SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI - MINTIC

Nombre del documento	Informe_Tratamiento_de_Riesgos_MINTIC.doc
Versión del documento	2.0
Fecha	12/12/2019
Resumen	El presente documento define las medidas de seguridad identificadas para desarrollar e implementar al 31 de diciembre del 2020 el plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en el Ministerio de Tecnologías de la Información y la Comunicaciones.

Control de Cambios		
Fecha	**Versión**	**Descripción**
31/07/2018	1.0	Creación.
12/12/2019	**2.0**	**Seguimiento.**

	Fecha	Nombre	Cargo o Perfil
Elaboró	12/12/2019	Esmeralda Carolina Orduz Olaya	Contratista Grupo Interno de Trabajo Transformación Organizacional
Revisó	16/12/2019	Andrés Díaz Molina	Asesor Despacho de la Ministra – Oficial de Seguridad y Privacidad de la Información
Aprobó	26/12/2019	Comité MIG # 38	

TABLA DE CONTENIDO

1. RESUMEN EJECUTIVO

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos del Ministerio Tecnologías de la Información y las Comunicaciones (MINTIC).

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad, el Ministerio TIC define medidas que serán aplicadas en el segundo semestre del año 2020.

Las anteriores medidas se definieron teniendo en cuenta la información del análisis de riesgos, el cual brindó información acerca de las necesidades del Proceso de Tecnología del Ministerio TIC en cuanto a la seguridad de la información y proporcionó las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

2. INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

3. DEFINICIONES

- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.

- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

4. OBJETIVOS

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que el MINTIC pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en la Entidad.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

5. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)[1]: se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en MINTIC.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por el Ministerio TIC, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

[1] Ibídem.

6. MARCO REFERENCIAL

6.1. POLÍTICA DE ADMINISTRACION DE RIESGOS

El Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones , a través de su Modelo Integrado de Gestión, se compromete a mantener una cultura de la gestión del riesgo asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC, regulando los riesgos de los procesos y proyectos luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los de seguridad y privacidad de la Información y Seguridad Digital de manera Integral.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores del Ministerio TIC.
Se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

- Evitar: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.

- Prevenir: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos

- Reducir o mitigar: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo

- Dispersar: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos

- Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, teniendo en cuenta lo expuesto en la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)[1], las "*(…) no se debe olvidar que dentro del análisis de los controles se debe tener en cuenta al dueño del riesgo (dueño del proceso), ya que la definición de los controles es el resultado de los análisis realizados a través del seguimiento y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados*"(…).

7. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)[2]:

GESTIÓN	ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA DE FIN
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Equipo de Gestión de Riesgos	30-jun-20	1-dic-20
	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo de Gestión de Riesgos	1-abr-20	29-may-20
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo de Gestión de Riesgos	27-abr-20	30-sep-20
		Realimentación, revisión y verificación de los riesgos identificados(Ajustes)	Equipo de Gestión de Riesgos	29-abr-20	30-sep-20
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Equipo de Gestión de Riesgos	30-jun-20	30-nov-20
	Publicación	Publicación Matriz de riesgos - SIMIG	Equipo de Gestión de Riesgos	29-jun-20	30-nov-20
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Equipo de Gestión de Riesgos	30-jun-20	1-dic-20
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Equipo de Gestión de Riesgos	30-jun-20	31-dic-20
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Equipo de Gestión de Riesgos	30-jun-20	31-dic-20
		Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados.	Equipo de Gestión de Riesgos	30-jun-20	31-dic-20
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Equipo de Gestión de Riesgos	30-jun-20	31-dic-20

[2] Ibídem.

Los controles seleccionados serán confrontados con los estándares ISO 27001:2013 y su anexo A; a fin de determinar las falencias del Ministerio TIC en este sentido.

7.1. DESARROLLO METODOLÓGICO

- **Fase 1: Análisis de la información**

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles (se desprenden de las medidas) aplicados en el Ministerio TIC.
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

- **Fase 2: Desarrollo de los proyectos**

En esta fase se realizarán las actividades que permitan la estructuración de las medidas.

- Determinar el nombre de la medida.
- Definir los responsables de cada medida.
- Establecer el objetivo de cada medida.
- Elaborar la justificación de la medida.
- Definir las actividades a realizar para el desarrollo de la medida.

- **Fase 3: Análisis de los proyectos**

- Definición de los controles relacionados con cada medida.
- Validar los riesgos mitigados por cada medida.
- Análisis de la aplicabilidad de las medidas.
- Priorización de las medidas.

- **Fase 4: Definición del organigrama de responsabilidad**

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por el Ministerio teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Identificación de las funciones del Ministerio en materia de seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo por parte del Ministerio.
- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

- **Fase 5: Ciclo de vida del tratamiento de riesgos**

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

7.2. OPORTUNIDAD DE MEJORA

MINTIC no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

8. RECURSOS

MINTIC, en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	La Oficina de Tecnologías de la información a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía de Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - Octubre de 2018 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías

9. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información identificados en la entidad, corresponderá al dueño del riesgo, 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.

10. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La medición se realiza con un indicador de gestión que está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicador que se alimenta de indicadores internos en el marco de la implementación del Eje de Seguridad de la Información y que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre Seguridad de la informa.

10.1 MEDICIÓN

La medición se realiza con un indicador de gestión que está orientado principalmente a determinar el porcentaje de implementación de los controles definidos en el tratamiento de riesgos de seguridad y privacidad de la información.

HOJA DE VIDA DEL INDICADOR

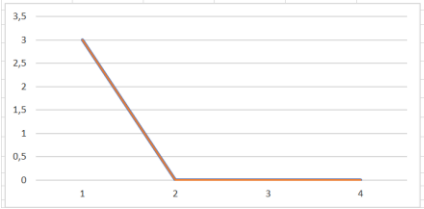
Despliegue de Objetivos	
Dimensión:	D2 Entorno del Ecosistema Digital
Objetivo:	O5 Consolidar al MINTIC como una organización centrada en la innovación, basada en procesos transversales y orientada al desarrollo potencial de las personas
Objetivo de Calidad asociado.:	Mejorar la eficiencia, eficacia y efectividad de los procesos del MinTIC / Mejorar los niveles de satisfacción de los servicios internos
Macro proceso:	Gestión de Recursos
Proceso	Gestión de Tecnologías de Información

Datos del Indicador			
Nombre del Indicador.:	Nivel de de implementacion de los controles para los riesgos de Seguridad y Privacidad de la Información, Segundad Digital y Continuidad de la Operación	Objetivo del Indicador.:	Medir el nivel de implementación de los controles para los nesgos de Seguridad y Privacidad de la Información, Segundad Digital y Continuidad de la Operación.
Tipo de Indicador.:	Eficacia	Frecuencia recolección de la info	Mensual
Responsable del análisis.:	Profesional encargado de coordinar el tema de Segundad Digital	Frecuencia del análisis de la info	Trimestral
Fuentes(s) de la Información.:	Informe de seguimiento al desarrollo y mantenimiento de sistemas de información / Formatos de acuerdos de desarrollo y de requerimientos acordados	Formula (Indice).:	Porcentaje de controles implementados = (#controles implementados / #controles definidos) *100

Metas:		
Rango		Calificación
Desde	Hasta	
85%	100%	Alto
60%	84%	Medio
0%	59%	Bajo

Variables	
1	Número de controles implementados
2	Número de definidos (aprobados)

Variable	Periodo 1	Periodo 2	Periodo 3	Periodo 4
1	0	0	0	0
2	0	0	0	0
Resultado	-	-	-	-



Análisis escrito del Periodo
PRIMER TRIMESTRE.
SEGUNDO TRIMESTRE
TERCER TRIMESTRE
CUARTO TRIMESTRE