COLOMBIA POTENCIA DE LA VIDA

Transporte

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

Versión 01 - 2024

UPIT
UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE

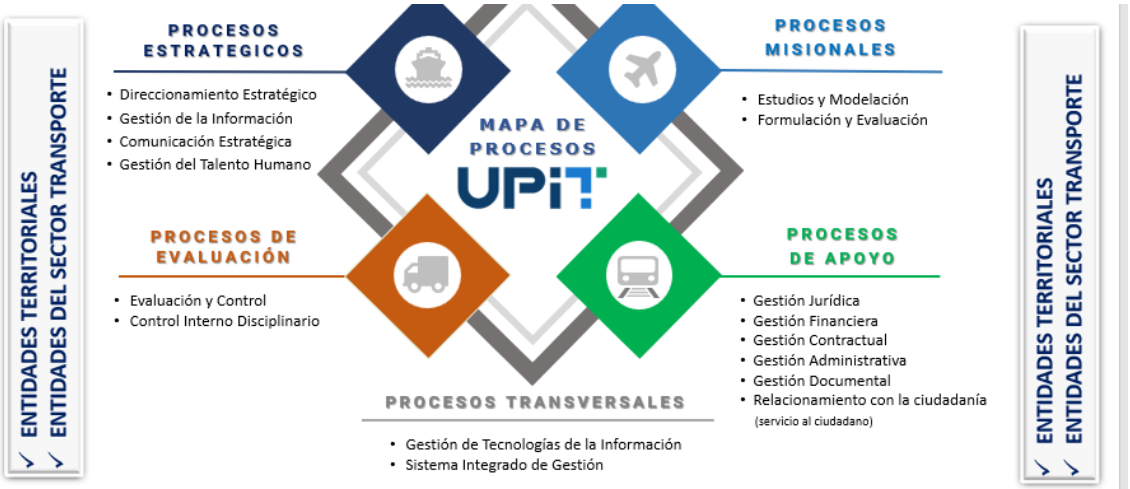
TABLA DE CONTENIDO

1. INTRODUCCIÓN

Preservar la seguridad de la información digital es un tema que se vuelve cada día más complejo y crítico debido al uso y masificación de las tecnologías de la información y las comunicaciones en las organizaciones, por esto es prioritario para la Unidad de Planeación de Infraestructura de Transporte – UPIT definir y adoptar prácticas integradas a sus procesos y operaciones, las cuales funcionen como estrategias para reducir o mitigar los riesgos de seguridad digital a los cuales se encuentran expuestos sus activos de información.

La UPIT debe fortalecer la confidencialidad, integridad y disponibilidad de los activos de información, con un enfoque basado en riesgos y cuyo proceso es importante para el gobierno corporativo, toma de decisiones, logro de los objetivos estratégicos y cumplimiento de su misionalidad.

Un componente fundamental desde la planificación del Sistema de Gestión de Seguridad de la Información y del proceso de identificación, análisis y evaluación de riesgos de seguridad digital, es la definición e implementación de un plan de tratamiento a estos riesgos, en el cual se determina implementar herramientas, sistemas, políticas, procesos, procedimientos, prácticas o mecanismos dinámicos y seguros que protejan la información y la infraestructura tecnológica que la soporta.



Mapa de Procesos de la UPIT

2. CONDICIONES GENERALES

La gestión de riesgos de seguridad de la información digital en la UPIT se basará siguiendo los lineamientos de la metodología propuesta por el Departamento Administrativo de la Función Pública "Guía para la administración del riesgo y el diseño de controles en entidades públicas V6 – 2022".

3. JUSTIFICACIÓN

El desarrollo de un plan de tratamiento de riesgos de seguridad digital permitirá a La Unidad de Planeación de Infraestructura de Transporte – UPIT, planear, implementar, mantener y mejorar las acciones encaminadas a proteger los activos de información de la entidad, a través de la adopción de herramientas, sistemas, políticas, procedimientos, prácticas o mecanismos dinámicos y seguros, así como dar cumplimiento a la normatividad establecida por el estado Colombiano, entre ellas el Modelo de Seguridad y Privacidad de la Información – MSPI, el decreto 1008 de 14 de junio 2018 y adoptar las buenas prácticas establecidas por estándares internacionales como ISO/IEC 27001:2013, ISO/IEC 27002:2015, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 emitida por el DAFP.

4. OBJETIVO

Presentar el plan de tratamiento definido para los riesgos de seguridad digital identificados por La Unidad de Planeación de Infraestructura de Transporte – UPIT el cual contribuirá al logro de los objetivos estratégicos, la visión de la entidad, el cumplimiento de los requisitos legales y reglamentarios vigentes y aplicables, la misionalidad y la preservación de la confidencialidad, integridad y disponibilidad de la información.

5. ALCANCE

El plan de tratamiento de riesgos definido en este documento aplica para los riesgos de seguridad digital identificados en la Unidad de Planeación de Infraestructura de Transporte – UPIT. Identificado y valorando los riesgos, así como diseño del tratamiento de estos con procesos de seguimiento y control.

6. RESPONSABILIDADES

La Oficina de Gestión de la Información o área definida, liderará la metodología y gestión de riesgos de seguridad digital propuesta por el Departamento Administrativo de la Función Pública, según las necesidades de la UPIT, coordinando el cumplimiento de este plan para la correcta identificación y valoración de riesgos de seguridad digital en la entidad.

Así mismo, ofrecerá acompañamiento en el desarrollo e implementación del proceso de administración de los riesgos de seguridad digital, identificará responsabilidades y armonizará los ejercicios para mitigar los riesgos.

A través de los referentes o líderes de los procesos se diligenciará el Mapa de Riesgos para registrar la gestión adelantada, así como la revisión, seguimiento y monitoreo de los riesgos y su plan de tratamiento.

El Oficial de Seguridad de la Información o quien cumpla sus funciones, velará por la adecuada elaboración e implementación del mapa de riesgos de seguridad digital de cada proceso, promoviendo su apropiación, entendimiento y evaluación del mismo.

Los responsables de implementar las acciones definidas para tratar, reducir o mitigar los riesgos de seguridad digital, deben estar relacionados en el plan de tratamiento de cada riesgo.

7. DEFINICIONES

Activo. En el contexto de seguridad digital, son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital, dentro de los cuales se puede mencionar:

- Información.
- Software.
- Recursos físicos.
- Servicios.
- Personas y sus cualificaciones, habilidades y experiencias.
- Elementos intangibles como la reputación y la imagen.

Activo de información. Conocimiento o datos que son de valor para la entidad. Ver modelo estándar de control interno para el Estado colombiano, MECI 1000:2005, Numeral 2.2 Componente Información.

Amenaza. Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Causas. Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Confidencialidad. Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Consecuencia. Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control. Medida que permite reducir o mitigar un riesgo.

Disponibilidad. Propiedad de ser accesible y utilizable a demanda por una entidad.

Evaluación del riesgo. Busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo Residual).

Gestión del riesgo. Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Identificación del riesgo. Se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

Integridad. Propiedad de exactitud y completitud.

Mapa de riesgos. Documento con la información resultante de la gestión del riesgo.

Política de administración de riesgos. Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riego.

Riesgo inherente. Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual. Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

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 del ambiente físico, digital y las personas.

Seguridad de la información. Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, puede involucrar otras propiedades como: autenticidad, trazabilidad, no repudio y fiabilidad.

Tolerancia al riesgo. son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Tratamiento del riesgo. Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

Valoración de riesgos. Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

8. DESARROLLO DEL PLAN

Para la definición del plan de tratamiento de riesgos de seguridad digital se señalan actividades que se listan a continuación.

- Definición de controles.
- Identificación del riesgo.
- Análisis del riesgo inherente.
- Evaluación del riego.
- Evaluación de controles existentes.
- Análisis del riesgo residual.
- Selección de la opción de tratamiento del riesgo.
- Definición del plan de tratamiento.

La Unidad de Planeación de Infraestructura de Transporte – UPIT, debe implementar el Sistema de Gestión de Seguridad de la Información - SGSI, y debe identificar los riesgos que puedan afectar la disponibilidad, integridad y confidencialidad de la información, estableciendo acciones que contribuyen a la preservación de estos principios de seguridad de la información. Las medidas a implementar se compararán con los controles del Anexo A de la NTC-ISO/IEC 27001:2013 para que no se omitan controles necesarios.

En el plan de tratamiento se determinan los siguientes ítems:

- **Opciones de manejo.** El propósito de esta etapa es seleccionar e implementar opciones o estrategias para abordar el riesgo y con base en ella diseñar las acciones a aplicar. Las opciones para el tratamiento de los riesgos son:

  - **Reducir el riesgo** mediante la aplicación de controles apropiados de manera que el riesgo residual se pueda reevaluar como aceptable.
  - **Asumir el riesgo** significa que se reconoce la exposición a la pérdida, pero no se toman acciones relativas a un riesgo en particular y la pérdida es aceptada, en caso de que ocurra.
  - **Evitar el riesgo** que da origen al riesgo particular.
  - **Compartir o transferir el riesgo** a entidades como aseguradoras o proveedores que puedan gestionar de manera eficaz el riesgo particular, siempre que no resulte un costo superior al del riesgo mismo.

- **Acción para tratar el riesgo.** Describir las medidas o controles a implementar para lograr el tratamiento del riesgo.

- **Soporte.** Relaciona la evidencia que soportará el cumplimiento de la acción definida para tratar el riesgo.

- **Documentos asociados al control.** Describen los documentos existentes y que de alguna manera se relacionan con la implementación del control.

- **Responsable.** Proceso o rol encargado de la implementación y ejecución de las acciones que tratarán el riesgo.

- **Tiempo de ejecución.** Fechas de inicio y terminación de la implementación de las acciones.

- **Indicador.** Relaciona las métricas que miden la implementación de la acción.

El plan de tratamiento del riesgo se debe registrar en el formato de Mapa de Riesgos de la UPIT, dicho formato se debe oficializar y aprobar.

9. SEGUIMIENTO Y EVALUACIÓN

Para el segundo semestre del año el equipo encargado de liderar la metodología y la gestión de los riesgos de seguridad digital revisará y evaluará el plan de tratamiento y las actividades que podrán desprenderse de este seguimiento, que se describe a continuación.

Tabla 1. *Actividades para gestionar el plan de tratamiento de riesgos de seguridad digital (si es necesario, las fechas de seguimiento y planeación son susceptibles a cambios).*

GESTIÓN DE RIESGOS				
Actividad	**Tareas**	**Responsable**	**Fecha Inicio**	**Fecha Final**
Revisión y actualización de los lineamientos para la administración del riesgo.	1. Definir la política de administración del riesgo de seguridad digital. 2. Definir la metodología para la gestión del riesgo de seguridad digital. 3. Oficializar Formato Mapa de Riesgos de seguridad digital.	Oficina de Gestión de la Información	01/01/2024	11/03/2024
Plan de formación y sensibilización.	1. Socialización y entrenamiento a los funcionarios y contratistas de la entidad sobre el proceso de administración de riesgos de seguridad digital.	Oficina de Gestión de la Información - Oficina de Comunicaciones	12/03/2024	12/04/2024
Diligenciamiento del mapa de riesgos de seguridad digital.	1. Identificación de los riesgos de seguridad digital. 2. Análisis del riesgo inherente. 3. Evaluación del riego inherente. 4. Definición de controles existentes. 5. Análisis del riesgo residual. 6. Selección de la opción de tratamiento del riesgo. 7. Definición del plan de tratamiento. 8. Realimentación, revisión y verificación de los riesgos identificados (ajustes).	Líderes de procesos	16/04/2024	10/07/2024
Aceptación de los riesgos residuales y aprobación del plan de tratamiento.	1. Generar documento con la aceptación de los riesgos residuales.	Líderes de procesos	11/07/2024	12/08/2024

GESTIÓN DE RIESGOS				
Actividad	**Tareas**	**Responsable**	**Fecha Inicio**	**Fecha Final**
	2. Generar documento con la aprobación del plan del tratamiento.			
Comunicación del riesgo.	1. Presentar a las partes interesadas los resultados del proceso de administración o gestión del riesgo.	Oficina de Gestión de la Información	13/08/2024	14/09/2024
Seguimiento al plan de tratamiento.	1. Realizar seguimiento al estado de implementación de los planes de tratamiento de riesgos y verificación de evidencias.	Oficina de Gestión de la Información	15/09/2024	31/10/2024
Evaluación de la efectividad de los controles.	1. Evaluación del tratamiento a los riesgos de seguridad digital.	Oficina de Gestión de la Información	01/11/2024	15/11/2024
Mejora continua.	1. Identificación de las oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de la efectividad de los controles del plan de tratamiento.	Oficina de Gestión de la Información	16/11/2024	30/11/2024
Monitoreo y revisión.	1. Generación, presentación y reporte de indicadores del plan de tratamiento.	Oficina de Gestión de la Información	01/12/2024	31/12/2024

10. MARCO NORMATIVO

- NTC-ISO/IEC 27001:2013
- NTC-ISO/IEC 27002:2015
- Ley 1712 de 2014
- Modelo de Seguridad y Privacidad de la Información
- Política de Gobierno Digital
- Decreto 612 de 2018

11. DOCUMENTOS ASOCIADOS

- Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6 emitida por el DAFP.

12. CONTROL DE CAMBIOS

Versión Generada	Fecha	Descripción del Cambio o Modificación
Versión aprobada por la Dirección General - Planeación	23-01-2024	Versión Inicial

Elaboró	Revisó	Aprobó
Gabino Hernández- Contratista Oficina de Gestión de la Información	Bismark Benjamín Buenaños Mosquera – Dirección General UPIT	Elkin Mauricio Escobar Sarmiento - Jefe Oficina de Gestión de la Información UPIT