IDEAM - INSTITUTO DE HIDROLOGÍA, METEOROLOGÍA Y ESTUDIOS AMBIENTALES.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN DEL IDEAM

IDEAM

CONTENIDO

RESUMEN EJECUTIVO 2

INTRODUCCIÓN 2

1. OBJETIVOS 3

1.1. OBJETIVO GENERAL 3

1.2. OBJETIVOS ESPECIFICOS 3

2. ALCANCE 3

3. GLOSARIO 4

4. DESARROLLO 4

4.1. RESPONSABILIDADES 5

4.2. METODOLOGÍA 5

5. TIEMPO DE EJECUCION 5

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 IDEAM.

El Plan de Tratamiento de Riesgo de seguridad Digital 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 IDEAM define medidas que serán aplicadas en el año 2022.

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 IDEAM 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.

INTRODUCCIÓN

En el marco de la implementación sostenimiento y mejora del SGSI en el IDEAM, una de las actividades de mayor relevancia en los diferentes contextos de la operación de procesos en la entidad es la gestión de los riesgos de seguridad digital evidenciados.

A través del análisis de riesgos de los activos de información del IDEAM definidos en el alcance, se han identificado riesgos asociados con la debilidad de los controles de acceso, inexistencia de mantenimientos preventivos, fallas en la infraestructura de IT, fallas en el suministro eléctrico, etc. Aunque se identificaron algunos controles implementados, la generación de procedimientos claros y precisos se hace imperante para mitigar el grado de exposición actual. Los controles implementados y los proyectos que se plantean a continuación promueven la mitigación de los riesgos identificados, sin embargo, la situación presente vislumbra debilidades que requieren atención inmediata.

Dentro de la definición de cada proyecto planteado para reducir los riesgos se encuentra el objetivo, justificación e información adicional con las actividades a realizar con su respectivo responsable.

Como parte de la gestión de riesgos del IDEAM, es trascendente incorporar los riesgos a los activos considerados más críticos y hacer el seguimiento y la revisión correspondientes a los planes de tratamiento establecidos, descritos en el documento anexo.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Estructurar las actividades que deberán ser desarrolladas por el IDEAM para reducir los riesgos previamente identificados con el fin evitar la materialización de estos.

1.2. OBJETIVOS ESPECIFICOS

- 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 IDEAM 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.
- Evaluar las medidas existentes a fin de determinar cuáles otras podrán ser adoptadas por el IDEAM.
- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en el Instituto
- Identificar los responsables de la aplicación de las medidas de tal forma que esto facilite su implementación.
- Definir los proyectos a implementar por parte del IDEAM que permitirán mitigar los riesgos identificados.

2. 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 la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016) y la metodología establecida por la entidad denominada "E-SGI-SI-I002 INSTRUCTIVO RIESGOS DE SEGURIDAD DE LA INFORMACIÓN": se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en el IDEAM.

El plan de tratamiento de riesgos evaluará las opciones de manejo y tratamiento para los riesgos identificados y evaluados en el análisis de riesgos, cuyos niveles de riesgo para cualquiera de las áreas de impacto resultaron como "Extremo" y "Alto", en el marco de la operación por procesos de IDEAM y dando alcance al Modelo de Seguridad y Privacidad de la información regido por MINTIC.

3. GLOSARIO

- **Amenaza**. Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en el Instituto (materializar el riesgo).
- **Control**. 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 organización.
- **Impacto**. Son las consecuencias que genera un riesgo una vez se materialice.
- **Probabilidad**. Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Riesgo**. Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Vulnerabilidad**. Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

4. DESARROLLO

La gestión del riesgo no es una actividad independiente que se separa de las actividades y los procesos del IDEAM, la gestión del riesgo es parte de las responsabilidades de la alta dirección y una parte integral del nuevo modelo de operación por procesos, gestión de proyectos y gestión de cambios, incluyendo la planificación estratégica.

Para el desarrollo del plan de tratamiento de riesgos en el IDEAM se debe poner en práctica lo definido en la guía de gestión - SGSI, teniendo en cuenta los controles existentes los cuales deben ser revisados constantemente y la definición de nuevos controles a implementar (Anexos ISO 27001:2013). Por tal razón la entidad deberá diseñar y ejecutar estrategias para tratar los riesgos identificados de acuerdo con su criticidad (Niveles Altos, Moderados y Extremos) y opciones de tratamiento:

- Asumirlos o aceptarlos
- Reducirlos
- Evitarlos
- Compartirlos o transferirlos

Los riesgos con nivel de criticidad baja pueden ser asumidos o aceptados, aunque no se requiere hacer tratamiento, se deben identificar los controles existentes de tal manera que permitan ser evaluados y analizados ya que con base a los resultados se determinará si son adecuados o deberán modificarse.

Es importante tener en cuenta evaluar y cuantificar las posibles pérdidas que implicarían para la entidad la no adopción de medidas contra el riesgo.

Para la ejecución del plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación Tecnológica, se realizarán las actividades acordes a lo establecido y lo definido en el Plan de Implementación del SGSI o Plan de Seguridad y privacidad de la información.

4.1. RESPONSABILIDADES

El IDEAM deberá definir los roles y responsabilidades de todas las partes interesadas en lo concerniente a la gestión de riesgos, promoviendo el monitoreo y revisión a la gestión en sus etapas, con el propósito de asegurar el cumplimiento de los planes de tratamiento proyectados, ejecutando los controles y acciones definidos, desarrollando e implementado procesos de control y gestión con el propósito de asegurar la efectividad y el cumplimiento de los objetivos institucionales.

Dichas responsabilidades son acordes a línea estratégica y las tres líneas de defensa del Modelo Integrado de Planeación y Gestión (MIPG), donde se aprueban las directrices para la gestión del riesgo en la entidad y la revisión y/o mejora de las políticas establecidas.

4.2. METODOLOGÍA

Con la gestión del riesgo se busca fortalecer las medidas de prevención y control de las actividades desarrolladas en el IDEAM para los riesgos de Seguridad de la Información, de acuerdo con la identificación, análisis, valoración y tratamiento de estos acorde a lo establecido en la metodología establecida por la entidad denominada “E-SGI-SI-I002 INSTRUCTIVO RIESGOS DE SEGURIDAD DE LA INFORMACIÓN”.

5. TIEMPO DE EJECUCION

El plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se actualiza y aprueba anualmente, el seguimiento se realiza conforme a lo definido en el plan de trabajo que se muestra a continuación:

Gestión de Riesgos	Revisar y actualizar los lineamientos referente al proceso de gestión de Riesgos de información	Elaboración y/o actualización del instructivo y herramientas de gestión de riesgos	Oficial de Seguridad de la Información / GAESI	3/02/2022	23/03/2022
	Sensibilización	Socialización a la oficina de informática de la Guía y Herramienta -Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Oficial de Seguridad de la Información / GAESI	3/03/2022	3/03/2022
	Identificación de riesgos de seguridad de la información	Identificación, Análisis, Evaluación de Riesgos de Seguridad y Privacidad de la Información	Oficial de seguridad de la Información / Referentes SGI - Proceso / GAESI	24/06/2022	15/07/2022
		Revisión y realimentación de los riesgos identificados proceso - Ajustes	Oficial de Seguridad de la Información / GAESI		
	Aceptación de Riesgos Identificados	Aceptación de Riesgos de Seguridad y Privacidad de la Información y plan de tratamiento (reunión oficina informática)	Líder del Proceso	18/07/2022	18/07/2022

	Publicación de Riesgos	Publicación de riesgos Seguridad de la Información en la intranet	Oficial de Seguridad de la Información/ Oficina de Planeación / GAESI	21/07/2022	21/07/2022
		Implementar Plan de Acción Riesgos de Seguridad	Oficial de Seguridad de la Información/ Oficina de Planeación / GAESI	25/07/2022	15/12/2022
	Seguimiento fase de tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Oficial de Seguridad de la Información/ Oficina de Planeación / GAESI	25/10/2022	15/12/2022
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Oficial de Seguridad de la Información/ Referentes SGI	1/12/2022	8/12/2022
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Oficial de Seguridad de la Información/ Referentes SGI / GAESI		
		Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo con los cambios solicitados	Oficial de Seguridad de la Información/ Referentes SGI / GAESI	12/12/2022	15/12/2022

6. 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.

7. OPORTUNIDAD DE MEJORA

El IDEAM 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. CONCLUSIONES

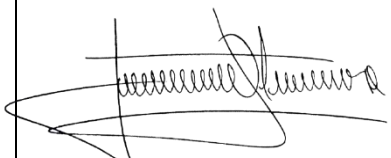
- Se deben desarrollar sesiones de sensibilización y concienciación orientado a los funcionaros sobre las políticas, normas y procedimientos de seguridad de la información a fin de que todos los funcionarios comprendan la importancia de proteger los activos de información.
- Se deben desarrollar actividades de capacitación y toma de conciencia con los colaboradores del Instituto para reducir la probabilidad de errores de tipo humano que afecten la seguridad de los activos de información.
- Para la ejecución de los proyectos se deben tener en cuenta que estos requieren de una coordinación eficiente debido a que la responsabilidad de la ejecución no recae solamente en un proceso.

9. ANEXOS

Ninguno Asociado.

10. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
01	29/10/2015	Actualización documento para SGI
02	26/06/2018	Actualización del documento y para dar cumplimiento al decreto 415
03	18/12/2019	Actualización del documento – contenido en cumplimiento al decreto 612 de 2018
04	18/01/2021	Actualización del documento – contenido en cumplimiento al CONPES 3995
05	17/01/2022	Actualización del documento.
06	18/03/2022	Actualización del documento.
07	05/04/2022	Actualización del documento

ELABORÓ:	REVISÓ:	APROBÓ:
		
Guillermo Otálora Luna **Oficial de Seguridad de la Información**	Eduardo Ramírez Acosta **Profesional Especializado Oficina Informática**	Alicia Barón Leguizamón **Jefe Oficina Informática**