TABLA DE CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

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).

- **Riesgo en la seguridad de la información:** Es un escenario bajo el cual una amenaza determinada puede explotar las vulnerabilidades de los activos o grupos de activos generando un impacto negativo a la Cooperativa y evitando que ésta pueda 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 del instituto.

- **Amenazas:** 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), o medios potenciales por los cuales las vulnerabilidades pueden ser explotadas u ocasionadas.

- **Probabilidad:** Es la posibilidad que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

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

- **Controles:** 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.

1. INTRODUCCIÓN

Dentro del marco del SGSI en el IDEAM, una de las actividades de mayor importancia es el análisis y tratamiento de los riesgos de los activos de información. Esta actividad permite identificar, analizar, evaluar y definir el manejo de los riesgos, para así apoyar el cumplimiento de los objetivos del instituto, y disminuir a un nivel aceptable el impacto de la materialización de dichos riesgos. La gestión de riesgos permite que los responsables de los procesos acompañen de manera más efectiva la implementación de los controles y acciones de mejora, con mucho más conocimiento de los objetivos y de la manera como se lleva a cabo este proceso.

2. OBJETIVO

Generar una guía de riesgos de seguridad de la información, el cual permita describir la metodología y actividades para la identificación, análisis, valoración y tratamientos de riesgos de seguridad de la información en el IDEAM.

3. METODOLOGÍA

El enfoque de riesgos presentado se basa en la identificación de las amenazas y vulnerabilidades presentes en los activos objeto del alcance; el cálculo de la probabilidad y el impacto de materialización de los riesgos y cómo pueden afectar las actividades impidiendo el logro de los objetivos del IDEAM.

Con base en los estándares ISO 27001:20131 e ISO 27002:20052 el desarrollo de esta metodología consta de los siguientes puntos:

- Definir el enfoque organizacional para la valoración del riesgo:
  - Desarrollar criterios para la aceptación de riesgos, e identificar los niveles de riesgo aceptables teniendo en cuenta la metodología aplicada en el IDEAM

- Identificar los Riesgos:
  - Identificar las amenazas a los activos relacionados previamente.
  - Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.

- Analizar y evaluar los riesgos:
  - Estimar los niveles de los riesgos.
  - Determinar la aceptación del riesgo o la necesidad de su tratamiento.

- Identificar y evaluar las opciones para el tratamiento de los riesgos.
- Seleccionar los controles para el tratamiento de los riesgos.

---

[1] La Norma ISO 27001:2005 indica los requerimientos para el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI).

[2] La Norma ISO 27002:2007 indica las mejores prácticas para la gestión de seguridad de la información.

Así, el objetivo de esta actividad es generar los procedimientos adecuados para la administración de riesgos; y a su vez generar un plan de tratamiento de riesgos que deberá ser ejecutado por el Instituto, con el fin de reducir los riesgos.

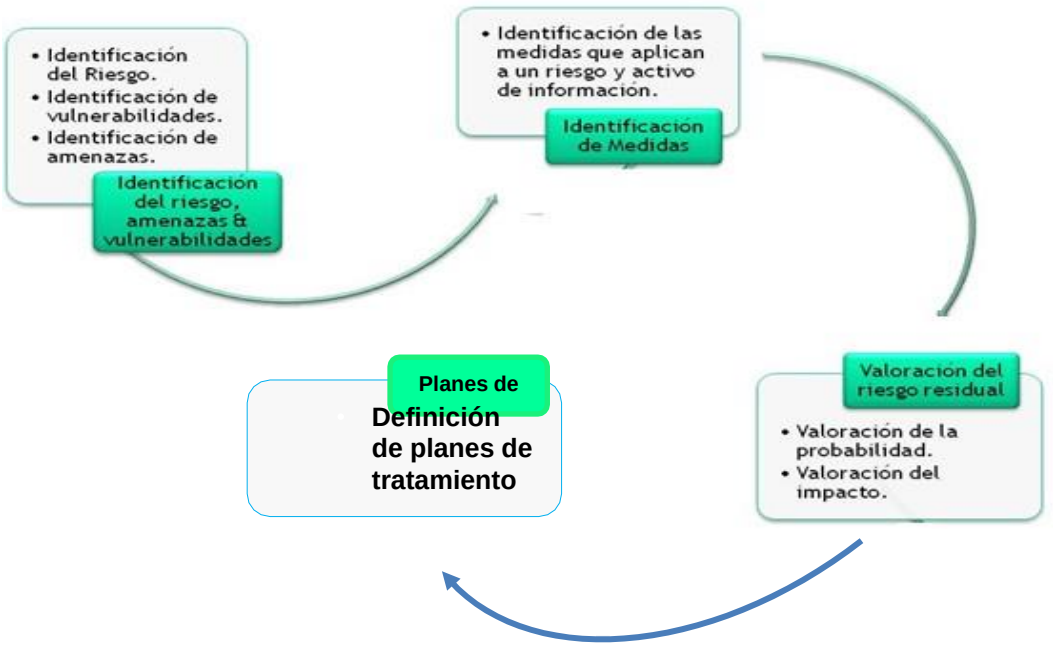

Figura 1. Actividades del Análisis de Riesgos.

3.1. COMPROMISO DE LA DIRECCIÓN GENERAL

Para el éxito en la implementación de una adecuada administración del riesgo, es indispensable el compromiso de Dirección General del IDEAM como encargada, en primera instancia, de estimular la cultura de la identificación y prevención de riesgos y en segunda instancia de definir las políticas de administración de riesgos. Para lograrlo es importante la definición de canales directos de comunicación y el apoyo a todas las acciones emprendidas en este sentido, propiciando los espacios y asignando los recursos necesarios. Así mismo, debe designar a un directivo de primer nivel que asesore y apoye todo el proceso de diseño e implementación del componente de administración del riesgo.

3.2. PROCEDIMIENTO TALLERES DE VALORACIÓN DE RIESGO

PREMISA: Para las actividades siguientes descritas en este procedimiento se hace necesario que el instituto antes de iniciar el proceso de análisis de riesgos tenga disponible el inventario de activos de información con su respectiva valoración. Esto es un requisito normativo dentro del SGSI.

3.2.1. Definir el personal involucrado en los talleres de análisis de riesgo

Se debe tener en cuenta que el personal que realice la identificación de riesgos debe tener pleno conocimiento del proceso al cual pertenecen los activos y de la interacción de éstos en el proceso. El personal encargado de realizar el análisis de riesgos sobre los activos de información en lo posible debe ser el mismo que realizó la identificación y valoración de los activos de información de cada uno de los procesos.

3.2.2. Programación de los Talleres de Riesgos

- La programación de los talleres de riesgos se realizará por procesos, es decir, que todos los procesos se citarán a reunión. Cuando se tengan activos de información que han sido identificados en todos los procesos o en varios de los procesos, se recomienda que las actividades de identificación y valoración sea realizada de forma conjunta entre todos los procesos que tienen injerencia o requieren el activo de información, es así como pueden programarse reuniones conjuntas entre personal de diferentes procesos.

3.2.3. Ejecución de los talleres

Los talleres deben ser desarrollados teniendo en cuenta el formato[3] establecido para la organización de la información descrita en este procedimiento.

MACROPROCESO	PROCESO	PROCEDIMIENTO	ACTIVO DE INFORMACIÓN	NRO. DE RIESGO	RIESGO DEL PROCESO	VULNERABILIDADES(Causas)	AMENAZAS (Agentes Generadores)	CONTROL EXISTENTE	PROBABILIDAD	VALOR PROBABILIDAD	IMPACTO - PERSONAS	VALOR IMPACTO A PERSONAS	NIVEL DE RIESGO IMPACTO A PERSONAS	IMPACTO - RECURSOS FINANCIEROS	VALOR IMPACTO IMPACTO A RECURSOS FINANCIEROS	NIVEL DE RIESGO RECURSOS FINANCIEROS	IMPACTO - DESARROLLO DE PROCESOS	VALOR IMPACTO A DESARROLLO DE PROCESOS	NIVEL DE RIESGO DESARROLLO DE PROCESOS	IMPACTO - CUMPLIMIENTO DE OBJETIVOS	VALOR IMPACTO - CUMPLIMIENTO DE OBJETIVOS	NIVEL DE RIESGO CUMPLIMIENTO DE OBJETIVOS	IMPACTO - MEDIO AMBIENTE	VALOR IMPACTO A MEDIO AMBIENTE	NIVEL DE RIESGO MEDIO AMBIENTE	IMPACTO - INFORMACIÓN	VALOR IMPACTO A LA INFORMACIÓN	NIVEL DE RIESGO INFORMACIÓN

[3] **Matriz de valoración de riesgo**

3.2.4. Selección del activo de información a analizar

De los activos de información del proceso se debe seleccionar uno a uno los activos de información para realizar el análisis de riesgo.

- *Ejemplo*

Macroproceso	Proceso	Activo de Información
Pronósticos y Alertas	Recepción y Graficación de Información Hidrometeorológica en Tiempo Real	Correo Electrónico

Tabla 1. Identificación de Activos

3.2.5. Identificador del riesgo

Corresponde a un número consecutivo asignado a cada riesgo identificado.

- *Ejemplo*

Macroproceso	Proceso	Activo de Información	No. De Riesgos
Pronósticos y Alertas	Recepción y Graficación de Información Hidrometeorológica en Tiempo Real	Correo Electrónico	1

Tabla 2. Identificador de riesgo

3.2.6. Identificación de Vulnerabilidades

Las vulnerabilidades son falencias o debilidades que pueden estar presentes en la tecnología, las personas o en las políticas y procedimientos de una compañía.

- Para la identificación de las vulnerabilidades se debe tener en cuenta el activo de información que se está analizando, el tipo de activo[4] los análisis técnicos (hacking ético), físicos (controles de acceso físico), y humanos (ingeniería social) de vulnerabilidades.
- Por cada *Activo de información* se pueden identificar diferentes vulnerabilidades.
- Para la selección de las vulnerabilidades se puede tener en cuenta el catálogo de vulnerabilidades disponible en la Tabla 3. *Catálogo* de Vulnerabilidades, sin embargo, se debe tener en cuenta que se deben identificar todas las vulnerabilidades de un activo de información independientemente de si esta se encuentra o no en el catálogo.

Vulnerabilidades
Falta de capacitación y entrenamiento para las funciones asignadas
Inadecuado control de acceso lógico y/o físico a los activos de información
Errores en la información obtenida de la fuente primaria
Inexistencia de mantenimientos predictivos, preventivos y/o correctivos o no adecuados de acuerdo a lo estipulado por el fabricante Mantenimiento relacionado con la infraestructura física, soporte eléctrico, ambiental ytecnológico
Fallas en la infraestructura de IT
Uso de protocolos inseguros
Fallas en la transmisión de los datos porque la batería se descarga (panel solar), lo que genera rangos negativos y otro tipo de inconsistencias
Inadecuada ubicación de las estaciones
Se encuentra configurado un servicio FTP plano
Fallas en el disco duro
No existe gestión de vulnerabilidades técnicas
El servidor es visible desde Internet y allí se encuentra el servicio de DA
Fallas técnicas
Deficiencias en el control de acceso físico
Existencia de otras aplicaciones en el mismo servidor
Credenciales de Administración compartidas (Sistemas de Información Geográfica y Administrador Hydras)
Fallas en el suministro eléctrico
Ancho de banda deficiente
Deficiencias en el diseño del modelo de la BD y el desarrollo de la aplicación
Inadecuada gestión de cambios

[4] Los tipos de activos de información están descritos en las matrices de Activos de Información.

Vulnerabilidades
Fallas en el suministro eléctrico / Falta de mantenimiento preventivo a los servidores
Deficiencias en los controles de acceso de personal externo (soporte técnico) Los proveedores externos que hacen mantenimiento tienen acceso a producción
Falta de conocimiento sobre seguridad de la información
Falta de conciencia sobre la seguridad de la información
Carencia de un presupuesto para operación y mantenimiento de TI, y/o dificultad para su ejecución
Carencia de personal idóneo para el uso de tecnologías y/o software
Falta de abastecimiento de los servicios públicos básicos: energía, agua, gas, aire acondicionado
Falta de documentación de los servicios y/o aplicaciones
Falta de políticas/normas/procedimientos de seguridad de la información
Falta de segregación de las funciones
Falta y/o inadecuada clasificación de activos de información
Inconformidad de los empleados y/o mal ambiente de trabajo
Inexistencia de respaldo y/o custodia de los activos de información
No existencia de un proceso de gestión de incidentes
Planeación de la capacidad de la plataforma inexistente o poco eficiente
Inadecuada prevención y detección de incendios
Inadecuada selección de personal para ingreso a la organización
Falta de mecanismos de monitoreo
Falta de revocación de los derechos de acceso al activo de información una vez el funcionario cambie de rol o se retire de la organización
Carencia de procedimientos adecuados de reutilización de medios y computadores
Falta de protección contra virus y código malicioso

Tabla 3. Catálogo de Vulnerabilidades

- **Ejemplo**

Macroproceso	Proceso	Activo de Información	No. De Riesgos	Riesgos del Proceso	Vulnerabilidades
Pronósticos y Alertas	Recepción y Graficación de Información Hidrometeorológica en Tiempo Real	Correo Electrónico	1	-	Mantenimientos no adecuados de la infraestructura
Pronósticos y Alertas	Recepción y Graficación de Información Hidrometeorológica en Tiempo Real	Correo Electrónico	2	-	Falta de documentación de los servicios o aplicaciones

Tabla 4. Identificación de Vulnerabilidades

3.2.7. Amenazas

Son un ente o escenarios internos o externos que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en el Instituto. (Materializar el riesgo) o medios potenciales por los cuales las vulnerabilidades pueden ser explotadas u ocasionadas.

- Los tipos de amenazas son:
    - *Recurso Humano*: Es el conjunto de personas vinculadas directa o indirectamente con el Activo de Información:
    - *Procesos*: Actividades para la transformación de elementos de entrada, en productos o servicios para satisfacer una necesidad
    - *Tecnológico*: Es el conjunto de herramientas empleadas para soportar el activo de información. Incluye: hardware, software y telecomunicaciones.
    - *Infraestructura Física*: Es el conjunto de elementos de apoyo para el funcionamiento de uno de los Activos de Información.
    - *Evento externo o natural*: Son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que se escapan en cuanto a su causa y origen al control del Instituto.

Para identificar las amenazas se debe tener en cuenta el activo de información, y las vulnerabilidades inherentes al activo. Es decir que para un activo de información por una vulnerabilidad se podrá seleccionar todas las amenazas que apliquen a las vulnerabilidades seleccionadas para el activo.

- **Ejemplo**

Macroproceso	Proceso	Activo de Información	No. De Riesgos	Riesgos del Proceso	Vulnerabilidades	Amenazas
Pronósticos y Alertas	Recepción y Graficación de Información Hidrometeorológica en Tiempo Real	Correo Electrónico	1	-	Mantenimientos no adecuados de la infraestructura	Procesos

Macroproceso	Proceso	Activo de Información	No. De Riesgos	Riesgos del Proceso	Vulnerabilidades	Amenazas
Pronósticos y Alertas	Recepción y Graficación de Información Hidrometeorológica en Tiempo Real	Correo Electrónico	2	-	Falta de documentación de los servicios o aplicaciones	Procesos
Pronósticos y Alertas	Recepción y Graficación de Información Hidrometeorológica en Tiempo Real	Correo Electrónico	3	-	Falta de documentación de los servicios o aplicaciones	Evento externo o natural

Tabla 5. Identificación de Amenazas.

3.2.8. Riesgos del Proceso

Consiste en la descripción del riesgo teniendo en cuenta que el riesgo corresponde al aprovechamiento de la vulnerabilidad por la amenaza. Para realizar esta descripción se puede tener en cuenta que la materialización del riesgo repercute en la afectación de una o varias de las propiedades de los activos de información, es por esta razón que la descripción de riesgo puede estar orientada en la propiedad del activo que se ve afectado si la amenaza aprovecha la vulnerabilidad como, por ejemplo:

- ✓ Pérdida de la disponibilidad del activo de información.
- ✓ Acceso no autorizado al activo de información que permite la utilización indebida o fraudulenta del mismo.
- ✓ Pérdida de la integridad del activo información que permite la utilización indebida o fraudulenta del mismo.
- ✓ Pérdida de la trazabilidad del activo de información
- ✓ Por no poder garantizar el no repudio, se podría afectar la percepción en la calidad de los servicios, cargas operativas, etc.

- **Ejemplo**

Macroproceso	Proceso	Activo de Información	No. Riesgo	Riesgos del Proceso	Vulnerabilidades	Amenazas
Pronósticos y Alertas	Recepción y Graficación de Información Hidrometeorológica en Tiempo Real	Correo Electrónico	1	Pérdida de la disponibilidad ad del activo de información	Mantenimientos no adecuados de la infraestructura	Procesos
Pronósticos y Alertas	Recepción y Graficación de Información Hidrometeorológica en Tiempo Real	Correo Electrónico	2	Pérdida de la integridad del activo información que permite la utilización indebida o fraudulenta del mismo	Falta de documentación de los servicios o aplicaciones	Procesos
Pronósticos y Alertas	Recepción y Graficación de Información Hidrometeorológica en Tiempo Real	Correo Electrónico	3	Pérdida de la integridad del activo información que permite la utilización indebida o fraudulenta del mismo	Falta de documentación de los servicios o aplicaciones	Evento externo o natural

Tabla 6. Descripción del Riesgo

3.2.9. Selección de los controles

Los controles deben ser identificados teniendo en cuenta la relación por amenaza- vulnerabilidad y la descripción del riesgo, estos controles pueden ser identificados tanto en las entrevistas de valoración de riesgos, como por resultado de auditorías o análisis tipo brecha de controles enmarcados en la gestión de la seguridad, los funcionarios deben validar si los controles identificados son empleados para la mitigación de los diferentes riesgos.

Para la selección de controles se puede tener en cuenta el siguiente catálogo:

Controles existentes
Control de calidad de la información empleada para los pronósticos y alertas.
Control de acceso físico sobre el expediente en el cual se guarda el activo.
Control de acceso lógico sobre el activo de información. Autenticación nativa del Sistema Operativo.
Proceso formal de entrega de documentación.
Control de acceso lógico sobre el activo de información. Autenticación nativa de la aplicación.
Control de acceso lógico sobre el activo de información. Autenticación propia del repositorio según políticas definidas en el Controlador de Dominio.
Control de acceso lógico sobre el activo de información. Autenticación nativa del Sistema Operativo.
Control de acceso lógico sobre el activo de información. Autenticación nativa de la aplicación.
Control de acceso físico sobre el expediente en el cual se guarda el activo.
Revisión y Calibración del equipo según buenas prácticas del fabricante.
Control de acceso físico (puertas, candados, etc.)
Revisión diaria y notificación de inconsistencias.
Control de acceso del sistema operativo.
Backup diario de la información.
VPN, credenciales de acceso.
Control de acceso del dispositivo
Llaves
Coordinación de actividades
Copias de respaldo mensual y mensual

Controles existentes
Ampliación del ancho de banda
Pruebas de estrés
Control de acceso de la base de datos
Auditoria sobre las tablas
Control de calidad

Tabla 7. Catálogo de controles.

3.2.10. Impacto inherente

Este valor se establece teniendo en cuenta: las consecuencias de materialización del riesgo (relación amenaza - vulnerabilidad), los controles existentes enfocados a reducir el impacto en caso de materialización y el tipo de recurso (Personas, Recursos Financieros, Desarrollo de procesos, Cumplimiento de Objetivos, Medio Ambiente, Información) afectado. Por cada tipo de recurso se cuenta con una escala que debe ser tomada como referencia para definir el valor.

- **Escalas de Impacto**

ESCALA DE IMPACTO AL RECURSO HUMANO		
5	Muy Crítico	Pérdida de la vida
4	Crítico	Se afecta permanentemente la integridad física, mental o social de la persona. Se requiere intervención reparadora, y quedan secuelas o consecuencias permanentes.
3	Moderado	Se afecta temporalmente la integridad física, mental o social de la persona. Se requiere intervención reparadora, pero no quedan secuelas ni consecuencias permanentes.
2	Leve	Se afecta temporalmente la integridad física, mental o social de la persona, sin necesidad de intervención reparadora.
1	Sin Afectación	No existe afectación al recurso

Tabla 8. Escala de impacto al recurso humano.

ESCALA DE IMPACTO DEL RECURSO FINANCIERO (Millones)		
5	Muy Crítico	X > 1.000'000.000
4	Crítico	100'000.000 > X < 1.000'000.000
3	Moderado	20'000.000 > X < 100'000.000
2	Leve	0 > X < 20'000.000
1	Sin afectación	No existe afectación al recurso

Tabla 9. Escala de impacto al recurso financiero.

ESCALA DE IMPACTO AL DESARROLLO DE PROCESOS		
5	Muy Crítico	La materialización del riesgo afecta al país.
4	Crítico	La materialización del riesgo afecta la operación del instituto.
3	Moderado	La materialización del riesgo afecta la operación del área o proceso y de otros procesos de la empresa.
2	Leve	La materialización del riesgo afecta la operación del área o proceso
1	Sin afectación	No existe afectación al recurso

Tabla 10. Escala de impacto al desarrollo de procesos.

ESCALA DE IMPACTO AL CUMPLIMIENTO DE OBJETIVOS		
5	Muy Crítico	La materialización del riesgo afecta el cumplimiento de los objetivos del País.
4	Crítico	La materialización del riesgo afecta el cumplimiento de los objetivos del instituto.
3	Moderado	La materialización del riesgo afecta el cumplimiento de los objetivos de más de un proceso.
2	Leve	La materialización del riesgo afecta el cumplimiento de los objetivos de un proceso.
1	Sin afectación	No existe afectación al recurso

Tabla 11. Escala de impacto al cumplimiento de objetivos.

ESCALA DE IMPACTO AL MEDIO AMBIENTE		
5	Muy Crítico	La materialización del riesgo produce impactos ambientales recuperables a largo plazo. (Más de 20 de años).
4	Crítico	La materialización del riesgo produce impactos ambientales que pueden ser recuperados en un periodo mediano de tiempo (de 10 a 20 años)
3	Moderado	La materialización del riesgo produce impactos ambientales que pueden ser recuperados en un periodo corto de tiempo. (Hasta 10 años).
2	Leve	La materialización del riesgo no produce impactos ambientales
1	Sin afectación	No existe afectación al recurso. Diferencia respecto al anterior ?

Tabla 12. Escala de impacto al medio ambiente.

ESCALA DE IMPACTO A LA INFORMACIÓN		
1	Muy Crítico	El evento afecta información confidencial o estratégica o indispensable para continuidad del negocio.
2	Crítico	El evento puede afectar información confidencial o estratégica o importante para la continuidad del negocio.
3	Moderado	El evento no afecta información confidencial ni estratégica o poco importante para la continuidad del negocio.
4	Leve	El evento no afecta información confidencial ni estratégica o no importante para la continuidad del negocio.
1	Sin afectación	No existe afectación al recurso

Tabla 13. Escala de impacto a la información.

3.2.11. Probabilidad Inherente

Este valor se establece teniendo en cuenta: la posibilidad de ocurrencia del riesgo (relación amenaza - vulnerabilidad), los controles existentes enfocados a reducir la probabilidad de ocurrencia del riesgo y la importancia del activo para la organización debido que esto puede aumentar el interés por vulnerarlo, tomando como referencia la escala de valoración disponible en la tabla Tabla 14. Escala de probabilidad.

ESCALA DE PROBABILIDAD		
5	Casi Certeza	Se espera que ocurra en la mayoría de las circunstancias
4	Probable	Posiblemente ocurrirá en la mayoría de las circunstancias
3	Posible	Podría ocurrir en algún momento
2	Improbable	Pudo ocurrir en algún momento
1	Raro	Puede ocurrir solo en circunstancias excepcionales

Tabla 14. Escala de probabilidad.

3.2.12. Calculo de riesgo residual

El cálculo del riesgo residual se efectúa con base en el valor establecido previamente de probabilidad e impacto y Corresponde al nivel de riesgo del Instituto con los controles existentes actualmente.

El nivel de riesgo inherente da la pauta para la definición de nuevos controles o mejoras de los existentes teniendo en cuenta que el nivel aceptable de riesgo es el nivel bajo para los demás niveles se deberá definir planes para su tratamiento.

La escala de valoración de riesgo Inherente es la siguiente:

Escala de Valoración de Riesgo
Extremo
Alto
Medio
Bajo

Tabla 15. Escala de Valoración de Riesgo Residual

PROBABILIDAD		IMPACTO				
		Sin Afectación	Leve	Moderado	Crítico	Muy Crítico
		1	2	3	4	5
Casi Certeza	**5**	A	A	E	E	E
Probable	**4**	M	A	A	E	E
Posible	**3**	B	M	A	E	E
Improbable	**2**	B	B	M	A	E
Raro	**1**	B	B	M	A	A

Tabla 16. Matriz de Riesgo Residual

- E= Extremo
- A= Alto
- M=Medio
- B=Bajo

3.2.13. Opciones de tratamiento

Las opciones para el tratamiento de los riesgos son las siguientes:

- Evitar el riesgo.
- Reducir el riesgo.
- Compartir o transferir los riesgos.
- Asumir el riesgo

3.2.14. Matriz opciones de Tratamiento

PROBABILIDAD		IMPACTO				
		Sin Afectación	Leve	Moderado	Crítico	Muy Crítico
		1	2	3	4	5
Casi Certeza	5	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos.	>Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos.	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos.	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos.
Probable	4	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	>Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos
Posible	3	> Asumir el riesgo	>Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos
Improbable	2	> Asumir el riesgo	>Asumir el riesgo	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos
Raro	1	> Asumir el riesgo	>Asumir el riesgo	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos	> Evitar el riesgo. > Reducir el riesgo. > Compartir o transferir los riesgos

Tabla 17. Matriz de Opciones de Tratamiento

3.2.15. Definición de planes de tratamiento

Se deben definir planes de tratamiento para los activos de información que se encuentren por fuera del nivel de riesgo aceptable.

Tal como lo contempla la *Guía de Administración del Riesgo* del DAFP (Departamento Administrativo de la Función Pública), los riesgos calificados como *Extremos* y *Altos* serán incluidos dentro de los planes de mitigación, y los riesgos calificados como *Medios* y *Bajos* serán monitoreados.

3.3. MONITORIZACIÓN

Una vez diseñado y validado el plan para administrar los riesgos, en el mapa de riesgos, es necesario monitorearlo teniendo en cuenta que estos nunca dejan de representar una amenaza para el Instituto.

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficacia en su implementación adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

A partir del análisis y calificación de riesgos, se debe formular un plan para el tratamiento de riesgos que identifique la gestión apropiada, los recursos, responsabilidad y prioridades para manejar los riesgos de seguridad de la información.

El IDEAM debe ejecutar procedimientos de seguimiento y revisión para detectar oportunamente los errores en los procesamientos e identificar con prontitud incidentes e intentos de violación de seguridad, así como determinar si las acciones tomadas para solucionar un problema de seguridad fueron eficaces.

HISTORIAL DE CAMBIOS

Versión	Fecha	Descripción
01	01/11/2017	Creación del documento
02	15/03/2018	Actualización del documento

ELABORÓ:	REVISÓ:	APROBÓ:
Luis Alejandro Pinilla Oficial de Seguridad de la Información	**Eduardo Ramírez Acosta** Profesional Especializado Oficina Informática	**Leonardo Cárdenas Chitiva** Jefe Oficina Informática