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

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 2021.

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.

OBJETIVOS

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.

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 Instiuto
- 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.

ALCANCE

En el plan de tratamiento de riesgos se evaluarán las opciones de manejo de riesgos y se definirán proyectos de 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.

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.

RESUMEN

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos, evitando aquellas situaciones que comprometan el logro de los objetivos del Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM). 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 proyectos, y para cada uno de ellos se define el nombre del proyecto, objetivo, justificación, responsable del proyecto, prioridad del proyecto, medidas relacionadas con el proyecto y la mitigación de riesgos, actividades o guías de implementación, observaciones y documentos de referencia; para el caso de IDEAM, se definieron los siguientes 15 proyectos:

No	PROYECTO
1	Control de Acceso Lógico
2	Definición del área de archivo (Incluye Archivo Digital)
3	Modelo de Atención de Incidentes de Seguridad de la Información (Control de Calidad).
4	Política de escritorio despejado, pantalla despejada y bloqueo de sesión.
5	Control de Acceso físico y protección de la información en oficinas.
6	Implementación de la Arquitectura de Seguridad
7	Definición de actividades para la ejecución de los mantenimientos
8	Adecuación del espacio para organizar los dispositivos activos de red.
9	Capacitación al personal
10	Abastecimiento de los servicios públicos básicos; energía, agua, gas, aire acondicionado.
11	Procedimientos de Continuidad del Negocio
12	Revisión, Actualización y Pruebas del Plan de Continuidad del Negocio (BCP)
13	Proceso de inducción sobre seguridad de la información
14	Plan de capacitación en el uso de los aplicativos para nuevos usuarios.
15	Procedimiento copias de respaldo y restauración

Tabla 1. Proyectos de Mitigación de Riesgos

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

Las medidas identificadas en la etapa de análisis de riesgos fueron relacionadas con cada uno de los proyectos para determinar los riesgos que se mitigarían con la implementación de los proyectos, ayudando a definir las características a tener en cuenta para la priorización de los proyectos.

MARCO REFERENCIAL

COMPROMISO DE LA ALTA Y MEDIA DIRECCIÓN

Para la implementación del Plan de Tratamiento de Riesgos es indispensable el apoyo y compromiso de Dirección General y los líderes de los procesos, debido a que son ellos los que aprueban las directrices en el tema seguridad de la información, y pueden definir estos procedimientos como estratégicos para el desarrollo del Instituto. Una vez la Dirección General se comprometa con el desarrollo de la seguridad en el Instituto, este mensaje podrá ser transmitido de forma directa a todos los funcionarios de los procesos en cabeza de sus directores.

El compromiso de la Alta Dirección abarca los planes de sensibilización y capacitación de sus empleados para que estos puedan asumir roles en el proceso de protección de la información.

POLÍTICAS DE ADMINISTRACION DE RIESGOS

Las políticas identifican las opciones para tratar y manejar los riesgos basados en la valoración de riesgos, permiten tomar decisiones adecuadas y fijar los lineamientos de administración del riesgo; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los funcionarios del IDEAM.

Se debe tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto.

Evitar el riesgo, tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

***Reducir el riesgo*,** implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

Compartir o transferir el riesgo, reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

***Asumir un riesgo*,** luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento.

METODOLOGÍA

El plan de tratamiento de riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información críticos del IDEAM., estas actividades serán estructuradas en el formato que se muestra en la Tabla 2. Formato de diligenciamiento de los proyectos.

Lo anterior se realizará teniendo en cuenta la información recolectada en la etapa de evaluación de riesgos, lo referente a los controles o medidas de seguridad existentes en el Instituto y a las vulnerabilidades y amenazas que facilitan la materialización de los riesgos.

Proyecto Número		**Nombre del Proyecto:**			
1		**Área/Cargo Responsable:**			
Objetivo del Proyecto:					
Justificación:					
INFORMACIÓN ADICIONAL DE LA MEDIDA					
Fecha:		**Versión**		**Responsable de hacer seguimiento:**	
Prioridad		**Fecha de revisión**		**Medida relacionada:**	
ACTIVIDADES A REALIZAR					
Actividades o Guía de Implementación				**Responsable**	
OBSERVACIONES Y MODIFICACIONES					
Observaciones:					
DOCUMENTACIÓN DE REFERENCIA					

Tabla 2. Formato de diligenciamiento de los proyectos.

DESARROLLO METODOLÓGICO

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

En esta fase se evaluarán los resultados de las reuniones efectuadas en la etapa de valoración de riesgos para lo cual se desarrollarán las siguientes actividades:

- Determinar los controles aplicados en el IDEAM.
- Determinar los riesgos que van a ser incluidos en el plan de tratamiento de riesgos según los niveles de riesgos.
- Definir los proyectos que harán parte del plan de tratamiento de riesgos.

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

En esta fase se realizarán las actividades que permitirán estructurar los proyectos:

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

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

En esta fase se realizará el análisis de las actividades desarrolladas en la fase 2, además de la información contenida en los documentos de análisis de riesgos y matriz de riesgos:

- Definición de los controles relacionados con cada proyecto.
- Validar los riesgos mitigados por cada proyecto.
- Análisis de la aplicabilidad de los proyectos
- Priorización de los proyectos.

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

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo; esta etapa deberá ser desarrollada por el IDEAM. Teniendo en cuenta su estructura organizacional. Las actividades que deben ser contempladas son:

- Identificación de las funciones de los grupos de control organizacional dentro del IDEAM.
- Definición del grupo de trabajo de gestión de riesgo por parte del IDEAM.

- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de los proyectos.

- **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 esta etapa 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 uno de los proyectos.
- **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.

RESULTADOS

DEFINICIÓN DE LOS PROYECTOS

Los proyectos del plan de tratamiento de riesgos se definieron teniendo en cuenta las vulnerabilidades identificadas por los funcionarios a nivel de los procesos, los controles que en el momento no se estén ejecutando y que además de ello no se encuentren documentados, lo cual representa una brecha de seguridad que puede facilitar la materialización de los riesgos sobre los activos de información.

PRIORIDAD DE LOS PROYECTOS.

La prioridad de los proyectos en primera instancia se definió teniendo en cuenta el número de riesgos correspondientes a las propiedades evaluadas (Confidencialidad, Integridad, Disponibilidad, Trazabilidad y No Repudio), a los cuales dan cobertura los proyectos. Esto se indica en la columna *Prioridad del proyecto* de la Tabla 3. *Prioridad de los proyectos*; en segundo lugar, se revisaron las vulnerabilidades mitigadas por el proyecto teniendo en cuenta la recurrencia de identificación de las mismas por parte de los funcionarios de los procesos evaluados. Luego se tuvo en cuenta la recurrencia de identificación de vulnerabilidades para los riesgos identificados en los niveles de riesgo EXTREMO y ALTO.

No	PROYECTO	PRIORIDAD
1	Control de Acceso Lógico	ALTA
2	Definición del área de archivo (Incluye Archivo Digital)	ALTA
3	Modelo de Atención de Incidentes de Seguridad de la Información (Control de Calidad)	ALTA
4	Política de escritorio despejado, pantalla despejada y bloqueo de sesión	MEDIA
5	Control de Acceso físico y protección de la información en oficinas	ALTA
6	Implementación de la Arquitectura de Seguridad	ALTA

No	PROYECTO	PRIORIDAD
7	Definición de actividades para la ejecución de los mantenimientos	BAJA
8	Adecuación del espacio para organizar los dispositivos activos de red	MEDIA
9	Capacitación al personal	MEDIA
10	Abastecimiento de los servicios públicos básicos; energía, agua, gas, aire acondicionado	BAJA
11	Procedimientos de Continuidad del Negocio	ALTA
12	Revisión, Actualización y Pruebas del Plan de Continuidad del Negocio (BCP)	ALTA
13	Proceso de inducción sobre seguridad de la información	MEDIA
14	Plan de capacitación en el uso de los aplicativos para nuevos usuarios.	MEDIA
15	Procedimiento copias de respaldo y restauración	ALTA

Tabla 3. Prioridad de los proyectos riesgos mitigados por proyecto

Los siguientes ítems pertenecen a la columna "*MITIGACIÓN DE RIESGOS POR PROYECTO*" del Formato de Diligenciamiento de los Proyectos:

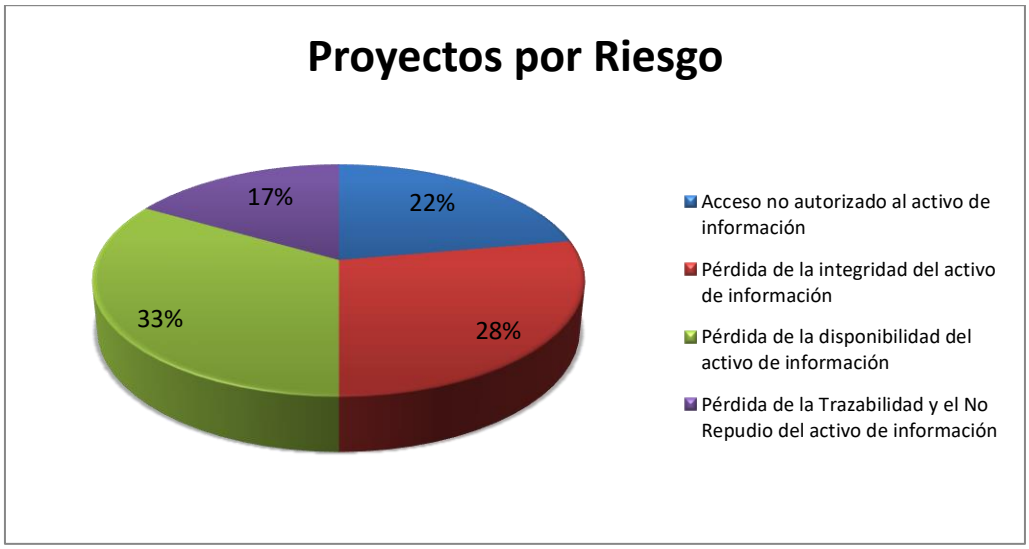
1- Acceso no autorizado al activo de información.
2- Pérdida de la integridad del activo de información
3- Pérdida de la disponibilidad del activo de información
4- Pérdida de la trazabilidad y el no repudio del activo de información

A continuación, se muestra la relación de los proyectos a implementar con respecto a los riesgos que éstos ayudan a mitigar.

PROYECTO	Acceso no autorizado al activo de información	Pérdida de la integridad del activo de información	Pérdida de la disponibilidad del activo de información	Pérdida de la Trazabilidad y el No Repudio del activo de información
Control de Acceso Lógico	x	x	x	x
Definición del área de archivo (Incluye Archivo Digital)	x	x	x	
Modelo de Atención de Incidentes de Seguridad de la Información (Control de Calidad)	x	x	x	x
Política de escritorio despejado, pantalla despejada y bloqueo de sesión	x	x		
Control de Acceso físico y protección de la información en oficinas	x	x	x	x
Implementación de la Arquitectura de Seguridad	x	x	x	x
Definición de actividades para la ejecución de los mantenimientos			x	
Adecuación del espacio para organizar los dispositivos activos de red		x	x	
Capacitación al personal		x		x
Abastecimiento de los servicios públicos básicos; energía, agua, gas, aire acondicionado			x	
Procedimientos de Continuidad del Negocio			x	
Revisión, Actualización y Pruebas del Plan de Continuidad del Negocio (BCP)			x	
Proceso de inducción sobre seguridad de la información	x	x	x	x
Plan de capacitación en el uso de los aplicativos para nuevos usuarios.	x	x	x	
Procedimiento copias de respaldo y restauración	x		x	x

Tabla 4. Mitigación de Riesgos por Proyecto

La siguiente gráfica muestra el porcentaje de proyectos con respecto a cada uno de los riesgos:



Gráfica 1. Distribución de Proyectos por Riesgo

EJECUCIÓN DE LOS PROYECTOS

Para la ejecucion de los proyectos se deberá realizar un plan de trabajo asociado al plan de implementación de Seguridad y Privacidad de la Información de la vigencia en desarrollo definiendo actividades, responsables asi como sus tiempos de ejecución, teniendo en cuenta los recursos disponibles para tal fin, además de tener en cuenta la tabla de prorizacion de ejecución de los proyectos propuestos.

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

CONCLUSIONES

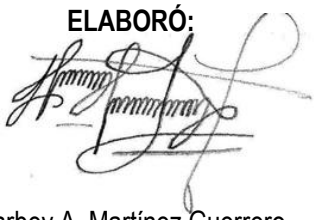
- Se definieron quince (15) proyectos teniendo en cuenta la información del análisis de riesgos realizado en el IDEAM.
- Se deben desarrollar sesiones de sensibilización y concienciación orientado a los funcionaros sobre las políticas, normas y procedimientos de seguridad de la información a fin de que 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.

ANEXOS

ANEXO 1: PLAN DE TRATAMIENTO DE RIESGOS

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

ELABORÓ:	**REVISÓ:**	**APROBÓ:**
 Harbey A. Martínez Guerrero **Oficial de Seguridad de la Información**	Eduardo Ramírez **Profesional Especializado Oficina Informática**	Alicia Barón Leguizamón **Jefe Oficina Informática (E)**