MINISTERIO DE TRANSPORTE

UPIT

UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE

PLAN PARA EL TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DIGITAL

Versión: 1.0

Fecha: Enero 31 - 2023

1. Introducción

La administración de riesgos es un método sistemático que permite establecer a las entidades, sean públicas o privadas, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos en función de la tecnología, equipos, infraestructura etc., asociados con una actividad, función o proceso, de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todo el equipo humano de la **Unidad de Planeación de Infraestructura de Transporte (UPIT)**, en cumplimiento de sus funciones, está expuesto a riesgos, por lo tanto, se hace necesario establecer una metodología alineada con lo definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (en adelante MinTIC), para identificar las causas y consecuencias que permitan evitar la materialización de los eventos detectados, teniendo como fin la seguridad de la información bajo los principios de Confidencialidad, Integridad, y Disponibilidad.

2. Objetivos

2.1. Objetivo general

Establecer la estructura metodológica base para la administración de riesgos de seguridad digital en la **Unidad de Planeación de Infraestructura de Transporte (UPIT)** así como el plan para llevar a cabo el tratamiento de los riesgos.

2.2. Objetivos específicos

- Establecer pautas para realizar la gestión de los riesgos de seguridad digital en la UPIT a través de la definición de una metodología base.
- Definir el plan para llevar a cabo el tratamiento de riesgos de seguridad digital durante las vigencias 2023 y 2024.

3. Alcance

Dado que la UPIT actualmente está iniciando con la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), y por lo tanto no ha desarrollado aún una gestión de riesgos, el presente plan tiene como alcance la definición de una metodología base para la gestión de los riesgos de seguridad digital alineada con lo especificado por el MinTIC, y la definición del plan de trabajo preliminar para llevar a cabo la gestión de riesgos de seguridad digital durante las vigencias 2023 y 2024.

4. Marco normativo

- **Decreto 1078 del 26 de 2015** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

- **ISO/IEC 27001:2013** "Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI)."

- **ISO/IEC 31000:2018** "Gestión del Riesgo - Directrices"

- **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".

- **Guía para la administración del riesgo y el diseño de controles en entidades públicas**. Departamento de la Función Pública (DAFP) V5[1]. **Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas**.[2]

- Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas[3].

5. Definiciones

Para la administración del riesgo de seguridad digital, se tendrán en cuenta los siguientes términos y definiciones:

[1]https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499
[2]https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%25C3%25BAblicas+-+Gu%25C3%25ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b
[3]
https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%25C3%25BAblicas+-+Gu%25C3%25ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

- **Administración de riesgos:** Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

- **Análisis del riesgo:** Etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

- **Causa:** Medios, circunstancias y/o agentes que generan riesgos.

- **Consecuencia**: Efectos que se pueden presentar cuando un riesgo se materializa.

- **Contexto:** Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

- **Control:** Acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

- **Evaluación del riesgo:** Resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

- **GRSD:** Gestión de Riesgos de Seguridad Digital.

- **Identificación del riesgo:** Etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos.

- **Impacto:** Medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

- **Mapa de riesgos:** Documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

- **Materialización del riesgo:** Ocurrencia del riesgo identificado

- **Probabilidad:** Medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

- **Proceso:** Conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

- **Riesgo:** Eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

- **Riesgo inherente:** Es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

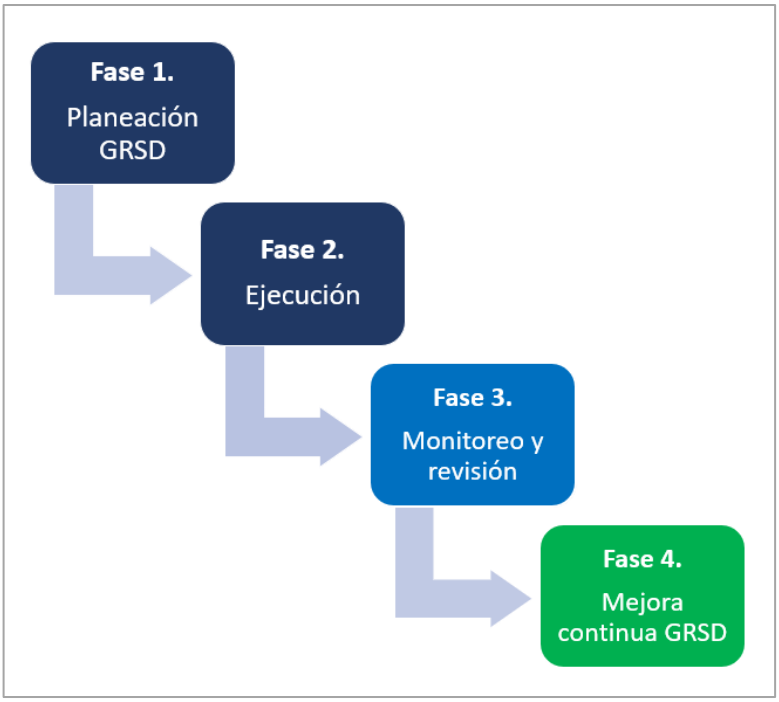
- **Valoración del riesgo:** Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

6. Metodología para la gestión de riesgos de seguridad digital

6.1. Descripción de la metodología

La metodología de referencia para llevar a cabo la gestión de riesgos de seguridad digital, se encuentra alineada con la "Guía para la administración de riesgos y el diseño de controles en entidades públicas" (DAFP en su última versión) y su anexo 4 "Lineamientos para la gestión de riesgos de seguridad digital (GRSD) en entidades públicas". Esta metodología contempla las fases de Planeación, Ejecución, Monitoreo y Revisión, y Mejora continua, tal como se muestra a continuación:

Ilustración 1. Metodología de Gestión de Riesgos de Seguridad Digital



Fuente: Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

6.2. Fases para el desarrollo de la metodología

A continuación, se mencionan cada una de las fases de la metodología. El detalle de estas fases se encuentra consignado dentro del documento "Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas".

Es importante aclarar que, como parte del desarrollo de la gestión de riesgos de seguridad digital, la UPIT dentro de su plan para el tratamiento de los riesgos de seguridad digital, realizará la revisión, adecuación y adopción de la presente metodología de manera progresiva según el nivel de madurez que vaya adquiriendo en su proceso de mejora continua.

6.2.1. FASE 1. Planificación de la Gestión de Riegos de Seguridad Digital

La fase de planificación permite a la UPIT determinar la información necesaria para llevar a cabo la gestión de riesgos, tal como el contexto, alcance, política, roles, activos e identificación de riesgos de seguridad digital, así como su respectivo tratamiento. Esta fase se contemplan las siguientes actividades:

1. Identificar y documentar el contexto interno y externo de la Entidad o dependencia especifica según sea su caso.
2. Determinar el alcance para aplicar la gestión de riesgos de seguridad digital. (Por el momento el alcance se enfoca en definir una metodología base y un plan dentro del cual se contemplen las actividades para desarrollar adecuadamente la gestión de riesgos.)
3. Definir la política de gestión de riesgo de seguridad digital.
4. Definir los roles y responsabilidades para la gestión de riesgos de seguridad digital.
5. Identificar los recursos necesarios para la Gestión de riesgos de seguridad digital
6. Identificar los activos de información y su clasificación de seguridad digital
7. Identificar los riesgos inherentes de seguridad digital
8. Identificar y evaluar los controles existentes
9. Tratar los riesgos de seguridad digital
10. Definir los planes de Tratamiento de Riesgos de Seguridad Digital e Indicadores para la Gestión del Riesgo

Dado que la UPIT actualmente está iniciando con el desarrollo de la gestión de riesgos, dentro de la fase de planeación se contemplan adicionalmente las siguientes actividades, las cuales son fundamentales para establecer las bases de la GRSD:

11. Realizar la revisión y/o actualización de la metodología de Riesgos de Seguridad Digital
12. Integrar la metodología de riesgos de seguridad digital con el Manual de Gestión y Administración Riesgos que defina la Entidad.
13. Aprobar y oficializar la metodología y los criterios de riesgo de seguridad digital.
14. Socializar la documentación aprobada para la gestión de Riesgos de Seguridad digital.

6.2.2. FASE 2. Ejecución

En esta fase se implementan los planes de tratamiento de riesgos definidos en la actividad "Definir los planes de Tratamiento de Riesgos de Seguridad Digital e Indicadores para la Gestión del Riesgo" de la Fase 1. Es importante aclarar que la implementación del plan de tratamiento es responsabilidad de cada una de las dependencias, así como transversalmente por parte del área de tecnología según aplique.

Aunque la implementación de los planes de tratamiento en algunos casos depende del presupuesto asignado, las diferentes dependencias deberán buscar controles compensatorios o alternativas con los recursos actuales para contribuir a la mitigación parcial o total de los riesgos.

6.2.3. FASE 3. Monitoreo y Revisión

Esta fase permite realizar el monitoreo constante de las situaciones que podrían generar riesgos de seguridad digital y con esto realizar su identificación, gestión y tratamiento.

En esta fase se llevan a cabo las siguientes actividades de control:

1. Registrar y reportar los incidentes de seguridad digital que generen riesgos a la UPIT.
2. Reportar la gestión del riesgo de seguridad digital al interior de la Entidad.
3. Reportar la gestión del riesgo de seguridad digital a autoridades o entidades especiales, según aplique para la UPIT.
4. Realizar auditorías internas y externas.
5. Aplicar la medición del desempeño en la implementación de los planes de tratamiento por cada una de las dependencias de la UPIT.

6.2.4. FASE 4. Mejoramiento continuo de la Gestión de Riesgos de Seguridad Digital

La mejora continua permite a la UPIT incrementar gradualmente su nivel de madurez a nivel de la gestión de riesgos de seguridad digital, la aceptación de los riesgos residuales y la implementación de controles para reducir constantemente los riesgos. En esta fase se definen las siguientes acciones:

1. Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes.
2. Establecer las posibles causas y consecuencias de los hallazgos identificados en el proceso de gestión de riesgos.
3. Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.

7. Plan para el tratamiento de los riesgos de seguridad digital

A continuación, se presenta el plan para desarrollar la metodología de gestión de riesgos de seguridad digital y así el tratamiento de los mismos. Dentro de este plan se incluyen las actividades para el desarrollo de la metodología con los respectivos periodos de ejecución.

7.1. Fase de planeación de la Gestión de Riesgos de Seguridad Digital (GRSD).

Parte 1. Definición de criterios y documentación.

FASE	ACTIVIDAD	2023											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Fase 1 Planeación GRSD	Realizar la revisión y/o actualización de la												

FASE	ACTIVIDAD	2023											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
	metodología de Riesgos de Seguridad Digital												
	Identificar y documentar el contexto interno y externo de la Entidad o dependencia especifica.												
	Determinar el alcance para aplicar la gestión de riesgos de seguridad digital												
	Definir la política de gestión de riesgo de seguridad digital.												
	Definir los roles y responsabilidades para la gestión de riesgos de seguridad digital.												
	Identificar los recursos necesarios para la Gestión de riesgos de seguridad digital												

FASE	ACTIVIDAD	2023											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
	Integrar la metodología de riesgos de seguridad digital con el Manual de Riesgos de la Entidad.												
	Aprobar y oficializar la metodología y los criterios de riesgo de seguridad digital.												
	Socializar la documentación aprobada para la gestión de Riesgos de Seguridad digital												

Parte 2. Identificación análisis y evaluación de riesgos.

FASE	ACTIVIDAD	2024											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Fase 1 Planeación GRSD	Identificar los activos de información y su clasificación de seguridad digital												
	Identificar los riesgos inherentes												

FASE	ACTIVIDAD	2024											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
	de seguridad digital												
	Identificar y evaluar los controles existentes												
	Tratar los riesgos de seguridad digital												
	Definir los planes de Tratamiento de Riesgos de Seguridad Digital e Indicadores para la Gestión del Riesgo Seguridad Digital e Indicadores para la Gestión del Riesgo												

7.2. Fases de Ejecución, Monitoreo y revisión

y Mejora continua

FASE	ACTIVIDAD	2024						2025					
		JUL	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN
Fase 2 Ejecución	Implementar los planes de tratamiento de riesgos (Dependiendo del presupuesto, actividades, fechas para el 2024)												
Fase 3 Monitoreo y Revisión	Registrar y reportar los incidentes de seguridad digital que generen riesgos a la UPIT.												
	Reportar la gestión del riesgo de seguridad digital al interior de la Entidad.												
	Reportar la gestión del riesgo de seguridad digital a autoridades o entidades especiales, según aplique para la UPIT.												
	Realizar auditorías												

FASE	ACTIVIDAD	2024						2025					
		JUL	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN
	internas y externas												
	Aplicar la medición del desempeño en la implementación de los planes de tratamiento por cada una de las dependencias de la UPIT.												
Fase 4 Mejora continua GRSD	Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes.												
	Establecer las posibles causas y consecuencias de los hallazgos identificados en el proceso de gestión de riesgos.												
	Determinar si existen otros hallazgos similares para establecer acciones												

FASE	ACTIVIDAD	2024						2025					
		JUL	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN
	correctivas y evitar así que se lleguen a materializar.												

8. Control de cambios

Fecha	Descripción del cambio o modificación	Versión generada

31/01/2023	Documento inicial	1.0