PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE INFORMACION DEL INSTITUTO MUNICIPAL DE TRANSITO Y TRANSPORTE DEL MUNICIPIO DE ALBANIA– LA GUAJIRA

HASSLER DANIEL QUINTANA DIAZ
Director

Enero de 2024

INTRODUCCION

Mediante la definición del Plan de Tratamiento de Riesgos se busca establecer medidas para mitigar los riesgos presentes en su análisis (perdida de confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información) evitando situaciones que generen incertidumbre en el cumplimiento de los objetivos de la Información y las Comunicaciones

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos identificados en los procesos de la entidad, estas acciones son organizadas en actividades, definiendo para cada una de ellas las tareas, el responsable y sus fechas de ejecución que serán aplicadas durante la vigencia del plan.

Las actividades se definieron teniendo en cuenta la información del análisis de riesgos, de las necesidades y el contexto de los procesos de la entidad en cuanto a la seguridad y privacidad de la información proporcionando las herramientas necesarias para identificar sus características y definir los pasos a seguir para su ejecución

Teniendo en cuenta lo anteriormente expuesto el Instrans, La Guajira implementa un plan de gestión de la seguridad de la información que sea de fácil entendimiento e implementación generando dentro de sus usuarios un parte de confiabilidad a la hora de confiar la información a los sistemas de información virtual que se vienen implementando dentro de la corporación .

El propósito del sistema de gestión de la seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías

El plan de tratamiento de riesgos de seguridad y privacidad de la información aporta la evidencia de los niveles de riesgos en que se encuentran los activos de información de la entidad mediante el nivel de madurez de la seguridad existente y sobre todo incentivar a los funcionarios a seguir las respectivas normas y procedimientos referentes a la seguridad y privacidad de la información

OBJETIVOS

OBJETIVO GENERAL

En la búsqueda de la protección del sistema informático, como de la información de manejo mediante las Tecnologías de la Información, el Instituto Municipal de Tránsito y Transporte de Albania INTRANS busca crear un mecanismo de tratamiento que permita asegurar y dar privacidad a la información de carácter confidencial, así como la protección de los sistemas a posibles agentes invasivos que puedan generar perdida de la información resguardada.

OBJETIVOS ESPECIFICOS

- Realizar un seguimiento minucioso el cual arroje como resultado el nivel de confiabilidad en la implementación del plan de gestión de seguridad de la información.
- Generar un mapa de riesgos informativos que nos permita identificar las causas generadoras e implementar diferentes estrategias o mecanismo de protección.
- Categorizar y valorar los activos de información.
- Generar un inventario de activos de la información que nos permita identificar la ubicación y propietarios de la información.
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información

MARCO NORMATIVO

- NTC/ISO 31000:2009 “Gestión del Riesgo. Principios y Directrices”
- Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las comunicaciones.
- NTC / ISO 27001:2013 “Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI)

IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en el INTRANS, se toma referencia la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Manual de implementación versión 3.02 del Ministerio de Tecnologías de la Información y las Comunicaciones.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar
2. Planificar: establecer el SGSI.
3. Hacer: implementar y utilizar el SGSI.
4. Verificar: monitorizar y revisar el SGSI.
5. Actuar: mantener y mejorar el SGSI

ACTIVIDADES ESTRATEGICAS

El principal activo de una organización es la información en sí, la cual puede estar en forma física como documentos impresos o escritos a mano, en medios electrónicos almacenados en Discos Duros Externos, Memorias USB o en forma digital, en los equipos de cómputo o en la Nube. Toda esta información requiere ser analizada para su protección.

1. Realizar Diagnóstico
2. Realizar Inventario de Activos de Información.
3. Realizar la Valoración de los Activos de Información.
4. Realizar el Plan maestro para ejecutar el plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)
5. Socializar avances de seguimiento al Plan de Tratamiento de Riesgo

CUMPLIMIENTO DE LA IMPLEMENTACION

Dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por la entidad

- Implementar la Política de Seguridad de la información.
- Implementar la Política de Administración de datos.
- Implementar la Política de Comunicaciones.
- Aspectos organizativos de la seguridad de la información
- Seguridad de la Información enfocada a los recursos humanos
- Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
- Revisión de los Controles de acceso
- Seguridad Física y del entorno
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

CRONOGRAMA

SEGUIMIENTO Y EVALUACION

Al finalizar cada etapa se presentará un informe de seguimiento y monitoreo a la secretaria General del INTRANS, con el fin de evaluar todos los pasos se han ido realizado y los avances en materia de seguridad de la información.

ENTREGABLES

1. Plan de tratamiento de riesgo
2. Política de Seguridad.
3. Análisis de recursos tecnológicos
4. Matriz de identificación del riesgo
5. Análisis del riesgo
6. Valoración del ries

ACTIVIDAD	FEBRERO				MARZO				ABRIL				MAYO				JUNIO			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1. Realizar Diagnóstico																				
2. Realizar Inventario de Activos de Información con los líderes de cada Proceso de acuerdo a los formatos de gestión documental.																				
5. Realizar la Valoración de los Activos de Información																				
6. Realizar el Plan maestro para ejecutar el plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)																				
7. Socializar avances de seguimiento al Plan de Tratamiento de Riesgo																				
8. Ejecutar controles de seguridad																				
9. seguimiento de mantenimiento preventivo y correctivo																				

República de Colombia
MINISTERIO DE TRANSPORTE

Calle 2 No. 4-13 (Albania – La Guajira)
7775377 3126786983
instrans@albania-laguajira.gov.co

VIGILADO SuperTransporte