PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTR

MINISTERIO DE TRANSPORTE

Grupo Tecnología de la Información y las Comunicaciones (TIC)

DICIEMBRE 2019

Elaborado por: Hugo Alejandro Casallas Larrotta
Juan Carlos Valenzuela Buitrago
Revisado por: José Ricardo Acevedo, Coordinador Grupo TIC
Aprobado por: Comité de Gestión y Desempeño Institucional

TABLA DE CONTENIDO

1. OBJETIVO 3
2. ALCANCE 3
3. TERMINO Y DEFINICIONES 3
4. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 4
4.1. ESTADO DE PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 4
4.2. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 4
4.3. RESULTADO DEL PLAN DE TRATAMIENTO DE RIESGOS 5
4.4. MONITOREO Y SEGUIMIENTO DEL PLAN DE TRATAMIENTO DE RIESGOS 5
5. COMUNICACIÓN 6

1. Objetivo

Establecer y detallar el estado del plan de tratamiento de los riesgos de seguridad y privacidad de la información del Ministerio de Transporte de acuerdo con el resultado de valoración y decisión de tratamiento sobre los mismos.

2. Alcance

El presente plan contempla el proceso Grupo Tecnología de la Información y las Comunicaciones TIC, acorde al alcance definido para el Sistema de Gestión de Seguridad y Privacidad de la Información.

3. Termino y Definiciones

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

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

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

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

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

MSPI: Modelo de Seguridad y Privacidad de la Información

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

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

4. Plan de tratamiento de riesgos de seguridad y Privacidad de la Información

El Ministerio de Transporte, con base a su compromiso en la protección de la información, identifica, valora, gestiona y trata los riesgos de seguridad de la información que se puedan presentar en la entidad y que pueden afecten el cumplimiento de la misión y visión del Ministerio de Transporte.

Para lo anterior cuenta con metodología basada en la guía para la gestión de riesgos definida por el DAFP (Departamento Administrativo de la Función Pública) donde se realice una gestión de riesgos unificada de los riesgos de gestión, corrupción y seguridad digital (Seguridad de la Información). Brindando un enfoque preventivo y anticipándose a las posibles vulnerabilidades o eventos que puedan afectar el logro de los objetivos institucionales y a la ciudadanía.

4.1. Estado de plan de tratamiento de riesgo de seguridad y privacidad de la información

El Ministerio de Transporte, realiza su primera gestión de riesgos de seguridad de la información en el tercer cuatrimestre de la vigencia 2019, donde se realiza una identificación de riesgos por activos y se plantea el plan de tratamiento de las vulnerabilidades y amenazas para iniciar su ejecución y con lo anterior a la mitigación de estas.

Teniendo en cuenta que no se había realizado tratamiento a los riesgos de seguridad de la información en vigencias anteriores, en su primera etapa los riesgos se encuentran en un nivel elevado, sin embargo, con base en los tratamientos planteados se espera reducirlos hasta que queden en un nivel residual o aceptable.

4.2. Riesgos de seguridad y privacidad de la información

Para la gestión de riesgos de seguridad de la información del 2019, se identificaron doscientos sesenta y uno (261) activos, estos se asociaron a quince (15) riesgos con origen de ciento ocho (108) vulnerabilidades y ciento ocho (108) amenazas. A continuación se encuentra la distribución de riesgos con los controles actuales:

Descripción	Distribución
Extremo	14
Alto	0
Moderado	1
Bajo	0

Para los quince (15) riesgos identificados, se genero una descripción común de los mismos, conforme a lo anterior se obtienen cinco (5) riesgos con descripción común los cuales se listan a continuación:

Descripción común de riesgos	
1	No disponibilidad de la información.
2	No disponibilidad de los sistemas de información.
3	Perdida de confidencialidad o no disponibilidad de la información.
4	Perdida de integridad, confidencialidad o no disponibilidad de la información.
5	Perdida de información o no disponibilidad de los sistemas de información.

Nota: Las vulnerabilidades, amenazas, o descripción detallada de los riesgos de seguridad de la información son información reservada, teniendo en cuenta que pueden poner en riesgo la operación y activos de información de la entidad. Únicamente se listará la descripción común del riesgo.

4.3. Resultado del plan de tratamiento de riesgos

Para los riesgos identificados se estableció un plan de tratamiento de riesgos de doscientos cincuenta y cuatro (254) actividades, para su primera fase con la ejecución del tratamiento se plantea el nivel de riesgo residual quede de la siguiente forma:

Valoración Riesgo Residual	
Descripción	**Distribución**
Extremo	0
Alto	7
Moderado	7
Bajo	1

Los controles propuestos para la mitigación de los riesgos contemplan generación de documentos con lineamientos y políticas de seguridad de la información, asignación de roles en el grupo TIC, concientización de personal e inversión en controles tecnológicos que permitan el adecuado resguardo y protección de los activos de información.

4.4. Monitoreo y seguimiento del plan de tratamiento de riesgos

Es responsabilidad de los dueños de los procesos realizar el monitoreo de los riesgos y analizar los resultados cuatrimestralmente y reportar los resultados del monitoreo y su análisis, el cual debe enviarse a la oficina de planeación para su análisis y consolidación.

El oficial de Seguridad asesora y apoyara a los dueños de proceso en la identificación de riesgos y planteamiento de tratamiento de los mismos. De igual forma, revisara la ejecución de los

tratamientos referentes a riegos de seguridad de la información y brindara retroalimentación al coordinador del grupo TIC para que sea informado a la alta dirección del Ministerio.

5. Comunicación

El presente documento será comunicado a las partes interesadas por medio de la página web del Ministerio de Transporte como documento de conocimiento público de la organización.

ELABORÓ	REVISÓ	APROBÓ
Nombre: José Ricardo Acevedo Cargo: Coordinador Grupo TIC y CIO Nombre: Juan Carlos Valenzuela Cargo: Especialista de seguridad de la información. Nombre: Hugo Alejandro Casallas Cargo: Oficial de Seguridad de la Información	Nombre: José Ricardo Acevedo Cargo: Coordinador Grupo TIC y CIO	Nombre: Ángela María Orozco Gómez Cargo: Ministra de Transporte Fecha: 26-Dic-2019