornadas de mantenimiento | Posible | Moderado | Operativo | **Alto** |
| **R4** | Pérdida parcial o total del servicio o equipo causado por inundaciones, incendio y movimientos telúricos. | Improbable | Catastrófico | Operativo | **Extremo** |
| **R5** | Indisponibilidad en la prestación de servicio tanto a usuarios internos como externos debido a problemas o cortes en los servicios públicos primarios | Probable | Mayor | Operativo | **Extremo** |
| **R6** | Divulgación de información por falta de procedimientos para manejo de medios y devolución de activos TI. | Posible | Moderado | Confidencialidad de la información | **Alto** |
| **R7** | Degradación y/o problemas en la prestación del servicio y fallos o mal funcionamiento de aplicaciones o activos de gestión de red, por configuración errónea, manipulación del software o aplicativo de manera indebida, debido a falta de gestión de versiones, actualizaciones y mala gestión de contraseñas. | Improbable | Menor | Operativo | **Bajo** |
| **R8** | Descarga, instalación y uso de Software no licenciado o no autorizado en los equipos de computo | Probable | Menor | Legal | **Alto** |
| **R9** | Daño, perdida de datos e información de la base de datos debido a falta de controles de acceso, copias de seguridad, documentación y por no contar con controles ante infecciones de malware | Posible | Mayor | Operativo | **Extremo** |
| **R10** | Falla, interferencia en el servicio de datos e Internet debido a conexión deficiente en el cableado y falta de mantenimiento de los dispositivos por parte del proveedor. | Posible | Moderado | Operativo | **Alto** |



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

| | | | | | |
|---|---|---|---|---|---|
| **R11** | Hurto y manipulación de la información de manera indebida, causado por la ausencia de controles de acceso de usuarios, conexiones de red desprotegidas, falta de protección de código malicioso, mala gestión de contraseñas, falta de procedimientos para baja de usuarios y uso de medios removibles no controlado | Posible | Mayor | Confidencialidad de la información | **Extremo** |
| **R12** | Ataques a los portales de la entidad y publicación de contenidos o correos con información confidencial o no autorizada, debido a configuraciones de seguridad débiles. | Posible | Mayor | Confidencialidad de la información | **Extremo** |
| **R13** | Error de acceso a sistemas bancarios y financieros debido a perdida de conectividad de Intranet y/o red | Improbable | Moderado | Operativo | **Moderado** |
| **R14** | Por no contar con una adecuada instalación eléctrica, se podría presentar el daño de los equipos tecnológicos en general. | Posible | Moderado | Operativo | **Alto** |
| **R15** | Errores en el uso del sistema debido a la ausencia de un eficiente control de cambios en la configuración, entrenamiento insuficiente del personal, falta de conciencia acerca de seguridad de la información. | Posible | Menor | Operativo | **Moderado** |
| **R16** | Errores en el uso de hardware y software debido a falta de capacitación técnica de personal de soporte técnico. | Raro | Menor | Operativo | **Bajo** |
| **R17** | Incumplimiento de compromisos debido a acciones deliberadas de los funcionarios causada por el inconformismo laboral, ausentismo y/o por contar con funcionarios sin la competencia requerida. | Posible | Moderado | Credibilidad o Imagen | **Alto** |
| **R18** | Suplantación o uso de personal no autorizado a los sistemas debido a gestión de acceso ineficiente y política de puestos de trabajo. | Improbable | Moderado | Confidencialidad de la información | **Moderado** |
| **R19** | Hurto, fraude o sabotaje de equipos, medios, información o documentos, debido a la falta de protección de cables y dispositivos, una inadecuada protección de la información en lugares no apropiados y por no contar con una práctica de clasificación de información que proponga los niveles de protección de esta. | Posible | Mayor | Confidencialidad de la información | **Extremo** |
| **R20** | Accesos no autorizados a oficinas debido a uso inadecuado o descuidado del control de acceso físico a oficinas y áreas protegidas. | Casi Seguro | Mayor | Confidencialidad de la información | **Extremo** |



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

## 7. TRATAMIENTO DEL RIESGO

### 7.1. OPCIÓN DE TRATAMIENTO:

Según la zona donde se ubica el riesgo residual, se determina la opción o estrategia de tratamiento a seguir para combatir el riesgo, para esta actividad se debe considerar la siguiente tabla:

| ZONA DE RIESGO RESIDUAL | NIVEL DE RIESGO ACEPTABLE | OPCIÓN O ESTRATEGIA DE TRATAMIENTO A SEGUIR |
|---|---|---|
| **Bajo** | Aceptable | Asumir |
| **Moderado** | Aceptable | Asumir/Reducir |
| **Alto** | No Aceptable | Reducir/Evitar/Transferir |
| **Extremo** | No Aceptable | Reducir/Evitar/Transferir |

**¿COMO TRATAR LOS RIESGOS?**

| TRATAMIENTO | DECISIÓN | MECANISMOS | EJEMPLO |
|---|---|---|---|
| **Transferirlo o compartir** | Buscar un tercero | Traspaso de la actividad a otra entidad mediante uso de contratos, acuerdos de seguros, alianzas estratégicas | Información de la entidad se puede duplicar y guardar en otro sitio |
| **Reducirlo** | Tomar medidas encaminadas a reducir probabilidad (medidas de prevención) e impacto (medidas de Protección) | Crear controles o mejorar los existentes | Una actividad de Inspección que hoy es manual se puede optimizar mediante la automatización |
| **Evitarlo** | Tomar medidas encaminadas a reducir probabilidad (medidas de prevención) e impacto (medidas de Protección) de manera que se pueda operar el proceso obviando el riesgo | Analizar las consecuencias de realizar cambios sustanciales a la actividad mediante rediseño, mejoramiento, optimización o eliminación | No lanzarse en una nueva línea de negocio |
| **Asumir** | Primero tome medidas para reducirlo o transferirlo y después genere planes de contingencia por si llegase a materializarse | Establecer los controles necesarios y si queda un riesgo residual diseñar planes de contingencia | Tercerizar la actividad mediante un seguro y después generar un plan para la recuperación de la actividad |

### 7.2. REGISTRO DEL TRATAMIENTO DEL RIESGO:

El registro del tratamiento de riesgos de seguridad de la información se realiza en los siguientes campos:

- Opción de tratamiento: Campo que se calcula automáticamente de acuerdo con la valoración del riesgo, teniendo en cuenta el Nivel de Riesgo Aceptable.
- Acciones de mejora: Es la redacción del control teniendo en cuenta la siguiente estructura; responsable de la ejecución + acción realizada + complemento.
- Soporte: Registro de la evidencia que deja la implementación de la acción de mejora.
- Responsable: Registrar el rol o cargo responsable de implementar la acción de mejora.
- Fecha implementación: Periodo de tiempo en el cual se implementará la acción de mejora.

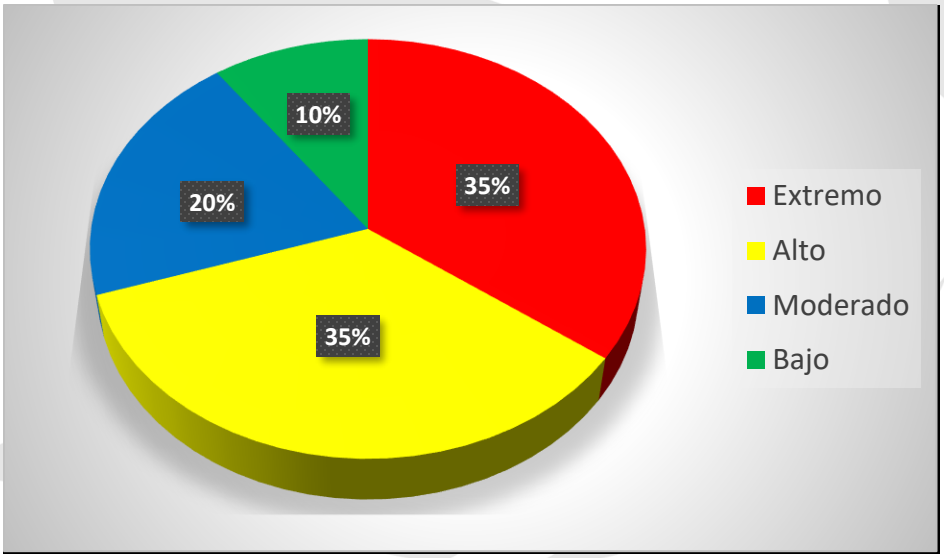


**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

## 7.3. RESULTADOS VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se discriminan los riesgos de seguridad de la información identificados por nivel de riesgo:

| NIVEL DE RIESGO | CANTIDAD RIEGOS | % |
|---|---|---|
| Extremo | 7 | 35% |
| Alto | 7 | 35% |
| Moderado | 4 | 20% |
| Bajo | 2 | 10% |
| **TOTAL** | 20 | 100% |






**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

## 7.4. ACCIONES PARA EL TRATAMIENTO DEL RIESGO:

| IDENTIFICACIÓN DEL RIESGO / VALORACIÓN DEL RIESGO | | | | PLAN DE TRATAMIENTO | | | | |
|---|---|---|---|---|---|---|---|---|
| **No.** | **RIESGO** | **TIPO IMPACTO** | **ZONA DE RIESGO** | **OPCION DE TRATAMIENTO** | **ACCIONES DE MEJORA** | **SOPORTE** | **RESPONSABLE** | **FECHA** |
| **R1** | Acceso no autorizado de personas a equipos y servidores por mala gestión de configuraciones de seguridad y ausencia de mecanismos de identificación y autenticación de usuario. | Confidencialidad de la información | **Alto** | Reducir/Evitar/ Transferir | -Revisión continua de acceso personal del área de sistemas | Sistema Biométrico | Oficina de Sistemas | Diciembre 2024 |
| **R2** | Daño a los equipos y servidores parte de funcionarios y/o terceros debido a exposición de temperaturas extremas y uso incorrecto de los mismos. | Operativo | **Moderado** | Reducir/Evitar/ Transferir | -Divulgación de Políticas de seguridad.<br>-Asignación de activos con responsabilidad sobre el mismo. | Actas de entrega de activos | Oficina de Sistemas | Diciembre 2024 |
| **R3** | Fallas parciales o totales de equipos debido a no realizar jornadas de mantenimiento | Operativo | **Alto** | Reducir/Evitar/ Transferir | -Implementar el plan de mantenimiento preventivo. | Plan de mantenimiento | Oficina de Sistemas | Diciembre 2024 |
| **R4** | Pérdida parcial o total del servicio o equipo causado por inundaciones, incendio y movimientos telúricos. | Operativo | **Extremo** | Reducir/Evitar/ Transferir | -Se debe contar con un Plan de Contingencia ante estos eventos | Plan de Contingencia | Oficina de Sistemas | Diciembre 2024 |
| **R5** | Indisponibilidad en la prestación de servicio tanto a usuarios internos como externos debido a problemas o cortes en los servicios públicos primarios. | Operativo | **Extremo** | Reducir/Evitar/ Transferir | -Coordinar medios alternos como plantas eléctricas y servicios de Internet | Reunión con Proveedores de Servicios | Oficina de Sistemas | Diciembre 2024 |
| **R6** | Divulgación de información por falta de procedimientos para manejo de medios y devolución de activos TI. | Confidencialidad de la información | **Alto** | Reducir/Evitar/ Transferir | -Establecer e implementar procedimientos para manejo de medios y devolución de activos TI | Procedimientos Establecidos | Oficina de Sistemas | Diciembre 2024 |
| **R7** | Degradación y/o problemas en la prestación del servicio y fallos o mal funcionamiento de aplicaciones o activos de gestión de red, por configuración errónea, manipulación del software o aplicativo de manera indebida, debido a falta de gestión de versiones, actualizaciones y mala gestión de contraseñas. | Operativo | **Bajo** | Asumir | -Realizar configuración de dispositivos adecuadamente<br>-Gestión y Actualización de Versiones de Aplicaciones<br>-Gestión adecuada de contraseñas | Configuración de Activos y Contraseñas | Oficina de Sistemas | Diciembre 2024 |
| **R8** | Descarga, instalación y uso de Software no licenciado o no autorizado en los equipos de cómputo. | Legal | **Alto** | Reducir/Evitar/ Transferir | -Mantener actualizado el Software de los equipos. | Software Actualizados | Oficina de Sistemas | Diciembre 2024 |
| **R9** | Daño, perdida de datos e información de la base de datos debido a falta de controles de acceso, copias de seguridad, documentación y por no contar con controles ante infecciones de malware. | Operativo | **Extremo** | Reducir/Evitar/ Transferir | -Establecer controles de acceso<br>-Implementar procedimiento de copia de seguridad<br>-Mantener actualizado el firewall | Procedimientos Consolidados | Oficina de Sistemas | Diciembre 2024 |
| **R10** | Falla, interferencia en el servicio de datos e Internet debido a conexión deficiente en el cableado y falta de mantenimiento de los dispositivos por parte del proveedor. | Operativo | **Alto** | Reducir/Evitar/ Transferir | -Coordinar un plan de mantenimiento de equipos y redes con el proveedor de servicio. | Plan de mantenimiento de redes | Oficina de Sistemas | Diciembre 2024 |



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **R11** | Hurto y manipulación de la información de manera indebida, causado por la ausencia de controles de acceso de usuarios, conexiones de red desprotegidas, falta de protección de código malicioso, mala gestión de contraseñas, falta de procedimientos para baja de usuarios y uso de medios removibles no controlado | Confidencialidad de la información | **Extremo** | Reducir/Evitar/ Transferir | -Establecer controles de acceso a usuarios<br>-Proteger las conexiones de Red.<br>-Realizar Gestión de Contraseñas<br>-Establecer procedimientos para baja de Usuarios<br>-Mantener actualizado el firewall | Procedimiento de Gestión de contraseñas, baja de usuarios y control de accesos | Oficina de Sistemas | Diciembre 2024 |
| **R12** | Ataques a los portales de la entidad y publicación de contenidos o correos con información confidencial o no autorizada, debido a configuraciones de seguridad débiles. | Confidencialidad de la información | **Extremo** | Reducir/Evitar/ Transferir | -Desarrollar configuraciones de seguridad solidas que eviten los ataques cibernéticos a la entidad | Configuraciones de seguridad establecidas | Oficina de Sistemas | Diciembre 2024 |
| **R13** | Error de acceso a sistemas bancarios y financieros debido a perdida de conectividad de Intranet y/o red | Operativo | **Moderado** | Asumir /Reducir | -Verificación de contrato de servicios de internet | Contrato servicios | Oficina de Sistemas | Diciembre 2024 |
| **R14** | Por no contar con una adecuada instalación eléctrica, se podría presentar el daño de los equipos tecnológicos en general. | Operativo | **Alto** | Reducir/Evitar/ Transferir | -Revisión y mantenimiento de las instalaciones eléctricas del instituto | Plan de mantenimiento | Oficina de Sistemas | Diciembre 2024 |
| **R15** | Errores en el uso del sistema debido a la ausencia de un eficiente control de cambios en la configuración, entrenamiento insuficiente del personal, falta de conciencia acerca de seguridad de la información. | Operativo | **Moderado** | Asumir /Reducir | -Capacitación del personal en los aplicativos y medidas de seguridad en el uso del sistema | Plan de capacitación | Oficina de Sistemas | Diciembre 2024 |
| **R16** | Errores en el uso de hardware y software debido a falta de capacitación técnica de personal de soporte técnico. | Operativo | **Bajo** | Reducir/Evitar/ Transferir | -Capacitación técnica a los funcionarios de soporte técnico | Plan de capacitación | Oficina de Sistemas | Diciembre 2024 |
| **R17** | Incumplimiento de compromisos debido a acciones deliberadas de los funcionarios causada por el inconformismo laboral, ausentismo y/o por contar con funcionarios sin la competencia requerida. | Credibilidad o Imagen | **Alto** | Reducir/Evitar/ Transferir | -Control de actividades de los funcionarios y de sus competencias. | Registro de actividades | Oficina de Sistemas | Diciembre 2024 |
| **R18** | Suplantación o uso de personal no autorizado a los sistemas debido a gestión de acceso ineficiente y política de puestos de trabajo. | Confidencialidad de la información | **Moderado** | Asumir /Reducir | -Establecer una gestión de accesos eficiente y segura | Gestión de Accesos | Oficina de Sistemas | Diciembre 2024 |
| **R19** | Hurto, fraude o sabotaje de equipos, medios, información o documentos, debido a la falta de protección de cables y dispositivos, una inadecuada protección de la información en lugares no apropiados y por no contar con una práctica de clasificación de información que proponga los niveles de protección de esta. | Confidencialidad de la información | **Extremo** | Reducir/Evitar/ Transferir | -Establecer una adecuada protección de los activos de información mediante el aseguramiento de oficinas, identificación de ingreso del personal, cámaras de seguridad. | Medidas de protección establecidas | Oficina de Sistemas | Diciembre 2024 |
| **R20** | Accesos no autorizados a oficinas debido a uso inadecuado o descuidado del control de acceso físico a oficinas y áreas protegidas. | Confidencialidad de la información | **Extremo** | Reducir/Evitar/ Transferir | -Revisión continua de acceso de personal | Sistema Biométrico | Oficina de Sistemas | Diciembre 2024 |



**CALLE 63 No. 13-61**, Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

## BIBLIOGRAFÍA

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Manual Operativo del Modelo Integrado de Planeación y Gestión. 2019.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Manual De Gobierno Digital. 2018.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. G.ES.05 Diseño e implementación de una estrategia de seguridad de la información. 2019.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI. 2019.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad de la información. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía Elaboración de la política general de seguridad y privacidad de la información. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía Procedimientos De Seguridad De La Información. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía Roles y Responsabilidades. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Gestión y Clasificación de Activos de Información. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía de Gestión de Riesgos.2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Manual de Políticas de Seguridad y Privacidad de la información. 2021.

INSTITUTO PARA LA ECONOMIA SOCIAL. Aplicación metodológica Gestión de Riesgos Operativos. 2017

UNIDAD NACIONAL PARA LA GESTIÓN DEL RIESGO DE DESASTRES. Plan Tratamiento de Riesgos. 2022.

INSTITUTO MUNICIPAL DE TRANSITO Y TRANSPORTE DE SOLEDAD. Resolución No. 003 D.T. enero 04 de 2021 Adopción del plan anual de adquisición de bienes y servicios para la vigencia fiscal 2021.



**CALLE 63 No. 13-61,** Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co

## CONTROL DE VERSIONES

| TITULO | ANALISIS Y EVALUACION DEL RIESGO TIC IMTTRASOL |
|---|---|
| PROCESOS | Gestión Tecnologías de la Información |

| VERSIÓN | FECHA DE APROBACIÓN | REFERENCIA DE CAMBIO |
|---|---|---|
| V 1.0 | 18-11-2021 | Versión Inicial |

**ENCARGADOS DE LA ELABORACIÓN Y REVISIÓN DEL DOCUMENTO**

| NOMBRE | ORGANIZACIÓN | CARGO | FECHA |
|---|---|---|---|
| Ingeniero<br>RAMSÉS ESCORCIA MAYA | Instituto Municipal de Tránsito y Transporte de Soledad | Jefe Oficina de Sistema y Telecomunicaciones | 10-01-2024 |
| RAMSES R. ESCORCIA M. JEFE OFICINA SISTEMAS IMTTRASOL FIRMA | | | |



**CALLE 63 No. 13-61,** Prolongación Avenida Murillo.
**Centro Comercial Nuestro Atlántico. Piso 2, Local 2005**
Soledad, Colombia
✆ **TELÉFONO (+5) 3931108 – 3930087 - 3930078** ✉ pqrsf@transitosoledad.gov.co