INSTITUTO DEPARTAMENTAL DE TRÁNSITO DEL CESAR – IDTRACESAR

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

VIGENCIA 2023

INTRODUCCION

Gestionar eficazmente la seguridad de la información y riesgos de seguridad digital de los sistemas de información de la entidad, así como en los activos que participan en sus procesos y que se encuentran expuestos, permite garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de Seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del Sistema de Gestión de Seguridad de la Información y en concordancia a la normativa aplicable.

El plan de tratamiento de riesgos de seguridad, cuyo objetivo es disponer de la información apropiada para el desarrollo de las funciones de la entidad, a través de la la cual busca gestionar información confiable, integra y oportuna para el desarrollo de las funciones y actividades institucionales.

Así mismo, este plan apoya la implementación de controles y acciones tendientes a la mitigación de los riesgos del proceso de gestión tecnológica, hallazgos de auditorias internas y apoya el cumplimiento del Modelo integrado de planeación y gestión del MINTIC, dentro de su política de gobierno Digital.

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

1. OBJETIVO

Presentar el Plan de Tratamiento para los riesgos de seguridad de la información, identificados en los procesos incluidos en el alcance del SGSI del Instituto Departamental de Tránsito del Cesar – IDTRACESAR.

1.1. Objetivos Específicos

- Identificar los riesgos asociados a los procesos y los activos de información que hacen parte del alcance del SGSI.
- Calcular el nivel de riesgo.
- Establecer el plan de tratamiento de riesgos.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos.

2. MARCO NORMATIVO

Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
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
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices
Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

3. DEFINICIONES

- **Activo**: cualquier elemento que tenga valor para la organización.
- **Análisis del riesgo:** Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- **Causa:** Elemento específico que origina el evento.
- **Contexto externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- **Contexto interno:** Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- **Controles:** Procesos, políticas y/o actividades que pueden modificar el riesgo.
- **Criterios de riesgos:** Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- **Evaluación del Riesgo:** Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
- **Evento:** Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- **Fuente:** Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.

- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Identificación del riesgo:** Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.
- **Riesgo aceptable:** Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento.
- **Riesgo:** Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de sus objetivos.
- **Riesgo de seguridad digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

4. DESARROLLO DEL PLAN

4.1. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto el Instituto Departamental de Tránsito del Cesar – IDTRACESAR. Es recomendable contar con técnicas tradicionales para identificar los riesgos

específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla. El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la Guía para la administración del riesgo y el diseño de controles en entidades públicas V4, emitida por el Departamento Administrativo de la Función Pública.

Ilustración 1. Estructura general de la metodología de riesgos

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

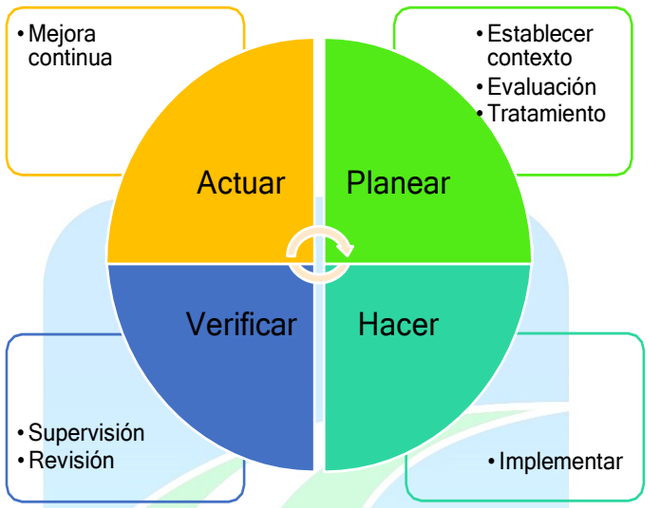

Ilustración 2. Ciclo PHVA y la gestión de riesgos

El proceso de identificación y evaluación de los riesgos de seguridad de la información está compuesto por los siguientes Hitos o actividades:

4.1.1 Programación y Agendamiento de Entrevistas

En esta fase se seleccionan los procesos incluidos en el alcance del SGSI del Instituto Departamental de Tránsito del Cesar – IDTRACESAR y se procede a programar y a agendar a los líderes de las dependencias y grupos internos de trabajo que conforman los procesos, para la identificación de riesgos.

4.1.2 Entrevista con los Líderes

Se entrevista a cada líder de dependencia o grupo, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se consignan en la Matriz de Riesgos.

4.1.3 Identificación y Calificación de Riesgos

En esta fase, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013): Ilustración 2. Ciclo PHVA y la gestión de riesgos El proceso de identificación y

evaluación de los riesgos de seguridad de la información está compuesto por los siguientes Hitos o actividades:

4.1.4 Valoración del Riesgo Residual

En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

4.1.5 Mapas de Calor donde se ubican los Riesgos

Luego se procede a ubicar los riesgos en un mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

4.2 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Una vez ejecutadas las etapas de análisis y valoración de riesgos, y con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones aplicando el apetito de riesgos definido por el Instituto Departamental de Tránsito del Cesar – IDTRACESAR.

Si el riesgo se ubica en una zona no aceptable, cada líder responsable de los riesgos identificados con el apoyo del responsable de sistemas e informática, debe definir e implementar los controles necesarios para llevar el riesgo a un nivel aceptable a través del plan de tratamiento de riesgos.

4.3 SEGUIMIENTO Y CONTROL

El seguimiento y control se realiza de acuerdo a la GUÍA PARA LA ADMINISTRACIÓN DE RIESGO Departamento Administrativo de la Función Pública (DAFP).

5. CRONOGRAMA

Para dar cumplimiento al ciclo de riesgo, el cronograma se establece anualmente, los riesgos de seguridad digital identificados se reflejarán en el Mapa de Riesgos Institucional, donde se establecerán las acciones de control y las fechas para implementar dichos controles, el responsable de sistemas e informática apoyará el proceso de definición de los controles con los líderes de cada uno de los grupos o dependencias.

La implementación se desarrolla en 2 fases, las cuales se definen a continuación:

1. Identificación y Valoración de Riesgos
2. Tratamiento de riesgos

6. RECURSOS

La estimación y asignación de los recursos para el Plan de Tratamiento de Riesgos de Seguridad de la información identificados en la entidad, corresponderá responsable del área administrativa y financiera, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

7. INDICADORES

La medición se realiza con un indicador de gestión que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y externo a través de la implementación y evaluación de controles.

El número de riesgos identificados como no aceptables no debe ser superior al 20% del total de riesgos identificados.

La Oficina responsable de sistemas e Informática asesorará a las demás áreas en el proceso de identificación y valoración de los riesgos de seguridad de información y seguridad digital, los líderes de las áreas solicitarán la inclusión de los mismos en el mapa de riesgos institucional, instrumento en donde se registran los riesgos identificados, su valoración y sus controles, para su seguimiento y control.

La oficina de sistemas e informática apoyará a los responsables de las áreas en la definición de los controles y hará seguimiento a su implementación, con el fin, de evidenciar en el siguiente ciclo la efectividad de los controles implementados y en consecuencia la disminución del riesgo No aceptable.

Así mismo, si se llegan a presentar incidentes de seguridad se validarán los riesgos identificados para determinar si obedece a un riesgo identificado y proceder a valorar, recalificar e implementar nuevos controles.

8. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información se aplica a los procesos del Instituto Departamental de Tránsito del Cesar – IDTRACESAR, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información – SGSI.

9. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. Administrar los eventos de seguridad de la información del Instituto Departamental de Tránsito del Cesar – IDTRACESAR.
2. Fortalecer la seguridad y disponibilidad de la información y plataforma tecnológica acorde con la declaración de aplicabilidad aprobada.
3. Cumplir con los requisitos legales aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.
4. Fomentar una cultura de seguridad de la información en los servidores públicos (funcionarios, contratistas, pasantes, judicantes y personal en comisión del Instituto Departamental de Tránsito del Cesar – IDTRACESAR.
5. Fortalecer el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

10. 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.

11. IDENTIFICACIÓN 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 de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

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, de acuerdo con su misión.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

12. SITUACION NO DESEADA

- Hurto de información o de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, por intromisión.
- Incendio en las instalaciones de la entidad por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Pérdida de información.
- Baja Cobertura de internet.
- Daño de equipos y de información.
- Atrasos en la entrega de información.
- Atrasos en asistencia técnica.
- Fuga de información.
- Manipulación indebida de información.

13. ORIGEN DEL PLAN DE GESTION

Debido al riesgo de pérdida de información es necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad; la información.

13.1 PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

1. Dar soporte al modelo de seguridad de la información al interior de la entidad.
2. Conformidad legal y evidencias de la debida diligencia.
3. Preparación de un plan de respuesta a incidentes.
4. Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.
5. Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

CARLOS ALBERTO VEGA MAESTRE
Director