



## PLAN GENERAL PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION

**TRANSCARIBE S.A.**

**ENERO DE 2022**

**CARTAGENA DE INDIAS**





## TABLA DE CONTENIDO

<b>1</b>	<b>CONTENIDO</b>	
<b>2</b>	<b>HISTORIA</b>	<b>3</b>
<b>3</b>	<b>INTRODUCCIÓN</b>	<b>4</b>
<b>4</b>	<b>OBJETIVO</b>	<b>5</b>
<b>5</b>	<b>ALCANCE</b>	<b>5</b>
<b>6</b>	<b>OBJETIVOS ESPECIFICOS</b>	<b>5</b>
<b>7</b>	<b>TERMINOS Y DEFINICIONES</b>	<b>6</b>
<b>8</b>	<b>VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD DE LA INFORMACION</b>	<b>9</b>
<b>8.1</b>	<b>ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>10</b>
<b>8.1.1</b>	<b>Criterios de evaluación del riesgo de seguridad de la información:</b>	<b>10</b>
<b>8.1.2</b>	<b>Criterios de Impacto</b>	<b>10</b>
<b>8.1.3</b>	<b>Criterios de Aceptación</b>	<b>11</b>
<b>8.2</b>	<b>VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>11</b>
<b>8.2.1</b>	<b>Identificación del riesgo</b>	<b>11</b>
<b>8.2.2</b>	<b>Estimación del riesgo</b>	<b>13</b>
<b>8.2.3</b>	<b>Determinación del riesgo inherente y residual</b>	<b>15</b>
<b>8.2.4</b>	<b>Evaluación de los riesgos</b>	<b>18</b>
<b>8.3</b>	<b>TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>19</b>
<b>8.4</b>	<b>MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>20</b>
<b>8.5</b>	<b>CRONOGRAMA VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION</b>	<b>20</b>





## 2 HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	03/01/2019	Versión uno del documento
1.0.1	25/01/2022	Versión dos del documento





### 3 INTRODUCCIÓN

No hay empresas que no se encuentre sumida en la tecnología digital, que reconocen el protagonismo de los datos que generan la información que se requieren en los procesos de gestión de nuestra entidad. Por consiguiente, la importancia de tener esta información identificada y protegida, incluyendo la de los sujetos o clientes internos o externos, enmarcada bajo las relaciones de cumplimiento y acuerdos comerciales y contractuales como los son los de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

Transcaribe S.A. decide entonces vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información aprobada por la Gerencia, y como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, íntegra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

- **Confidencialidad:** Propiedad que la información sea concedida únicamente a quien esté autorizado.
- **Integridad:** Propiedad que la información se mantenga exacta y completa.
- **Disponibilidad:** Propiedad que la información sea accesible y utilizable en el momento que se requiera.





## 4 OBJETIVO

Proporcionar al Sistema Integrado de Transporte Masivo de Cartagena de Indias – Transcaribe S.A. de herramientas tecnológicas con enfoque sistemático que provea las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información, a través de métodos que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y expedición de políticas, así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo.

## 5 ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, será aplicada sobre cualquier proceso del Sistema Integrado de Transporte Masivo de Cartagena de Indias – Transcaribe S.A., en cualquiera de sus sistema de información actual o futuro, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificando los riesgos de seguridad de la información actuales.

## 6 OBJETIVOS ESPECIFICOS

El beneficio del apoyo y cumplimiento de los propósitos de la política estratégica de seguridad de la información en TRANSCARIBE S.A., se declaran los siguientes objetivos específicos:

- Capacitar al personal de la entidad para que conozcan el sistema de seguridad de la información de la entidad.
- Buscar el apoyo irrestricto de la Alta dirección y demás dependencia a este plan.
- Ofrecer principios que propendan por la unificación y el conocimiento de los criterios para la administración de los riesgos de seguridad de la información de la entidad.
- Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas de seguridad de la información que se apliquen al entorno de gestión de la Entidad.
- Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas a estos.





- Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información y su mitigación.
- Reducir toda posibilidad de que una brecha o evento produzca determinado impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.
- Lograr y mantener a través de la implementación de medidas de control el nivel de probabilidad e impacto residual de los riesgos a el nivel aceptable por parte de la Alta Gerencia.

## 7 TERMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información, en beneficio de unificar criterios dentro de la entidad.

**Administración del riesgo:** Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

**Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

**Análisis de riesgos:** Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

**Amenaza:** Es la causa potencial de una situación de incidente y no deseada por la organización

**Causa:** Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

**Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**Consecuencia:** Resultado de un evento que afecta los objetivos.





**Criterios del riesgo:** Términos de referencia frente a los cuales la importancia de un riesgo se evalúa.

**Control:** Medida que modifica el riesgo.

**Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

**Evaluación de riesgos:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

**Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

**Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

**Evitación del riesgo:** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

**Factores de Riesgo:** Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

**Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

**Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

**Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

**Integridad:** Propiedad de la información relativa a su exactitud y completitud.

**Impacto.** Cambio adverso en el nivel de los objetivos del negocio logrados.

**Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

**Matriz de riesgos:** Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.





**Monitoreo:** Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.

**Propietario del riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

**Proceso:** Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

**Riesgo Inherente:** Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

**Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

**Riesgo:** Efecto de la incertidumbre sobre los objetivos.

**Riesgo en la seguridad de la información:** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

**Reducción del riesgo:** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

**Retención del riesgo:** Aceptación de la pérdida o ganancia proveniente de un riesgo particular

**Seguimiento:** Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

**Tratamiento del Riesgo:** Proceso para modificar el riesgo” (Icontec Internacional, 2011).

**Valoración del Riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

**Vulnerabilidad:** Es aquella debilidad de un activo o grupo de activos de información

**Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

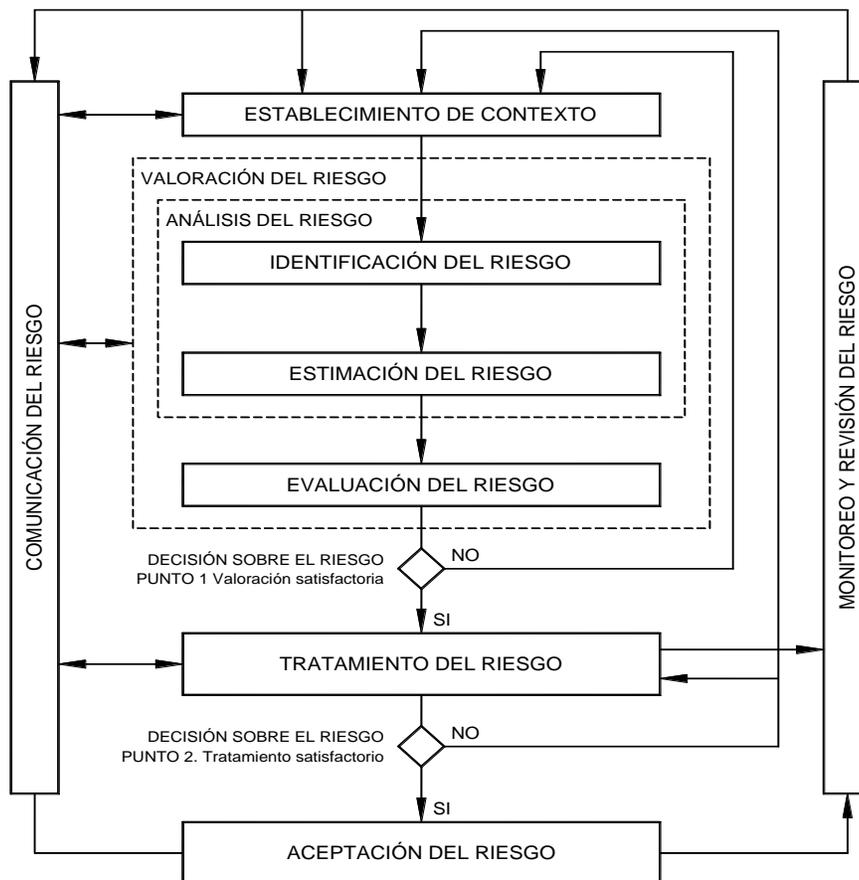
**SGSI:** Sistema de Gestión de Seguridad de la Información.





## 8 VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD DE LA INFORMACION

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñado basado tanto en la norma **ISO/IEC 31000** como en la **ISO 27005** como base para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:



La gestión de riesgos de seguridad de la información deberá ser iterativa para las actividades de valoración de riesgos y/o tratamiento de estos.





## 8.1 ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de TRANSCARIBE S.A. y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos de la entidad. En el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr mantener niveles de riesgos aceptables para la esta.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

### 8.1.1 Criterios de evaluación del riesgo de seguridad de la información:

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información en TRANSCARIBE S.A.
- La criticidad de los activos de información involucrados (Servidores, Motores de Base de Datos, Equipo de computas y demás Sistemas de Información).
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de TRANSCARIBE S.A.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de TRANSCARIBE S.A.

### 8.1.2 Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados (Servidores, Motores de Base de Datos, Equipo de computas y demás Sistemas de Información).
- Huecos en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)





- Operaciones deterioradas (afectación a clientes internos o externos)
- Pérdida del negocio y del valor financiero de este.
- Alteración de planes o fechas límites.
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

Los niveles de clasificación y reglas y sus impactos establecidos por TRANSCARIBE S.A. se podrán tomar del documento – *De los procedimientos de políticas de seguridad informática de Transcaribe S.A.*

### 8.1.3 Criterios de Aceptación

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de la Entidad y de las partes interesadas, por tanto, las escalas de aceptación de riesgos de seguridad de información se podrán tomar del documento La matriz de riesgos institucional de la entidad y del mapa de riesgos de Transcaribe S.A.

## 8.2 VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Entidad, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo
  - Identificación de los riesgos
  - Estimación del riesgo
- Evaluación del riesgo

### 8.2.1 Identificación del riesgo

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación.

Los **activos de información** se clasifican en dos tipos:





## 1. Primarios:

- a. **Procesos o subprocesos y actividades del Negocio:** procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.
- b. **Información:** información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.
- c. **Actividades y procesos de negocio:** que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

## 2. De Soporte

- b. **Hardware:** Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
- c. **Software:** Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
- d. **Redes:** Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
- e. **Personal:** Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- f. **Sitio:** Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)





g. **Estructura organizativa:** responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las **amenazas** que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de TRANSCARIBE S.A.

Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios.
- Inspección física.
- Uso de las herramientas para el escaneo automatizado de los sistema de información y las redes de datos locales.

Para cada una de las **amenazas** analizaremos las **vulnerabilidades** (debilidades) que podrían ser explotadas.

Finalmente se identificarán las **consecuencias**, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

### 8.2.2 Estimación del riesgo

La estimación del riesgo busca establecer la *probabilidad* de ocurrencia de los riesgos y el *impacto* de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad:** La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.





- **Impacto:** Hace referencia a las consecuencias que puede ocasionar a la entidad la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

**Formulario para el registro de la estimación de los riesgos de seguridad de la información:**

Para realizar el análisis de riesgo de un proceso, se creará un formato para ellos el cual las personas del equipo deberán calificar el impacto y la probabilidad de cada uno de los riesgos identificados de acuerdo con los niveles para la estimación de los riesgos que deberán ser tomados del documento.

PROBABILIDAD			
Concepto	Escala	Descripción	Frecuencia
Raro	1	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
Improbable	2	Es muy poco factible que el evento se presente.	Al menos de 1 vez en Los últimos 5 años.
Posible	3	El evento podría ocurrir en algún momento.	Al menos de 1 vez en Los últimos 2 años.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos de 1 vez en El último año.
Casi seguro	5	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

**Adaptado del MAPA DE RIESGO TRANSCARIBE S.A. Año 2018.**

IMPACTO		
Concepto	Escala	Descripción
Insignificante	Menor a 3	La materialización del riesgo <b>puede ser controlado</b> por los participantes del proceso, y <b>no afecta los objetivos del proceso</b> .





Menor	Entre 3 y 7	La materialización del riesgo ocasiona <b>pequeñas demoras</b> en el cumplimiento de las actividades del proceso, y <b>no afecta significativamente el cumplimiento de los objetivos</b> de la Agencia. Tiene un impacto bajo en los procesos de otras áreas de la Entidad.
Moderado	Entre 8 y 11	La materialización del riesgo <b>demora el cumplimiento de los objetivos del proceso</b> , y tiene un <b>impacto moderado en los procesos de otras áreas</b> de la Agencia. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Mayor	Entre 12 y 13	La materialización del riesgo <b>retrasa el cumplimiento de los objetivos de TRANSCARIBE S.A.</b> y tiene un <b>impacto significativo en la imagen pública</b> de la Entidad y/o de la Alcaldía de Cartagena. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras
Catastrófico	Mayor o igual a 14	La materialización del riesgo <b>imposibilita el cumplimiento de los objetivos de TRANSCARIBE S.A.</b> , tiene un <b>impacto catastrófico en la imagen pública de la Entidad y/o de la Alcaldía de Cartagena</b> . Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras.

**Adaptado para el MAPA DE RIESGO TRANSCARIBE S.A. Años 2013 - 2018.**

### **8.2.3 Determinación del riesgo inherente y residual**

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario sin controles) y ver el grado de exposición al riesgo que tiene la entidad. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.





MATRIZ DE CALIFICACIÓN DE LOS RIESGOS

PROBABILIDAD		IMPACTO / CONSECUENCIAS					
			1	2	3	4	5
			Insignificante	Menor	Moderado	Mayor	Catastrófico
1	1	Raro	B	B	M	A	A
2	2	Improbable	B	B	M	A	E
3	3	Posible	B	M	A	E	E
4	4	Probable	M	A	A	E	E
5	5	Casi seguro	A	A	E	E	E
<b>ACCION</b>							
B	ZONA DE RIESGO	BAJO	Asumir el riesgo				
M	ZONA DE RIESGO	MODERADO	Asumir, reducir el riesgo				
A	ZONA DE RIESGO	ALTO	Reducir, evitar, compartir o transferir el riesgo				
E	ZONA DE RIESGO	EXTREMO	Evitar, reducir, compartir o transferir el riesgo				

**Esquema general de Matriz de Riesgo Institucional.**

Código	Nombre	Categoría	Procesos	Causas	Efectos
TC01	No aplicación de la normatividad vigente para la infraestructura de tecnología de la entidad	Riesgos de Proceso	Tecnología de la Información	Desconocimiento de las normas legales vigentes.	Demandas a la institución o sanciones por no aplicación de la norma Infraestructura de tecnología de la información desactualizada.
TC02	2. El plan Estratégico de tecnología de Información no se enmarca dentro del Plan Estratégico de la entidad.	Riesgos de Proceso	Tecnología de la Información	Falta de análisis del contexto institucional. Desconocimiento profundo del Plan Estratégico. El Plan Estratégico no se haya realizado con participación de todas las dependencias de la entidad. Falta de compromiso de la alta dirección en la determinación de estrategias efectivas.	Debilitamiento de los ejes misionales de la entidad. Disminución de la productividad y competitividad. Obsolescencia tecnológica. Poca adaptación a los cambios del entorno. Desarrollos en la infraestructura de tecnología de información que no responden a la estrategia de la entidad.





TC03	3. Interrupción en la prestación de los servicios de TIC	Riesgos de Proceso	Tecnología de la Información	Fallas físicas y/o lógicas en la infraestructura de TI. Obsolescencia de la infraestructura tecnológica (Hardware y Sistemas de información). Falta de monitoreo periódico sobre la operación de la infraestructura de tecnología de información.. Falta de oportunidad en la gestión de contratación. Falta de mantenimiento preventivo y/o correctivo de los equipos y software de la infraestructura de tecnología de información y de telecomunicaciones.	Afectación de los procesos institucionales. No disponibilidad de la información.
TC04	4. Recursos insuficientes para atender la demanda de servicios de TIC.	Riesgos de Proceso	Tecnología de la Información	Recursos financieros y presupuestales limitados. Tramites de apoyo complejos. Crecimiento de la demanda de servicios de la entidad. Obsolescencia de la tecnología. Cambios inesperados en los planes de trabajo de las dependencias.	Deterioro de la imagen de la dependencia y la Institución Afectación en la ejecución de los procesos institucionales





TC05	Pérdida, alteración o inconsistencia de los datos.	Riesgos de Proceso	Tecnología de la Información	Insuficientes sistemas de protección y/o seguridad física y lógica de la infraestructura de TIC.. Falta de mantenimiento preventivo y/o correctivo de los equipos y software de la infraestructura de TIC.. No aplicación correcta del procedimiento para la administración de las cuentas de usuarios. No aplicación correcta del procedimiento para la generación de respaldos, ni para la restauración.. Falta de un sistema integrado. Desastres naturales. Impericias por parte de los usuarios. Ataques externos.	Afectación en la continuidad de la operación Reprocesos Demandas legales por incumplimiento de compromisos de la Institución internos y externos. Deterioro de la imagen institucional. No disponibilidad de la infraestructura de tecnología de información y de telecomunicaciones. Pérdidas económicas. Retardo en los procesos Institucionales.
TC06	Manipulación de información a favor de terceros o particulares.	Riesgos de Corrupción	Tecnología de la Información	Falta de distribución de responsabilidades. Accesos sin control a bases de datos y aplicaciones. Ingeniería social.	Pérdida de imagen y credibilidad del proceso Procesos disciplinarios Demandas a la institución o sanciones.
TC07	Soborno (Cohecho)	Riesgos de Corrupción	Tecnología de la Información	Toma de decisiones de contratación de bienes o servicios informáticos a conveniencia personal. Concentración de información de determinadas actividades o procesos en una persona.	Adquisición de mal servicio que no garantice el cumplimiento de los objetivos Investigaciones disciplinarias, sanciones
TC08	Tráfico de influencias (amiguismo, persona influyente)	Riesgos de Corrupción	Tecnología de la Información	Concentración de autoridad de determinadas actividades o procesos en una persona.. Deficiencias en procesos y procedimientos. Falta de ética en los funcionarios.	Pérdida de imagen y credibilidad del proceso Procesos disciplinarios

## 8.2.4 Evaluación de los riesgos





Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto a la Alta Gerencia y demás dependencias que conforman la entidad.

### 8.3 TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

COSTO - BENEFICIO	OPCION DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	<b>Evitar</b> el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	<b>Transferir o compartir</b> el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	<b>Reducir o Mitigar</b> el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	<b>Retener o aceptar</b> el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que





permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

**Nota:** Será conveniente que para la selección de los controles se consideren posibles restricciones o limitantes que impidan su elección tales como: restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, uso, de personal o las restricciones para la integración de controles nuevos y existentes.

#### **8.4 MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Entidad por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte: (a) nuevos activos o modificaciones en el valor de los activos, (b) nuevas amenazas, (c) cambios o aparición de nuevas vulnerabilidades, (d) aumento de las consecuencias o impactos, (e) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

#### **8.5 CRONOGRAMA VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION**

La Entidad definirá y mantendrá un cronograma de actividades para la realización de la valoración de los riesgos de seguridad de la información en los procesos de la organización, basado con su criticidad y su valor para el cumplimiento de los objetivos misionales de Sistema Integrado de Transporte Masivo de Cartagena de Indias TRANSCARIBE S.A.

