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

INSTITUTO DEPARTAMENTAL DE TRÁNSITO DEL CESAR – IDTRACESAR

VIGENCIA 2024

TABLA DE CONTENIDO

INTRODUCCIÓN

En un mundo cada vez más interconectado y digitalizado, la seguridad de la información se convierte en un pilar fundamental para cualquier organización, especialmente aquellas encargadas de gestionar datos sensibles y críticos para la sociedad, como el Instituto Departamental de Tránsito del Cesar (IDTRACESAR). En este contexto, la adopción de un enfoque proactivo y sistemático para la gestión de riesgos de información se vuelve imperativa.

El presente Plan de Tratamiento de Riesgos de Información para el IDTRACESAR tiene como objetivo principal salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información gestionados por la institución. A través de un proceso riguroso de evaluación, análisis y tratamiento de riesgos, se busca identificar las amenazas potenciales que podrían afectar la operatividad y la reputación del IDTRACESAR, así como implementar medidas preventivas y correctivas efectivas para mitigar dichos riesgos.

Este plan se fundamenta en estándares reconocidos internacionalmente, incluyendo las normativas ISO 27001 y ISO 31000, que proporcionan directrices claras y mejores prácticas en materia de seguridad de la información y gestión de riesgos. Al adoptar un enfoque basado en estos marcos de referencia, el IDTRACESAR demuestra su compromiso con la excelencia operativa y la protección de los intereses de sus usuarios.

A lo largo de este documento, se delinean las etapas clave del proceso de tratamiento de riesgos, desde la identificación y evaluación inicial hasta la implementación y revisión continua de controles de seguridad. Se enfatiza la importancia de la colaboración interdepartamental, la capacitación del personal y la adaptación constante a un entorno tecnológico en evolución como pilares fundamentales para el éxito de la estrategia de seguridad de la información del IDTRACESAR.

Este plan no solo constituye un marco estructurado para la gestión de riesgos de información, sino también un compromiso organizacional con la transparencia, la responsabilidad y la protección de los datos confiados a la institución. En última instancia, su implementación efectiva fortalecerá la resiliencia del IDTRACESAR frente a las amenazas cibernéticas y garantizará la continuidad de sus operaciones en beneficio de la comunidad a la que sirve.

1. OBJETIVO

El objetivo general del Plan de Tratamiento de Riesgos de Información para el Instituto Departamental de Tránsito del Cesar (IDTRACESAR) es establecer un marco integral y efectivo para la identificación, evaluación, tratamiento y monitoreo de los riesgos asociados a la seguridad de la información. El plan busca salvaguardar los activos de información del IDTRACESAR, garantizando su confidencialidad, integridad y disponibilidad, así como fortalecer la resiliencia de la institución frente a las amenazas cibernéticas y operativas.

A través de la implementación de este plan, el IDTRACESAR aspira a:

Identificar y comprender las amenazas y vulnerabilidades que podrían comprometer la seguridad de la información gestionada por la institución.

Evaluar de manera sistemática y rigurosa la probabilidad e impacto de los riesgos identificados, priorizando aquellos que representan una mayor amenaza para los objetivos y operaciones del IDTRACESAR.

Implementar medidas de control y tratamiento adecuadas para mitigar, transferir, aceptar o evitar los riesgos identificados, asegurando una gestión efectiva y proporcional a la naturaleza y magnitud de cada riesgo.

Establecer un sistema de monitoreo continuo y revisión periódica de los controles de seguridad implementados, con el fin de detectar y responder de manera oportuna a cambios en el entorno de riesgo y nuevas amenazas emergentes.

Promover una cultura organizacional de seguridad de la información, fomentando la concientización y capacitación del personal, así como la colaboración y coordinación interdepartamental en la gestión de riesgos.

Mediante la consecución de estos objetivos, el Plan de Tratamiento de Riesgos de Información para IDTRACESAR contribuirá a fortalecer la confianza de los usuarios y la sociedad en general en la capacidad del Instituto para proteger y preservar la integridad y confidencialidad de la información bajo su custodia, garantizando así la prestación eficiente y segura de sus servicios y funciones.

2. ALCANCE

El alcance del Plan de Tratamiento de Riesgos de Información para el Instituto Departamental de Tránsito del Cesar (IDTRACESAR) abarca todos los aspectos relacionados con la gestión de riesgos de seguridad de la información dentro de la institución. Este plan incluye:

- **Identificación de Activos de Información:** El plan considera la identificación de todos los activos de información críticos para el funcionamiento del IDTRACESAR, incluyendo datos de conductores, vehículos, documentos legales, sistemas de información y cualquier otro recurso de información relevante.
- **Evaluación de Riesgos:** Se realizará una evaluación exhaustiva de las amenazas y vulnerabilidades que podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información del IDTRACESAR. Esta evaluación se llevará a cabo utilizando metodologías reconocidas y estándares internacionales, como ISO 27001 y ISO 31000.
- **Análisis de Riesgos:** Se analizará la probabilidad de ocurrencia y el impacto potencial de los riesgos identificados en la operatividad y reputación del IDTRACESAR. Se asignarán niveles de riesgo a cada amenaza para priorizar la asignación de recursos y la implementación de controles adecuados.
- **Tratamiento de Riesgos:** El plan define las estrategias y medidas de tratamiento de riesgos para mitigar, transferir, aceptar o evitar las amenazas identificadas. Se implementarán controles técnicos, administrativos y organizativos según sea necesario para reducir la exposición al riesgo y fortalecer la seguridad de la información.
- **Implementación de Controles:** Se establecerán procedimientos claros y prácticos para la implementación y gestión de controles de seguridad de la información en toda la organización. Esto incluye la actualización de políticas, la configuración de sistemas de seguridad, la capacitación del personal y la supervisión continua de los controles implementados.
- **Monitoreo y Revisión:** Se llevará a cabo un monitoreo continuo de la eficacia de los controles de seguridad implementados, mediante auditorías periódicas, análisis de incidentes de seguridad y revisiones de cumplimiento con los estándares y regulaciones aplicables.
- Plan de Contingencia: Se desarrollará un plan de contingencia y recuperación de desastres para garantizar la disponibilidad y continuidad de las operaciones del IDTRACESAR en caso de incidentes de seguridad o interrupciones del servicio.

El alcance del Plan de Tratamiento de Riesgos de Información para IDTRACESAR se extiende a todos los procesos que manejan información dentro de la institución, con el objetivo de garantizar un enfoque integral y coherente en la gestión de riesgos de seguridad de la información.

3. TÉRMINOS Y DEFINICIONES

Activos de Información: Son todos los recursos de información, tanto digitales como físicos, que son valiosos para la organización. Esto incluye datos de clientes, registros financieros, propiedad intelectual, sistemas de información, documentos impresos, entre otros.

Amenaza: Es cualquier evento o circunstancia que tiene el potencial de causar daño o comprometer la seguridad de los activos de información. Las amenazas pueden ser naturales (como desastres naturales), humanas (como errores humanos o ataques de hackers) o tecnológicas (como fallas de hardware o software).

Vulnerabilidad: Es una debilidad o deficiencia en un sistema o proceso que podría ser explotada por una amenaza para comprometer la seguridad de la información. Las vulnerabilidades pueden ser técnicas (como fallos de seguridad en software) o humanas (como la falta de capacitación del personal).

Riesgo: Es la combinación de la probabilidad de ocurrencia de una amenaza y el impacto que tendría esa amenaza si se materializara. Los riesgos se evalúan para determinar su nivel de riesgo, que puede ser alto, medio o bajo, y para priorizar la asignación de recursos para su tratamiento.

Tratamiento de Riesgos: Es el proceso de seleccionar y aplicar medidas de control para mitigar, transferir, aceptar o evitar los riesgos identificados. El tratamiento de riesgos busca reducir la exposición al riesgo a un nivel aceptable para la organización.

Controles de Seguridad de la Información: Son medidas o salvaguardas diseñadas para proteger los activos de información contra amenazas y vulnerabilidades. Los controles pueden ser técnicos (como firewalls o encriptación), administrativos (como políticas y procedimientos) o físicos (como cerraduras y sistemas de seguridad física).

ISO 27001: Es un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). La ISO 27001 proporciona un marco para la gestión sistemática y efectiva de la seguridad de la información en una organización.

ISO 31000: Es un estándar internacional que proporciona directrices para la gestión de riesgos en organizaciones. La ISO 31000 establece los principios, el marco y el proceso para la gestión de riesgos, ayudando a las organizaciones a identificar, evaluar y tratar los riesgos de manera efectiva.

4. OBJETIVOS ESPECIFICOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. **Identificación exhaustiva de activos de información**:
   - ✓ Identificar todos los activos de información críticos para el funcionamiento del IDTRACESAR, incluyendo datos de conductores, vehículos, documentos legales y sistemas de información.

2. **Evaluación detallada de amenazas y vulnerabilidades:**
   - ✓ Realizar un análisis exhaustivo de las amenazas y vulnerabilidades que podrían afectar la seguridad de la información del IDTRACESAR, considerando factores internos y externos.

3. **Priorización de riesgos según su impacto y probabilidad:**
   - ✓ Clasificar los riesgos identificados según su impacto potencial y la probabilidad de ocurrencia, para priorizar la asignación de recursos y la implementación de controles de seguridad.

4. **Implementación de controles técnicos y administrativos:**
   - ✓ Desplegar controles técnicos como firewalls, sistemas de detección de intrusiones y encriptación de datos para proteger los activos de información del IDTRACESAR.
   - ✓ Establecer controles administrativos como políticas de seguridad de la información, procedimientos de gestión de incidentes y capacitación del personal en seguridad.

5. **Desarrollo de un plan de contingencia y recuperación:**
   - ✓ Elaborar un plan de contingencia y recuperación de desastres que detalle los procedimientos y recursos necesarios para mantener la continuidad de las operaciones del IDTRACESAR en caso de incidentes de seguridad o interrupciones del servicio.

6. **Realización de auditorías y revisiones periódicas:**
   - ✓ Llevar a cabo auditorías de seguridad de la información de forma regular para evaluar la eficacia de los controles implementados y garantizar el cumplimiento de los estándares y regulaciones aplicables.
   - ✓ Realizar revisiones periódicas del plan de tratamiento de riesgos de información para asegurar su relevancia y efectividad en un entorno en constante evolución.

7. **Fomento de la conciencia y cultura de seguridad:**
   - ✓ Promover la conciencia y la cultura de seguridad de la información entre los empleados del IDTRACESAR mediante programas de capacitación, sesiones informativas y campañas de sensibilización.
   - ✓ Incentivar la colaboración y comunicación interdepartamental en materia de seguridad de la información para garantizar una respuesta efectiva ante posibles incidentes y amenazas.

5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI

EL SGSI es aplicable a los activos de información de todos los procesos del Instituto Departamental de Tránsito del Cesar – IDTRACESAR, verificándolo y aplicándolo a las sedes, comprende las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con la declaración de aplicabilidad avalada por el Comité de Seguridad de la Información y el Comité Institucional de Gestión y Desempeño.

6. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité institucional de gestión y desempeño asumirá las funciones del Comité Seguridad de la Información que es creado en el Instituto Departamental de Tránsito del Cesar – IDTRACESAR, mediante acto administrativo, el cual tiene dentro de sus funciones: definir y aprobar las directrices, políticas y mecanismos de control y seguimiento de la Información de la Entidad de conformidad con el marco normativo vigente.

Está conformado por:

- ✓ El Profesional especializado Administrativo y Financiero quien lo presidirá y los siguientes funcionarios asistirán como invitados, con voz, pero sin voto:

- ✓ El jefe responsable de Control Interno o quien haga sus veces en el Instituto Departamental de Tránsito del Cesar – IDTRACESAR.

Las Funciones del Comité de Seguridad de la Información son:

- ✓ Promover la mejora continua del Sistema de Gestión de Seguridad de la Información SGSI del Instituto Departamental de Tránsito del Cesar – IDTRACESAR.
- ✓ Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SCSI del Instituto Departamental de Tránsito del Cesar – IDTRACESAR.
- ✓ Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información del Instituto Departamental de Tránsito del Cesar – IDTRACESAR.
- ✓ Adoptar las medidas y acciones a que haya lugar, de conformidad con los resultados de los diagnósticos del estado de la seguridad de la información del Instituto Departamental de Tránsito del Cesar – IDTRACESAR, con el fin de tomar y establecer las medidas necesarias.

- ✓ Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual que puedan generar pérdidas patrimoniales o afectar los recursos de información de la entidad.
- ✓ Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información.
- ✓ Revisar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.
- ✓ Recomendar la investigación de los incidentes de seguridad de la información ante las instancias necesarias cuando haya lugar a ello.
- ✓ Evaluar los planes de acción para mitigar y/o eliminar riesgos en seguridad de la información.
- ✓ Alinear sus acciones y decisiones a la normatividad vigente en materia de tecnologías y seguridad de la información.
- ✓ Las demás funciones inherentes a la naturaleza del Comité.

Funciones del secretario técnico son:

- ✓ Convocar a los integrantes del Comité a las sesiones ordinarias y extraordinarias.
- ✓ Elaborar las actas de reunión del Comité oportunamente.
- ✓ Enviar la agenda a los miembros del Comité oportunamente.
- ✓ Llevar y custodiar el archivo de las actas y demás documentos soporte del Comité.
- ✓ Verificar el quórum al inicio de las sesiones.
- ✓ Recibir y preparar la respuesta a los documentos que sean de competencia del Comité.
- ✓ Firmar las actas que hayan sido aprobadas.
- ✓ Realizar seguimiento a los compromisos y tareas pendientes del Comité.
- ✓ Las demás que le sean asignadas por el Comité.

7. ETAPAS PARA LA GESTIÓN DEL RIESGO INFORMATICO

Visión general para administración del riesgo de seguridad de la información

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

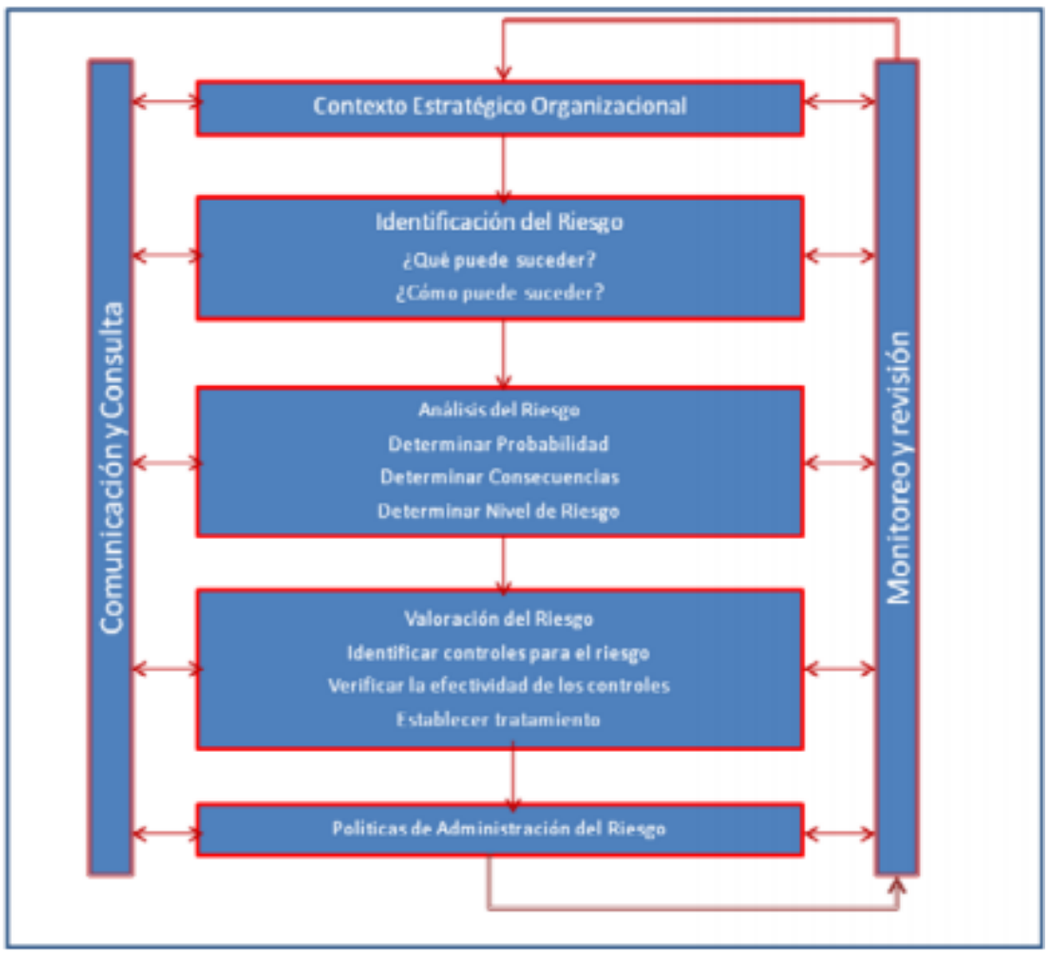

Imagen 1: Proceso para la administración del riesgo
Fuente: Tomado de la Cartilla de Administración de Riesgos del DAFP

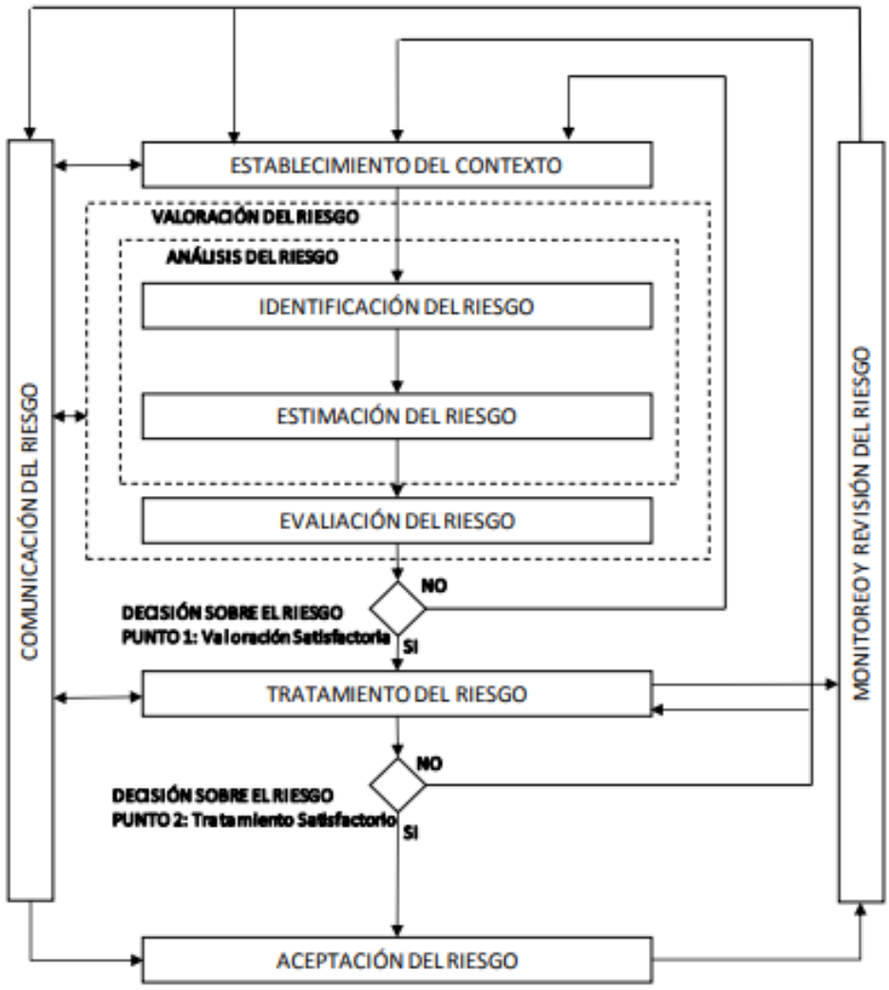

Imagen 2: Proceso para la administración del riesgo en seguridad de la información
Fuente: Tomado de la NTC-ISO/IEC 27005

El proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración.

El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riesgo con un contexto revisado (por ejemplo, los criterios de evaluación del riesgo los criterios para aceptar el riesgo o los criterios de impacto).

La eficacia del tratamiento de tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual en esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con

cambios en los parámetros del contexto (por ejemplo, criterios para la valoración del riesgo, de aceptación o de impacto del riesgo)

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la entidad. Esto es especialmente importante en una situación en la que la implementación de los controles se omite o se pospone, por ejemplo, por costos.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDAD DE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Tabla 1: Etapas de la Gestión del Riesgo a lo Largo del MSPI
Fuente: Cartilla Seguridad y Privacidad de la Información MINTIC.

Contexto estratégico

El contexto estratégico se tiene en cuenta en el proyecto del MSPI desde el inicio, sobre todo en el momento de definir el objetivo y el alcance del proyecto, así como la política de Seguridad de la Entidad, esto debido a que es necesario tener claro el entorno en el cual se desarrollará el proyecto, precisando cuál será el contexto en el que se desenvolverá, qué procesos involucrará, cual es el flujo de dicho o dichos procesos, y de ésta forma identificar sus objetivos y finalmente, de allí obtener los riesgos de Seguridad asociados.

De igual forma el personal asignado para el desarrollo del MSPI tiene como ventaja, el contexto estratégico avanzado para los modelos de Gestión establecidos en la Entidad, analizando los flujos de procesos ya identificados, para aportar su visión desde el MSPI. Sin embargo cabe mencionar que la guía señala las siguientes estrategias a través de las cuales se puede hacer ese levantamiento del contexto Estratégico

- ✓ Inventario de Eventos
- ✓ Talleres de Trabajo
- ✓ Análisis de Flujo de Procesos

Criterios básicos

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques, pero debe ser adecuado y que contenga criterios como: criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo:

Criterios de evaluación del riesgo:

Desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización teniendo en cuenta los siguientes aspectos

- ✓ El valor estratégico del proceso de información para la entidad
- ✓ La criticidad de los activos de información involucrados en el proceso
- ✓ Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- ✓ La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- ✓ Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

De igual modo, los criterios de evaluación de impacto del riesgo y se pueden utilizar para especificar las prioridades del tratamiento del riesgo.

Criterios de Impacto:

Desarrollo de los criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos: Nivel de clasificación de los activos de información de los procesos:

- ✓ Brechas en la seguridad de la información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- ✓ Operaciones deterioradas
- ✓ Perdida del negocio y del valor financiero
- ✓ Alteración de planes y fechas limites
- ✓ Daños para la reputación
- ✓ Incumplimiento de los requisitos legales

Criterios de Aceptación del Riesgo

Es recomendable desarrollar y especificar criterios de aceptación del riesgo; estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas

La organización debería definir sus propias escalas para los niveles de aceptación del riesgo. Durante el desarrollo, se deberían considerar los siguientes aspectos:

- ✓ Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas
- ✓ Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado
- ✓ Los diferentes criterios de aceptación del riesgo pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes podrían no ser aceptados aunque se puede permitir la aceptación de riesgos altos si esto se especifica como un requisito contractual
- ✓ Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Alcance y límites para la gestión de riesgos en Seguridad de la información

Es importante que la entidad defina el alcance y los límites y el alcance para de esta manera garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo.

.

Al definir el alcance y los límites la entidad debería considerar la siguiente Información

- ✓ Objetivos estratégicos de, políticas y estrategias de la organización
- ✓ Procesos de la entidad
- ✓ Funciones y estructura de la entidad
- ✓ Los requisitos legales, reglamentarios y contractuales aplicables a la organización
- ✓ La política de seguridad de la información de la organización
- ✓ El enfoque global de la organización hacia la gestión del riesgo
- ✓ Activos de información
- ✓ Ubicación de la organización y sus características geográficas
- ✓ Restricciones que afectan a la organización

- ✓ Expectativas de las partes interesadas
- ✓ Entorno sociocultural
- ✓ Interfaces (Ej. Intercambio de información con otras entidades)

Identificación de riesgos

De acuerdo con lo planteado en la guía, la identificación del riesgo se hace con base en causas identificadas para los procesos, dichas causas pueden ser internas o externas, según lo que haya identificado la Entidad a través del Contexto estratégico.

Es importante establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible, revisar los procesos según la clasificación del MECI y del modelo de gestión, con este punto se revisa la pertinencia del alcance planteado para el MSPI.

Análisis de Riesgos

Para la entidad es muy importante documentar y especificar cada una de las etapas surtidas para el proceso de Gestión de Riesgos, de allí la Entidad tendrá su propia guía para poder replicar este mismo procedimiento para cualquier etapa que sea necesaria, ya sea para el momento en la que la Entidad decida extender el alcance de la aplicación del MSPI, o para la etapa de revisión de los controles, en la cual la entidad sólo debería poder aplicar la misma metodología simplemente teniendo como base el trabajo ya adelantado en las primeras etapas del MSPI.

A continuación, se presentan varias etapas propuestas para la generación del análisis de riesgos de la Entidad, basadas la norma ISO27005

Identificación del Riesgo

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas deberían recolectar datos de entrada para esta actividad.

Identificación de Los Activos

Un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. Para realizar esta identificación es necesario revisar la guía de gestión de activos adjunta al MSPI.

Identificación de las Amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas.

Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas)

Identificación de Controles Existentes

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo la duplicidad de controles, además de esto mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.

Los controles que se planifican para implementar de acuerdo con los planes de implementación de tratamiento de riesgo se deberían considerar en la misma forma que aquellos que ya están implementados.

Identificación de las Vulnerabilidades

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes.

Se pueden identificar vulnerabilidades en las siguientes áreas:

- ✓ Organización.
- ✓ Procesos y procedimientos.
- ✓ Rutinas de gestión.
- ✓ Personal
- ✓ Ambiente físico
- ✓ Configuración del sistema de información.
- ✓ Hardware, software y equipos de comunicaciones.
- ✓ Dependencia de partes externas.

Identificación de las Consecuencias

Para la identificación de las consecuencias es necesario tener:

- ✓ Lista de activos de información y su relación con cada proceso de la entidad.

- ✓ Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

Evaluación de Riesgo

"Por Probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

Por Impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo".

Esta se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada "Matriz de Calificación, Evaluación y respuesta a los Riesgos", con la cual la guía presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo,

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Imagen 3: Matriz de Calificación, Evaluación y respuesta a los Riesgos
Fuente: Guía de Riesgos DAFP

Valoración de controles para el tratamiento de Riesgos

Esta etapa se debe tener en cuenta la evaluación realizada e inicia con la evaluación de los controles existentes en la Entidad, estableciendo su descripción, su formalidad (¿se aplican?, ¿están documentados?) y su efectividad (calificación en la matriz de riesgos) para luego ser comparados con los criterios definidos en las etapas de identificación y análisis de riesgos, de esta forma se busca escoger los controles que permitan disminuir los valores de

exposición del riesgo, y luego se debe hacer un recalculo comparando nuevamente con los criterios establecidos y así buscar un nivel aceptable del riesgo en cada proceso para los temas de Seguridad; en la definición de éstos nuevos controles, se utiliza la “estructura de controles” que presenta la guía de controles del MSPI, para hacer un trabajo documentado y Ordenado.

Plan de implementación

Luego de elegir cuáles controles son los más adecuados para tener un nivel de riesgo aceptable para el o los procesos incluidos en el alcance del MSPI, se debe diseñar un plan de tratamiento de riesgos incluyendo los de Seguridad de la información, en el cual se defina qué tratamiento se dará a los riesgos de acuerdo con las opciones entregadas, qué acciones se implementarán, quienes serán los responsables de esta implementación. Este plan debe plantear claramente cada acción, etapa y procedimientos que se ejecutarán para poder ser monitoreado y lograr el seguimiento a la ejecución de este.

Teniendo en cuenta que se debe tener la aprobación del plan de tratamiento de riesgos por parte de los dueños de cada riesgo, que en este caso y como se ha venido planteando, corresponderían a los dueños de los procesos, es indispensable que la aceptación del plan de tratamiento de riesgos y del riesgo residual se haga en el comité interdisciplinario designado para estos temas en la Entidad y así se logra dar la participación de las diferentes áreas incluidas en el proceso y finalmente de la Dirección.

8. EQUIPO DE RESPUESTA INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Establézcase como órgano consultivo del Comité, el Equipo de Respuesta a incidentes de Seguridad de la Información conformado por el Profesional Especializado Administrativo y Financiero y los demás profesionales de la entidad, quienes tendrán a su cargo las siguientes funciones:

- ✓ Emitir conceptos sobre los aspectos necesarios para garantizar la seguridad de la Información.
- ✓ Proponer los temas, la información y los indicadores que el Comité de Seguridad de la Información determine que habrán de considerarse de interés de la Entidad.
- ✓ Asesorar y proponer acciones para orientar y mejorar la Seguridad de la Información del Instituto Departamental de Tránsito del Cesar – IDTRACESAR.

- ✓ Coordinar con el Área responsable de las Tecnologías de la Información y Sistemas, la definición de proyectos y medidas de seguridad de la Información.
- ✓ Realizar el registro detallado e informar oportunamente la ocurrencia de eventos e incidentes de seguridad de la información, con el fin que el área de Tecnologías y Sistemas de información tome las acciones correspondientes.
- ✓ Establecer contacto con diferentes organismos especializados en materia de seguridad de la información, de acuerdo con el marco de cooperación nacional definido en el CONPES 3854 de 2016.

9. PLAN DE TRABAJO Y CRONOGAMA DE ACTIVIDADES

Actividad No.	Acción o Actividad	Producto	Responsable	Fecha de inicio	Fecha Fin
1	Gestionar y/o actualizar los activos de información en cada dependencia y/o proceso (si aplica)	Informe Tecnico	Profesional de gestión de TIC	01/02/2024	30/12/2024
2	Gestionar los Capacitaciones Seguridad TI	Capacitaciones	Profesional de gestión de TIC	01/02/2024	30/12/2024
3	Socializar la Guía de gestión de incidentes de seguridad de la información	Socialización realizada	Profesional de gestión de TIC	01/02/2024	30/12/2024
4	Elaborar plan de concientización, formación, socialización en seguridad de la información y apropiación del SGSI.	Documento Administrativo	Profesional de gestión de TIC	01/02/2024	30/12/2024
5	Implementar las estrategias y campañas incluidas en el plan de concientización, formación, socialización en seguridad de la información y apropiación del SGSI.	Estrategias y campañas	Profesional de gestión de TIC	01/02/2024	30/12/2024
6	Realizar pruebas de vulnerabilidades y pen test de acuerdo con el alcance y la	Documento Administrativo	Profesional de gestión de TIC	15/02/2024	30/12/2024

	metodología establecida				
7	Elaborar Plan de copias de respaldo de la información para la vigencia 2023	Plan de copias de respaldo de la información	Profesional de gestión de TIC	15/02/2024	30/12/2024
8	Definir Mantenimiento preventivo y correctivo periódicos de Hardware y software	Plan de mantenimiento de equipos ejecutado	Profesional de gestión de TIC	15/02/2024	30/12/2024
9	Realizar mantenimiento correctivo y preventivo a la UPS de la red eléctrica regulada de la entidad	Plan de mantenimiento de UPS y redes eléctricas ejecutado	Profesional de gestión de TIC	15/02/2024	30/12/2024
10	Definir un Plan de capacitación, sensibilización y comunicación en seguridad de la información	Plan de capacitación ejecutada	Profesional de gestión de TIC	15/02/2024	30/12/2024

10. MARCO LEGAL

El Plan Estratégico de Tratamiento de Riesgos de Seguridad Digital, aplicado al Instituto Departamental de Tránsito del Cesar – IDTRACESAR. se encuentra directamente relacionado a la normativa nacional colombiana, por tal razón es compromiso de esta entidad seguir detalladamente las pautas que presenta el MINTIC para las entidades del estado.

Se presentan las normas a considerar aplicables con respecto a la elaboración del documento PTRSI y otras regulaciones relevantes del Instituto Departamental de Tránsito del Cesar – IDTRACESAR. en el tema tecnológico.

- ✓ Directiva Presidencial No. 10 de 2002 Programa de renovación de la Administración Pública: hacía un Estado Comunitario.
- ✓ Ley 790 de 2002. Programa de Reforma de la Administración Pública.
- ✓ Conpes 3248 de 2003. Renovación de la Administración Pública.
- ✓ Decreto 3816 de 2003. Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública.
- ✓ Decreto Nacional 1151 del 14 de abril de 2008. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.

- ✓ Ley 1341 2009. Define principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional de Espectro
- ✓ Decreto 235 de 2010. Intercambio de información entre entidades para el cumplimiento de funciones públicas.
- ✓ Decreto 2693 2012. Establece los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011
- ✓ Ley 1551 de 2012. Por la cual se dictan normas para modernizar la organización y el funcionamiento de los municipios.
- ✓ Decreto 2573 del 12 de diciembre 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.
- ✓ 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.
- ✓ Decreto 103 de 2015. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- ✓ Resolución 3564 2015. Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)
- ✓ Decreto 1078 del 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- ✓ Resolución 2405 2016. Adopta el modelo del Sello de Excelencia Gobierno en Línea y se conforma su comité
- ✓ Decreto 728 2016. Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico
- ✓ Decreto 415 de 2016. Por el cual se establece que el director de TI, conocido como Chief Information Officer (CIO) es el encargado de coordinar y alinear la ejecución de los procesos relacionados con tecnología en todas las organizaciones.
- ✓ Decreto 1413 de 2017. Actualiza el Decreto Único Reglamentario del sector de las TIC, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales
- ✓ Decreto 1008 2018. Establece los lineamientos generales de la política de Gobierno Digital y actualizando el Decreto Único Reglamentario del sector de las TIC
- ✓ NTC / ISO 27001:2018. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
- ✓ NTC / ISO 31000 – 2018. Gestión del Riesgo. Principios y directrices.
- ✓ CONPES 3975 2019. Política Nacional Para La Transformación Digital E Inteligencia Artificial
- ✓ Directiva 02 2019. Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones

- ✓ Ley 1955 2019. Simplificación de interacción digital los ciudadanos y el Estado
- ✓ Decreto 2106 del 2109. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Publica Efectiva
- ✓ Decreto 620 mayo 2020. Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
- ✓ Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- ✓ Resolución 2160 de 2020. Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos
- ✓ Conpes 3995 de 2020. Este documento CONPES busca fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.
- ✓ Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5 Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública diciembre de 2020
- ✓ Resolución 2893 de 2020. Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPA, y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado colombiano, y se dictan otras disposiciones
- ✓ Ley 2080 de 2021. Por medio de la cual se reforma el código de procedimiento administrativo y de lo contencioso administrativo -ley 1437 de 2011- y se dictan otras disposiciones en materia de descongestión en los procesos que se tramitan ante la jurisdicción
- ✓ Directiva Presidencial 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- ✓ Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- ✓ Decreto 767 de 2022. 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
- ✓ Resolución 1117 de 2022 Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios

inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital

- ✓ Resolución 746 de 2022. Por el cual se modifica la estructura de la Agencia Nacional de Infraestructura y se determinan las funciones de sus dependencias.
- ✓ Decreto 338 de 2022. Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones
- ✓ Directiva Presidencial 02 de 2022. Reiteración de la política pública en materia de seguridad digital.
- ✓ Resolución 460 de 2022. Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
- ✓ Decreto 088 de 2022. Por el cual se adiciona el Titulo 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
- ✓ Resolución 1951 de 2022. Por la cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales; se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital.

11. REQUISITOS TÉCNICOS

- ✓ Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de Gestión de la Seguridad de la Información.
- ✓ Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información, Seguridad y privacidad como habilitador de la política de Gobierno
- ✓ Norma Técnica Colombiana NTC/ISO 31000:2018 Gestión de riesgo, Directrices

CONTROL DE CAMBIOS

FECHA	RAZÓN DEL CAMBIO	VERSIÓN
30/01/2024	Elaboración del documento	1.0

TABLA DE APROBACIÓN

ELABORADO POR:	REVISADO POR:	APROBADO POR:
EIDER ALCIDES RIVERO MOLINA	DIANA MARGARITA DAZA GONZÁLEZ	DIANA MARGARITA DAZA GONZÁLEZ